

Study on Potential Policy Measures to Promote the Uptake and the Use of AI in Belgium in Specific Economic Domains

Part 1: Gap Analysis



Disclaimer: this study has been executed by a contractor external to the FPS Economy, S.M.E.s, Self-employed and Energy. The opinions reflected in the study are the author's own and do not form any indication of the position of the FPS Economy or the Belgian State regarding the subject of the study. The FPS Economy cannot be held responsible for any inaccuracies as to the information contained in the study.



FPS Economy, S.M.E.s, Self-employed and Energy

Rue du Progrès 50 – 1210 Brussels

Enterprise no: 0314.595.348



○ 0800 120 33 (free number)



○ SPFEco



○ @spfeconomie



○ [linkedin.com/company/fod-economie](https://www.linkedin.com/company/fod-economie) (bilingual page)



○ [instagram.com/spfecocom](https://www.instagram.com/spfecocom)



○ [youtube.com/user/SPFEconomie](https://www.youtube.com/user/SPFEconomie)



○ economie.fgov.be

Responsible publisher:

Séverine Waterbley

Chair of the Board of Directors

Rue du Progrès 50 – 1210 Brussels

Internet version

225-21

TABLE OF CONTENTS

COMMON ABBREVIATIONS	8
CHAPTER 1 – PRELIMINARY CONSIDERATIONS AND OUTLINE STUDY	10
CHAPTER 2 – INTELLECTUAL PROPERTY (WP 2).....	13
1. Introduction	13
2. The Applicability of Intellectual Property Regimes on AI-Technology.....	13
2.1. IP-Protection for AI-Technology	13
2.1.1. Copyright	13
2.1.2. Patent Law.....	15
2.1.3. Conclusions	20
2.2. IP-Protection for Data	20
2.2.1. Definition of Data(base).....	21
2.2.2. Database Protection	24
2.2.3. Trade Secret/Contractual Protection.....	27
2.2.4. Conclusion	28
3. The Applicability of Intellectual Property Regimes on AI-Output.....	28
3.1. Copyright.....	29
3.1.1. Condition for Protection: Originality.....	29
3.1.2. Authorship/Ownership of AI-assisted Output.....	32
3.1.3. Other Restrictions Under Copyright: Moral Rights, Term of Protection and Exceptions	34
3.2. Sui Generis/Related Rights	34
3.2.1. Sui Generis Database Right.....	34
3.2.2. Rights of Phonogram and Film Producers.....	35
3.2.3. Rights of Broadcasters	37
3.2.4. Rights of Publishers of Press Publications	38
3.3. Patent Law	38
3.3.1. Inventorship	38
3.3.2. Patentability of AI-assisted output.....	42
A. Novelty	42
B. Inventive step.....	43
3.4. Trademark/Design Law	44
3.4.1. Trademark Protection for AI-Generated/-Assisted Output	44
A. Object of Protection: a Trademark	45
B. Formal Requirements?.....	45
C. Conclusion	45
3.4.2. Design Protection for AI-Generated/-Assisted Output AI	46
3.4.3. Other Topics under Trademark/Design Law	46
3.5. Ownership of AI-Generated Output.....	47
3.6. Infringement of Intellectual Property Rights by AI-Systems	51
3.6.1. IP-Infringement Through Input: Training of AI-Systems.....	51
3.6.2. IP-Infringement Through Output: Reproduction or Adaptation	53
3.6.3. Liability for Intellectual Property Infringement.....	53
4. Overview of the Identified Gaps.....	55
CHAPTER 3 – CONSUMER AND MARKET (WP 3)	58

1. Introduction	58
2. Competition Law (WP 3.1.)	58
2.1. Regulatory Framework	58
2.2. The Influence of AI on Competition	60
2.3. The Impact of AI on the Structure and Concentration of Markets	61
2.3.1. Data as a Competitive Advantage	61
2.3.2. Concentration	62
2.3.3. Transparency.....	63
2.4. AI-Related Competition Issues.....	63
2.4.1. Collusion by Algorithms.....	64
A. The Use of AI to Facilitate Collusion	64
B. Collusion Solely Achieved by Algorithms	65
C. Applicable Competition Law Regulations	65
D. The Attribution of Liability	66
2.4.2. Personalised Pricing.....	66
A. The Use of AI to Set up Personalised Pricing	67
B. Current Competition Law Legislation.....	68
2.5. Overview of the Identified Gaps	69
3. Consumer Protection (WP 3.2.).....	70
3.1. Introduction	70
3.2. AI is the Object of the Contract.....	70
3.2.1. Legal Rules on Warranty.....	71
A. Currently Applicable Legal Framework.....	71
B. Modifications Prescribed by Directives 2019/770 and 2019/771.....	73
B.1. Scope of Rules	73
B.2. Substantial Rules and Applicable Sanctions	75
3.2.2. Information obligations	80
A. Consumer Protection Law	81
B. Data Protection Law	84
3.2.3. Unfair Commercial Practices.....	85
A. Unfair Commercial Practices Towards Consumers	86
B. Unfair Market practices Towards Undertakings	87
3.2.4. Liability for Defective Products.....	88
3.3. AI is Used to Conclude the Contract	91
3.3.1. Use of Automated Means for Prospection	92
3.3.2. Information Obligations	93
A. Consumer Protection Law	93
B. Data Protection Law	98
3.3.3. Unfair Commercial Practices.....	99
3.3.4. Requirements for Consent	100
3.4. Overview of the Identified Gaps	101
CHAPTER 4 - TELECOMMUNICATION AND INFORMATION SOCIETY (WP 4).....	104
1. Introduction	104
2. AI Safety and Cybersecurity (WP 4.1.).....	104
2.1. Introduction	104
2.2. Security and Safety Related to AI.....	105
2.2.1. What are Cybersecurity and Safety Regarding AI?	105
2.2.2. What Characteristics of AI-systems Influence Security and Safety?.....	107
2.3. Legal Rules Governing the Security of the Design (or Security by Default) of AI-systems	109
2.3.1. Introduction.....	109
2.3.2. General Contract and Tort Law	109
A. Contract Law	109
B. Tort Law and Product Liability.....	112

2.3.3. General and Sectoral Product Safety law	114
2.3.4. General Data Protection Regulation	116
2.3.5. General Non-Sectoral Cybersecurity Regulation: The NIS Act and the CIC Act	118
2.3.6. Sectoral Cybersecurity Regulations – Security of the Design	123
2.3.7. Certification Under the EU Cybersecurity Act.....	125
2.4. Legal Requirements Governing the Security of the AI-System Post-Release	126
2.4.1. Introduction	126
2.4.2. Monitoring and Preventing Risk Post-Release	127
A. General Risk-Management under General and Specific Contract Law	127
B. General Tort Law	128
C. General Risk Management Under Book IX of the Code on Economic Law and Sectoral Product Safety Legislation.....	128
D. General Risk-Management under Data Protection Law	129
E. General Risk-Management under Non-Sectoral Cybersecurity Rules – NIS and CIC ..	130
F. General Risk Monitoring and Management under Sectoral Cybersecurity Rules	131
2.4.3. Corrective and Reporting Measures With Regard to AI-systems	132
A. General Contract and Tort Law	132
B. Product Safety Legislation	133
C. Notification Requirements and Corrective Obligations on the Basis of Data Protection Law	134
D. Non-Sectoral Cybersecurity Laws	135
E. Sectoral Cybersecurity Laws	135
2.5. Using AI to Support (Cyber)security	137
2.5.1. Can the Use of Automated Intrusion Detection Systems for Safety and/or Security be Mandated by Current Rules?	137
2.5.2. Limits on Automated Decision-Making on the Basis of the GDPR.....	139
2.5.3. Automated Intrusion Detection and Other Human Rights (Examples): Non-Discrimination, Due Process and Freedom of Expression	141
2.5.4. Who Will Defend the Defenders? On the Security of Autonomous Intrusion Detection Systems.....	142
2.6. Overview of the Identified Gaps	142
3. Data-Economy (WP 4.2.)	144
3.1. Introduction	144
3.2. Data Portability (B2C and B2B)	145
3.2.1. Personal Data Portability.....	146
A. Data Protection.....	146
B. Payment Services	147
3.2.2. Non-Personal Data Portability	148
A. Supply of Digital Content or Service	148
B. Free Flow of Non-Personal Data	149
3.2.3. European Commission’s Proposal for a Digital Markets Act.....	149
3.3. Data Sharing Regarding Numerous Individuals, Entities or Objects (G2B, B2G and B2B)	150
3.3.1. G2B Data Sharing.....	151
A. Compulsory Sharing of Public Sector Information	151
B. Voluntary Sharing of Public Sector Information	153
3.3.2. B2G Data Sharing.....	155
A. Soft Law.....	156
B. European Commission’s Proposal for a Data Governance Act	157
3.3.3. B2B Data Sharing	158
A. Soft Law.....	158
B. Transparency in B2B Data Sharing	159
C. European Commission’s Proposal for a Data Governance Act	160
D. European Commission’s Proposal for a Digital Markets Act.....	161
3.4. Overview of the Identified Gaps	161
4. Electronic Identification and Trust Services for Electronic Transactions (eIDAS Regulation) (WP 4.3.)	162

4.1. Introduction	162
4.2. The eIDAS Regulation	163
4.3. The Four Guiding Principles Applied to the Use of Artificial Intelligence	163
4.3.1. Freedom to (not) Use Electronics	164
4.3.2. Functional Equivalency	164
4.3.3. Technological Neutrality	164
4.3.4. Non-discrimination principle	164
4.4. Using AI to Fight Fraud in the Context of Trust Services	165
4.5. The Phenomenon of Batch Signing	165
4.6. Overview of the Identified Gaps	166
5. E-Commerce (WP 4.4.)	166
5.1. Introduction	166
5.2. Preliminary Remarks General Safeguards	168
5.2.1. Transparency	168
5.2.2. Harmonisation	169
5.3. Scope and Intermediaries Activities	170
5.3.1. Mere Conduit and Caching	170
5.3.2. Hosting Services	171
5.4. Focus on Liability Exemption for Hosting Services	171
5.4.1. The Distinction Between an Active and Passive Hosting Service	172
5.4.2. Actual Knowledge	173
5.4.3. Measures Taken by the Hosting Service Provider Against the Illegal Content	174
5.5. The Prohibition of the General Obligation to Monitor	176
5.6. Conclusion Regarding the Use of AI	176
5.7. Overview of the Identified Gaps	178
CHAPTER 5 – INSURANCES (WP 5)	180
1. Introduction	180
2. AI in Insurance: Benefits and Concerns	180
2.1. AI in Insurance: Benefits	180
2.2. AI in Insurance: Concerns	181
2.2.1. Data Quality	181
2.2.2. Transparency and Explainability of AI	182
2.2.3. Taking Into Account Consumer’s Individual Price Sensitivity	182
2.2.4. Absence of Human Intervention	183
2.2.5. Interoperability	183
2.2.6. Third-Party Services and Outsourcing	183
2.2.7. Pricing Competition and Adverse Selection	184
2.2.8. Availability, Access and Affordability of Insurance	184
2.2.9. Direct and Indirect Discrimination	184
2.2.10. Ethics, Fairness and Sustainability S-goal	185
3. Policy Proposals Made by Interest Groups	186
4. Current Belgian Legal Framework	187
4.1. General Point of Attention: ‘Multi-layered’ Belgian law	187
4.2. Current Belgian Law Regarding ‘Operational-Related’ Concerns	188
4.2.1. Compliance Monitoring and Supervision of AI-Technologies in Insurance	188
4.2.2. General Data Protection Regulation	189
4.3. Current Belgian Law Regarding ‘Impact-Related’ Concerns	189
4.3.1. Insurance Contract Law	189
4.3.2. Conduct of Business Rules	190
4.3.3. General Anti-Discrimination Laws	191
4.3.4. Consumer Law Applicable to Insurance Contracts Concluded with Consumers	191
5. Shortcomings/Gaps of the Current Legal Framework	192

5.1. Shortcomings Regarding 'Operational Related' Concerns.....	192
5.1.1. General Data Protection Regulation	192
5.1.2. Data Portability.....	196
5.1.3. Control of AI-Technologies/Algorithms	196
5.1.4. Financial/Conduct of Business Supervision.....	198
5.2. Shortcomings Regarding 'Impact-Related' Concerns	198
5.2.1. Insurance Contract Law	199
5.2.2. Conduct of Business Rules	199
6. Overview of the Identified Gaps With regard to AI and Insurances	200
6.1. 'Operational-Related' Gaps.....	200
6.2. 'Impact-Related' Gaps	200
CHAPTER 6 – CONCLUSIONS	202

COMMON ABBREVIATIONS

CDR: Council Regulation (EC) No 6/2002 of 12 December 2001 on Community Designs

CCL: Code of Civil Law

CDSM Directive: Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market

CEL: Code of Economic Law

CIA: confidentiality, integrity, availability

CIC Act: Act of 1 July 2011 on the security and protection of critical infrastructures

CJEU: Court of Justice European Union

Database Directive: Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

DMA (Proposal): Digital Market Act (Proposal)

DSA (Proposal): Digital Service Act (Proposal)

DGA (Proposal): Data Governance Act (Proposal)

EC: European Commission

EIOPA: European Insurance and Occupational Pensions Authority

ENISA: European Union Agency for Cybersecurity

Enforcement Directive: Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights

EPC: European Patent Convention

EPO: European Patent Office

GDPR: Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data

InfoSoc Directive: Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

NIS Directive: Directive 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems

ODD: Open Data Directive (Directive 2019/2024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information)

OES: Operators of Essential Services

OSP: Operator Security Plan

P2b Regulation: Regulation on platform-to-business relations (Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services)

Proposal NIS 2 Directive: Proposal for directive on measures for high common level of cybersecurity across the Union

PSD2: Payment Services Directive 2 (Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market)

PSA: Person Skilled in the Art

Rental and Lending Rights Directive: Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property

Software Directive: Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs

TFEU: Treaty of the Functioning of the European Union

TMR: Trade Mark Regulation (Regulation (2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark)

CHAPTER 1 – PRELIMINARY CONSIDERATIONS AND OUTLINE STUDY

Artificial intelligence (AI) and robots are becoming increasingly important in our daily lives.¹ AI systems are already used for a variety of purposes and deployed in many sectors. Examples are self-driving vehicles, surgical robots, chatbots or virtual assistants. It goes even further. AI systems are increasingly being used for fraud detection, diagnosis of diseases (cf. IBM's WATSON)² or marketing purposes (cf. personalised targeting). It is also deployed in sports to reduce injuries or make tactical decisions and may even be relied upon in the legal profession. For instance, LawGeex developed an algorithm to review contracts. In an experiment, human lawyers took an average of 92 minutes to complete the task achieving an accuracy level of 85 percent. The software only took 26 seconds to review the contracts and achieved an accuracy level of 94 percent.³ Even more striking, Google Brain developed an AI system (AutoML) that has created its own "child".⁴ In sum, we "are in the midst of a robotics revolution".⁵

Before proceeding with the study, a proper definition of the concept of AI is required. Although there is currently not a universally accepted technical or legal definition, a distinction is often made between weak, strong and super AI. Artificial narrow intelligence (ANI) or weak AI refers to systems that can perform a specific or few tasks very well, in some cases even better than humans. They operate within a predefined environment (e.g. facial recognition, recommendation systems or self-driving cars). Artificial general intelligence (AGI) or strong AI refers to machines that exhibit human intelligence. AGI aims to perform any intellectual task that a human being is able to do. General AI refers to a system that is intelligent in all domains just like humans. Artificial superintelligence (ASI) – 'singularity' – is the point at which AI systems will outsmart humans. It refers to any intellect that greatly exceeds the cognitive performance of humans in virtually all domains of interest (p. 5-6).⁶ Nowadays, all AI application are (still) weak.⁷

A distinction is often made between a knowledge-based approach (top-down) on the one hand and a data-based approach on the other hand (bottom-up). The former implies that an expert in the field tries to pour his/her knowledge into a model (e.g. a set of rules, patterns or logical statements). This model is subsequently implemented as a series of instructions – and thus as an algorithm – in the machine to obtain its goal. Such systems aim to capture the knowledge of human experts (e.g. doctors) to support autonomous decision-making. The data-driven approach emerged because of the large amount of available data. Systems are presented with many examples of input and the corresponding output. This process of deducing patterns and learning from examples/experience is called machine learning (ML).⁸ Machine learning is the scientific study of algorithms of computer systems that learn through experience. ML algorithms build a model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so. The system itself finds or recognises patterns in order to provide correct answers.⁹ For instance, AI systems can be shown thousands of images of cats and dogs to

¹ R. LEENES et al., "Regulatory challenges of robotics: some guidelines", *Law, Innovation and Technology* 2017, vol. 9, no. 2, p. 2; G. HALLEVY, "Criminal Liability of Artificial Intelligence Entities - From Science Fiction to Legal Social Control", *Akron Intellectual Property Journal* 2010, vol. 4, no. 2, p. 172.

² P. MARKS, "Dr House goes digital as IBM's Watson diagnoses rare diseases", *New Scientist*, 18 October 2016.

³ C. JEFFREY, "Machine-learning algorithm beats 20 lawyers in NDA legal analysis", *Techspot*, 31 October 2018.

⁴ A. SULLEYMAN, "Google AI creates its own 'child' AI that's more advanced than systems built by humans", *Independent*, 5 December 2017.

⁵ R. CALO, "Robots in American Law", University of Washington School of Law Research Paper no. 2016-04, p. 3.

⁶ European Commission, "AI Watch Historical Evolution of Artificial Intelligence", November 2020, p. 5-6. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120469/jrc120469_historical_evolution_of_ai-v1.1.pdf.

⁷ R. DEVILLÉ, N. SERGEYSSELS and C. MIDDAG, "Basic Concepts of AI for Legal Scholars", in J. DE BRUYNE and C. VANLEENHOVE, *Artificial Intelligence and the Law*, Antwerp, Intersentia, 2021, p. 1-21; S.J. RUSSELL AND P. NORVIG, *Artificial Intelligence: a modern approach*, Pearson Education Limited, 2016, 1132 p.

⁸ R. DEVILLÉ, N. SERGEYSSELS and C. MIDDAG, "Basic Concepts of AI for Legal Scholars", in J. DE BRUYNE and C. VANLEENHOVE, *Artificial Intelligence and the Law*, Antwerp, Intersentia, 2021, p. 1-21. Also see: E. MANNENS, "Wat je moet weten over AI", in J. DE BRUYNE and N. BOUTECA, *Artificiële intelligentie en maatschappij*, Gompel & Svacina, 2021, p. 17-49.

⁹ European Commission, "AI Watch Historical Evolution of Artificial Intelligence", November 2020, p. 5-6.

learn the distinctions (cf. supervised learning). After a while, the system will be able to make a distinction between dogs and cats.

The European Commission (EC) defines AI as systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based acting in the virtual world (e.g. voice assistants, image analysis software or speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).¹⁰ The High Level Expert Group on AI – also known as the AI HLEG – expands this definition.¹¹ AI systems are software (possibly embedded in hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.¹² Artificial intelligence is also defined in the recent Proposal for a Regulation on AI. It refers to software that is developed with one or more of the techniques and approaches listed in Annex I (e.g. machine learning approaches, logic and knowledge-based approaches and statistical approaches) and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations or decisions influencing the environments they interact with (article 3(1)). We will rely on this working definition of AI.¹³

The rise of AI systems is no surprise considering their many benefits. They can be more accurate and efficient because they process information faster than humans.¹⁴ Consequently, they may perform many tasks ‘better’ than their human counterparts.¹⁵ Companies from various economic sectors already rely on AI-applications to decrease costs, generate revenues, increase product quality and improve their competitiveness.¹⁶ AI systems and robots can also have advantages for the specific sector in which they are to be used. For instance, traffic will become safer with autonomous vehicles. The number of accidents should decrease as computers are generally much better drivers than humans. More generally, transport will become more time-efficient with autonomous car technology. Self-driving cars will also enable people currently facing restrictions in operating a vehicle – such as the elderly, minors or disabled people – to fully and independently participate in traffic.¹⁷ At the same time, however, several challenges exist as well. Think of AI systems that discriminate against women in a job application¹⁸ or identify black persons on a picture as gorillas (cf. bias)¹⁹ Other ethical questions include the human-machine relationship, and especially which role humans may still play in an AI-era. Another ethical issue relates to the choice that a self-driving car has to make when a collision may occur, for instance between hitting an old

¹⁰ European Commission, “Communication on Artificial Intelligence for Europe”, 25 April 2018, COM(2018) 237 final, p. 1.

¹¹ Following the launch of its AI Strategy in 2018, the European Commission appointed a group of 52 experts to advise for its implementation. The group members were selected following an open selection process and comprised representatives from academia, civil society and industry.

¹² High-Level Expert Group on Artificial Intelligence, “A definition of AI: Main capabilities and scientific disciplines”, 8 April 2019, p. 6.

¹³ European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI, COM/2021/206 final.

¹⁴ S.G. TZAFESTAS, *Roboethics: A Navigating Overview*, Athens, Springer, 2015, p. 147.

¹⁵ H.M. DEITEL and B. DEITEL, *Computers and Data Processing: International Edition*, Orlando, Academic Press, 2014, p. 434. See in this regard the experiment with supercomputer WATSON and the identification of lung cancer cases (I. STEADMAN, “IBM’s Watson is better at diagnosing cancer than human doctors”, *Wired*, 11 February 2013).

¹⁶ S.H. IVANOV, “Robonomics - Principles, Benefits, Challenges, Solutions”, *Yearbook of Varna University of Management* 2017, vol. 10, p. 283-285.

¹⁷ See for example: J.R. ZOHN, “When Robots Attack: How Should the Law Handle Self Driving Cars That Cause Damages?”, *University of Illinois Journal of Law, Technology and Policy* 2015, vol. 2, p. 471.

¹⁸ J. DASTIN, “Amazon scraps secret AI recruiting tool that showed bias against women”, *Reuters*, 10 October 2018.

¹⁹ J. VINCENT, “Google ‘fixed’ its racist algorithm by removing gorillas from its image-labeling tech”, *The Verge*, 12 January 2018.

man and two toddlers (cf. trolley dilemma²⁰). The increased use of AI systems also affects the labour market as many professions are likely to disappear in the long term, at least change significantly. Just think of taxi drivers when vehicles become autonomous.²¹ Some even predict that AI systems could challenge/threaten humanity in the long term.²²

More importantly, the commercialisation of AI will also pose several challenges from a legal and regulatory point of view as it affects nearly all legal domains.²³ In this study, we will examine the impact of AI on several legal domains that are relevant for the Federal Public Service Economy. More specifically, the study will focus on intellectual property (chapter 2), consumer and market (chapter 3), telecommunications and information society (chapter 4) and insurances (chapter 5). The main conclusions are summarised in a final part (chapter 6). It should be noted that all the chapters should be read together to have a proper understanding of the impact of AI on the legal framework and identified domains. The study is based on desk research and legal analysis. The scope of the application of the legal rules are identified for each chapter. It will then be analysed to which extent they apply to AI and where shortcomings in the legal framework may remain. In each chapter, the main gaps in the legal framework will be provided as well in a separate part. The legal comparative study as well as the normative recommendations will be based upon this analysis.

²⁰ This trolley dilemma has been criticised. It is too simplistic and does not really represent a real dilemma.

²¹ See for more information: M. WEBB, "The Impact of Artificial Intelligence on the Labor Market", 6 November 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3482150; C.B. FREY and M.A. OSBORNE, "The future of employment: How susceptible are jobs to computerisation?", *Technological Forecasting and Social Change* 2017, vol. 114, 254-280.

²² See: N. BOSTROM, *Superintelligence: Paths, Dangers, Strategies*, Oxford, Oxford University Press, 2014, p. 328.

²³ R. LEENES et al., o.c., p. 2. See in general: M. EBERS and S. NAVAS (eds.), *Algorithms and Law*, Cambridge, Cambridge University Press, 2020, 319 p.; A. DE STREEL and H. JACQUEMI, *L'intelligence artificielle et le droit*, CRIDS, Larcier, 2018, 482 p.; J. DE BRUYNE and C. VANLEENHOVE, *Artificial Intelligence and the Law*, Antwerp, Intersentia, 2021, 520 p.

CHAPTER 2 – INTELLECTUAL PROPERTY (WP 2)

1. Introduction

In this part we will discuss how AI-technology fits in the current intellectual property framework. In general, we aim to provide insight into what extent the Belgian (and European) intellectual property framework is still fit-for-purpose in the age of AI. More specifically, the analysis will consist of four parts. In the first part, we will discuss to what extent AI-systems/-technologies can be protected by intellectual property rights. We will look at the AI-model/-software, hardware and the data such systems require to function (part 2). In the second part, we will turn to AI-generated results and discuss if and how they may be protected under the various intellectual property regimes. We will make a further distinction between results that have been generated without any human intervention and results involving human intervention. In this part we will also discuss the possibility of intellectual property infringement by AI-systems (part 3). In a concluding part, the main gaps are briefly summarised (part 4).²⁴

2. The Applicability of Intellectual Property Regimes on AI-Technology

In this part the report will discuss if and to what extent AI-systems themselves may be protected by Belgian/European intellectual property law. We will first look into the question of how AI-software and -hardware may be covered by copyright and/or patent law (part 2.1.). Subsequently, we will address how data may be protected by intellectual property rights (part 2.2.). The focus on copyright and patent law is justified by the fact that trademark and/or design law seem rather unsuitable for protecting AI-systems themselves. Of course, services or goods including AI-components will be able to have their brand, logo or product appearance protected by trademarks, respectively design rights, insofar as they meet the validity requirements.²⁵ We do not think, however, that this will give rise to any peculiar issues that need to be addressed in this report.

2.1. IP-Protection for AI-Technology

2.1.1. Copyright

In order to enjoy copyright, it is required that works constitute a concrete and original expression by the author(s).

Belgian copyright law only protects 'works' (Article XI.165 Code of Economic Law – CEL). Although this term is not defined, it is generally understood to exclude mere ideas, methods of operation or mathematical concepts as such from copyright protection and reserve it for actual, concrete

²⁴ This chapter is based on previous research on this topic including: J. VANHERPE, "AI and IP – a tale of Two Acronyms", in J. DE BRUYNE en C. VANLEENHOVE, *Artificial Intelligence and Law*, Antwerpen, Intersentia, 2021, p. 207-239, forthcoming; J. ALLAN e.a., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, Luxembourg, Publications Office of the European Union, 2020; M. IGLESIAS, S. SHAMUJLA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, Luxembourg, Publications Office of the European Union, 2020.

²⁵ In this regard, one needs to acknowledge that the words 'AI' or 'artificial intelligence' lack distinctive character in relation to AI-related goods or services, rendering them unavailable for trademark protection in this context. With regard to product appearance, it is rather unlikely that e.g. an AI-algorithm would have a new product appearance, resulting in an individual character. See: Art. 4 and 7 of Regulation 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark, *OJ L* 154/1, p. 1-99, and Art. 3-6 of Council Regulation 6/2002 of 12 December 2001 on Community designs, *OJ L* 3, p. 1-24.

creations or expressions of ideas.²⁶ No further conditions apply, meaning that works can take all kinds of shapes and forms.²⁷

Furthermore, these works must be 'original'. The interpretation of this criterion has been harmonised to a considerable degree by the case law of the Court of Justice of the European Union (CJEU), often later confirmed by the Belgian Court of Cassation. In summary, the condition of originality entails that a work needs to be an intellectual creation of its author(s) reflecting the personality of the author and expressing his/her free and creative choices in the production of the work.²⁸ By making certain choices, the author applies his "personal touch" to the work.²⁹ Under Belgian copyright law, the subjective component of the originality criterion (i.e. the author's personality) is thus of paramount importance.³⁰

Importantly, Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs extended copyright protection to computer programs. Article 1 stipulates that computer programs (including their preparatory design material) shall be protected by copyright, just as literary works within the meaning of the Berne Convention. It also reaffirms that such protection only applies to the expression in any form of a computer program. Vice versa, it excludes ideas and principles underlying any element of a computer program, including those which underlie its interfaces, from protection by copyright. Finally, it stipulates that computer programs will be protected if they are original meaning that they should be their author's own intellectual creation (see *supra*). Articles XI.294 and XI.295 CEL constitute the transposition into Belgian law.

AI-systems derive their 'intelligence' mainly from the innovative software on which they run. In an AI-context it is, however, crucial to keep the requirement of a concrete expression in mind. This requirement will in fact prevent an algorithm 'as such', providing a certain functionality, from enjoying copyright protection.³¹ After all, algorithms are methods of operation or mathematical concepts which are being implemented in a concrete software program.³² This is also confirmed by recital 11 of Directive 2009/24: "In accordance with this principle of copyright, to the extent that logic, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected under this Directive" (own underlining).

The object and source code of AI-software, through which the underlying algorithms and ideas are implemented, will, however, be considered to be sufficiently concrete, allowing for copyright

²⁶ Art. 9, §2 TRIPS; Cass. 17 February 2017, *IRDI* 2017, no. 2, p. 135; F. GOTZEN and M.-C. JANSSENS, *Wegwijs in het intellectueel eigendomsrecht*, Brugge, Vanden Broele, 2019, p. 36.

²⁷ See, for instance, art. 2 of the Berne Convention: "the expression "literary and artistic works" shall include every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression [...]"; F. GOTZEN and M.-C. JANSSENS, *Wegwijs in het intellectueel eigendomsrecht*, o.c., p. 42.

²⁸ CJEU, 16 July 2009, no. C-5/08, ECLI:EU:C:2009:465, *Infopaq/Danske Dagblades Forening*, §37-39 and §45; CJEU 22 December 2010, no. C-393/09, ECLI:EU:C:2010:816, *BSA/Ministerstvo kultury*, §46; CJEU 23 January 2014, no. C-355/12, ECLI:EU:C:2014:25, *Nintendo/PC Box*, §21; CJEU 13 November 2018, no. C-310/17, ECLI:EU:C:2018:899, *Levola/Smilde*, § 36-40.

²⁹ CJEU 1 December 2011, no. C-145/10, ECLI:EU:C:2011:798, *Painer/Standard*, §92 and §99; Cass. 31 October 2013, RW 2013-2014, p. 1464; Cass. 17 March 2014, *ICIP* 201, no. 2, 251; 4; Cass. 14 December 2015, *ICIP* 2016, p. 193.

³⁰ The objective component being that a certain minimum level of (human) intellectual work is required. See: F. GOTZEN and M.-C. JANSSENS, *Wegwijs in het intellectueel eigendomsrecht*, o.c., p. 37.

³¹ CJEU 2 May 2012, no. C-406/10, ECLI:EU:C:2012:259, *SAS/World Programming*, §39-40 and §46 (in this judgment, the CJEU ruled out copyright protection for the functionality of a computer program, the programming language and the format of data files used in a computer program as they do not form an expression of the software); J. VANHERPE, "AI and IP – a tale of Two Acronyms", in J. DE BRUYNE en C. VANLEENHOVE, *Artificial Intelligence and Law*, Antwerpen, Intersentia, 2021, p. 207-239, forthcoming; M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, Luxembourg, Publications Office of the European Union, 2020, p. 9. Moreover, one could also argue that an algorithm is determined by technical and functional prerequisites, excluding copyright protection under the so-called 'technical restriction' in copyright law.

³² See for instance the definition by the Cambridge dictionary of 'algorithm': a set of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem.

protection if they meet the originality-threshold.³³ That threshold is generally easily reached in practice, resulting in copyright protection for the large majority of AI-software. Besides, the Graphical User Interface (GUI) of such software will usually be eligible for ‘ordinary’ copyright protection, unless the expression, arrangement or configuration of the components of the GUI is dictated by their technical function.³⁴

Due to the multiplicity of authors in a software programming context and the widespread use of open source software, applying software copyright protection in practice is not that evident.³⁵ These issues are, however, not AI-specific and a further elaboration on these issues would surpass the scope of this report.³⁶

2.1.2. Patent Law

Patent law aims to reward investment into research and development in order to incentivise further innovation. It does so by providing patentees with an exclusive right to exclude others from exploiting a certain ‘invention’, a technological improvement that takes the form of a product or a process (or both) (Article XI.3 CEL).

In order to be eligible for a patent, the invention must satisfy a number of conditions. First, there are certain exclusions to patent protection based on the claimed subject matter. The list of excluded subject matter under the European Patent Convention (EPC) and the Belgian Code of Economic Law (CEL) (respectively Article 52-53 EPC and Article XI. 4-5 CEL) includes e.g. ideas that are deemed too abstract to qualify for patent protection, such as computer programs, mere presentations of information, discoveries, methods for performing mental acts or doing business and mathematical methods (such as pure algorithms).

This constitutes a first obstacle for organisations seeking to obtain patent protection for AI-related technology as AI and machine learning are based on computational models and algorithms. In a recent update of its ‘Guidelines for Examination’, the European Patent Office (EPO) explicitly confirmed that it intends to treat the underlying computational models and algorithms *per se* as a kind of mathematical method.³⁷ This implies that AI in abstract form is not patentable *as such* in accordance with Article 52 EPC.³⁸ The Guidelines further mention that the guidance provided for mathematical methods can be used for such computational models and algorithms.

The guidance in relation to mathematical methods further clarify that the exclusion applies if a claim is directed to a purely abstract mathematical method and the claim does not require any technical means. If a claim, on the contrary, is directed either to a method involving the use of technical means (e.g. a computer) or to a technical device, its subject-matter has a technical character as a whole and is not excluded from patentability.

Interestingly, the updated guidelines further draw special attention to the clarity of terms used in claims related to mathematical methods, stating that ‘this is of particular importance where such terms are used in significantly different ways in the application itself and/or in relevant prior art documents, as this maybe an indicator that the terms have no well-recognised [technical] meaning

³³ Art. 10, §1 TRIPS Agreement (Computer programs, whether in source or object code, shall be protected as literary works); CJEU, 22 December 2010, no. C-393/09, ECLI:EU:C:2010:816, *BSA/Ministerstvo kultury*, §33-35; M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, Luxembourg, Publications Office of the European Union, 2020, p. 9.

³⁴ CJEU, 22 December 2010, no. C-393/09, ECLI:EU:C:2010:816, *BSA/Ministerstvo kultury*, §48-51.

³⁵ See in an AI-context, e.g. TensorFlow (www.tensorflow.org) or Keras (www.keras.io)

³⁶ See also: J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., p. 232, §34, forthcoming.

³⁷ European Patent Office (EPO), “Guidelines for Examination, Part G, Chapter II, 3.3.1”, 2020, available at www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm.

³⁸ M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 6

and may leave the reader in doubt as to the meaning of the technical features to which they refer, which may lead to findings of lack of technical character of the claims'.³⁹ One can indeed imagine that this may well be relevant in relation to AI-systems, as the technology is still evolving and fundamental research is still being conducted. The Guidelines therefore also additionally state that "terms such as "support vector machine", "reasoning engine" or "neural network" may, depending on the context, merely refer to abstract models or algorithms and thus do not, on their own, necessarily imply the use of a technical means. This has to be taken into account when examining whether the claimed subject-matter has a technical character as a whole" (see also *infra*).⁴⁰

Moreover patent protection for AI is also available under the regime of computer-implemented inventions (CII – "software patents").⁴¹ A computer-implemented invention is one which involves the use of a computer, computer network or other programmable apparatus, where one or more features are realised wholly or partly by means of a computer program.⁴² If such computer program produces a "further technical effect" when run on a computer, it obtains a 'technical character' and becomes patentable.⁴³

A "further technical effect" is a technical effect going beyond the "normal" physical interactions between the program (software) and the computer (hardware) on which it is run. The normal physical effects of the execution of a program, e.g. the circulation of electrical currents in the computer, are not in themselves sufficient to confer technical character to a computer program (T 1173/97 and G 3/08). An example of such further technical effect is the control of a technical process or of the internal functioning of the computer itself or its interfaces. Subsequently, if such further technical effect has been established, the computational efficiency of an algorithm affecting the established technical effect contributes to the technical character of the invention and thus to inventive step (for instance, where the design of the algorithm is motivated by technical considerations of the internal functioning of the computer.)

Once it has been ascertained that the claimed invention indeed has a technical character, one must investigate whether it also satisfies a number of substantive conditions. More specifically, an invention must be novel and inventive as well as industrially applicable (Article 52 *jo* 54-57 EPC, Article XI.3 *jo* Article XI.6-7 CEL). The novelty requirement implies that the invention may not form part of the state of the art (i.e. what has been made available to the public) at the date of filing of the patent application, while the condition of inventive step requires the invention to not have been obvious to a theoretical person skilled in the art (PSA) on the basis of this state of the art.⁴⁴ Finally, the invention must be susceptible to use in an industrial context (Article 57 EPC, Article XI.8 CEL). In contrast to the regime on excluded subject matter set out above, these conditions do

³⁹See: European Patent Office (EPO), "Guidelines for Examination, Part G, Chapter II, 3.3", 2020 available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3.htm.

⁴⁰ European Patent Office (EPO), "Guidelines for Examination, Part G, Chapter II, 3.3.1", o.c.

⁴¹ M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 8.

⁴² The Guidelines define 'computer program' as "a sequence of computer-executable instructions specifying a method". See: European Patent Office (EPO), "Guidelines for Examination, Part G, Chapter II, 3.6", 2020, available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_6.htm.

⁴³ European Patent Office (EPO), "Guidelines for Examination, Part G, Chapter II, 3.6", o.c.; M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 6. See for a list of examples: M. HASHIGUCHI, "The Global Artificial Intelligence Revolution Challenges Patent Eligibility Laws", *J Bus & Tech L* 2017, p. 1, 16-19, 23; M. HASHIGUCHI, "Artificial Intelligence and the Jurisprudence of Patent Eligibility in the United States, Europe, and Japan", *Intell Prop & Tech LJ* 2017, p. 3, 6-7.

⁴⁴ Respectively Art. 54-55 EPC and Art. 56 EPC. In determining whether a certain invention involves inventive step (and is therefore not 'obvious'), the EPO as well as the Belgian courts apply the so-called 'problem-solution approach'. This approach involves (i) determining the so-called 'closest prior art', (ii) establishing the 'objective technical problem' in the state of the art, and (iii) considering whether or not the claimed invention, starting from the closest prior art and the objective technical problem, would have been obvious to the skilled person ('could-would approach', see in more detail EPO, "Guidelines for Examination, Part G, Chapter VII.5", available at www.epo.org/law-practice/legal-texts/html/guidelines/e/g_vii_5.htm).

not appear to pose any challenges specific to AI-related inventions. These conditions equally apply to the electronical hardware components related to AI (e.g. semiconductor technology, sensors,...) which can also be patented.

For the assessment of inventive step, the Guidelines state that “all features which contribute to the technical character of the invention must be taken into account. When the claimed invention is based on a mathematical method, it is assessed whether the mathematical method contributes to the technical character of the invention. A mathematical method may contribute to the technical character of an invention, i.e. contribute to producing a technical effect that serves a technical purpose, by: i) its application to a field of technology, and/or ii) being adapted to a specific technical implementation (T 2330/13)”. The specific criteria for assessing these two situations are explained in more detail in the Guidelines.⁴⁵ The sub-part of the Guidelines on AI interestingly also provide some examples of AI-technology from various fields of technology which the EPO deemed patentable (or not). For example, this will be the case for a neural network used ‘in a heart-monitoring apparatus for the purpose of identifying irregular heartbeats’ as it makes technical contribution. The EPO further indicates that the classification of digital images, videos, audio or speech signals based on low-level features (e.g. edges or pixel attributes for images) are typical technical applications of classification algorithms.⁴⁶ On the contrary, classifying text documents solely in respect of their textual content is not regarded to be *per se* a technical purpose but a linguistic one (T 1358/09). Classifying abstract data records or even ‘telecommunication network data records’ without any indication of a technical use being made of the resulting classification is also not *per se* a technical purpose, even if the classification algorithm may be considered to have valuable mathematical properties such as robustness (T 1784/06). In summary, it is advisable that applicants explicitly include the field of technology in the application and ensure that the objective technical problem is directly derivable from the application in order to allow for the determination of (the level of knowledge of) the skilled person.

Furthermore, the Guidelines also state the following: “Where a classification method serves a technical purpose, the steps of generating the training set and training the classifier may also contribute to the technical character of the invention if they support achieving that technical purpose”.⁴⁷ It has been suggested that this may mean that a European patent would in principle be granted to a method of training an AI or machine learning algorithm, or to a method of generating training data for this purpose, if it is possible to credibly link the method to a reliable and repeatable technical effect.^{48 49}

However, the application of these principles in practice is often unclear. Further guidance regarding the patentability of computer-implemented inventions may be developed by the Enlarged Board of Appeal at the EPO in its forthcoming decision in the *Pedestrian simulation* case

⁴⁵ European Patent Office (EPO), “Guidelines for Examination, Part G, Chapter II, 3.3 – Technical applications / Technical implementations”, 2020 available https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3.htm

⁴⁶ European Patent Office (EPO), “Guidelines for Examination, Part G, Chapter II, 3.3.1”, o.c.

⁴⁷ This may seem at odds with the addition in the recent update of the Guidelines for mathematical methods, which states “Merely specifying the technical nature of data may not be sufficient on its own to define an invention [...]. Even if the resulting method would not be considered a purely abstract mathematical method as such, it may still fall under the excluded category of methods for performing mental acts as such if no use of technical means is implied”.

⁴⁸ S. JONES, “Patentability of AI and machine learning at the EPO”, *Kluwer Patent Blog*, 21 December 2018, available at <http://patentblog.kluweriplaw.com/2018/12/21/patentability-of-ai-and-machine-learning-at-the-epo/>. See also: M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 7.

⁴⁹ According to ROGITZ, the Japan Patent Office (JPO) comes to suggest in their recently added ten new case examples pertinent to artificial intelligence-related technology to Annex A of the Examination Handbook for Patent and Utility Models (see *infra*) that novel input data and output data may be sufficient to establish an inventive step when seeking patent protection in Japan for AI-inventions. See: J.M. ROGITZ, “Japan Patent Office Case Examples on Artificial Intelligence offer Guidance for Other Offices on Treating AI Inventions”, 28 February 2019, available at <https://www.ipwatchdog.com/2019/02/28/jpo-examples-on-artificial-intelligence-offer-guidance-for-other-offices/id=106835/>

(G 1/19).⁵⁰ This pending case concerns an invention whereby the movement of a pedestrian crowd is simulated so as to inform the architectural design of venues such as railway stations or stadia. More specifically, The Enlarged Board will have to decide on whether computer-simulated inventions need a 'direct link with physical reality' or if having 'technical effect [and] purpose' is sufficient. Back in 2006, the Boards of Appeal has already held that simulation methods cannot be denied a technical effect merely on the ground that they do not yet incorporate the physical end product (T 1227/05). In other words, the Enlarged Board is now considering what is patentable in the realm of computer simulation technology, and to what extent the (simulated) technical aspects of an invention can/should be considered. Upholding the approach adopted in T 1227/05 will likely broaden the chances of patentability for AI-technologies in various industries and will render technical design software tools patentable.⁵¹

Apart from these eligibility concerns, there may be another obstacle for innovators seeking to patent AI-related innovation. This relates to the so-called 'patent bargain' between patentee and issuing government. It implies that a prospective patentee must disclose their invention in a way that is 'sufficiently clear and complete for it to be carried out by a person skilled in the art' (Article 83 EPC, Article XI.18 CEL), in return for the temporary monopoly right granted by a patent.⁵² This requirement of disclosure may be at odds with the apparent 'black box' nature of many forms of AI technology – in particular in a deep learning context –, which may make it impossible to know precisely why an AI-system arrived at a certain conclusion in a specific case.⁵³ Arguably, such AI-related inventions can therefore not be explained in a 'sufficiently clear and complete' manner, rendering the grant of a patent for such an invention impossible. As of yet, however, the scope of the disclosure requirement in AI-related inventions is not crystal-clear. In a report of the IP5 expert round table on AI it is further mentioned that the extent of the disclosure depends on what is claimed and that disclosing how an AI-model was trained (e.g. a classifier) while also providing the data used for such training may contribute to achieving a sufficient disclosure.⁵⁴ The latter has in the meantime been confirmed by the EPO's Board of Appeal in T 161/18 in relation to the training of a neural network. Moreover, while explaining why an AI-system made (or did not make) a specific decision may not be possible in some cases, experts will generally be able to disclose the algorithm, the AI-system's function(ing), structure, the applicable parameters and the basic principles to which the AI-system adheres in the description of the patent.⁵⁵ Interestingly, the Board of Appeal refused a patent application in relation to a neural network back in 2000 for not disclosing the specific information required to setup the neural network, ruling out the possibility that a person skilled in the art would be able to carry out the invention (T 0521/95). Subsequently, one can infer from this decision that it may be necessary to describe in detail the topology of a neural network and how the weights are set and, more generally, how the claimed AI-technology

⁵⁰ J. VANHERPE, "AI and IP – a tale of Two Acronyms", o.c., §10, forthcoming.

⁵¹ A. SANDYS, "Patentable or not? Regulating AI inventions for a digital future", *JUVE Patent* 24 July 2020, available at <https://www.juve-patent.com/news-and-stories/legal-commentary/patentable-or-not-regulating-ai-inventions-for-a-digital-future/>

⁵² See also B. HIGGINS, "The Role of Explainable Artificial Intelligence in Patent Law", *Intell Prop & Tech LJ* 2019, p. 2-4; M. IGLESIAS, S. SHAMUILA AND A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 7.

⁵³ M. HASHIGUCHI, "The Global Artificial Intelligence Revolution Challenges Patent Eligibility Laws", o.c., p. 29-30.

⁵⁴ X., *Report from the IP5 Expert round table on artificial intelligence*, Munich, 31 October 2018, 3, par. 9 and 10, available at https://www.fiveipoffices.org/material/ai_roundtable_2018_report/ai_roundtable_2018_report

⁵⁵ European Patent Office (EPO), "Guidelines for Examination, Part F, Chapter III, 1, §4", 2020, available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iii_1.htm; B. HIGGINS, "The Role of Explainable Artificial Intelligence in Patent Law", o.c., p. 5.

can be brought to a working example.⁵⁶ It is quite plausible that patent offices⁵⁷ will indeed deem that (a selection of) the above-mentioned information, depending on the claimed invention, is sufficient for patenting purposes, insofar as the claims are clearly formulated and supported by the description.⁵⁸ After all, an overly strict application of the disclosure requirements might discourage companies from pursuing patent protection and resort to use trade secret protection instead.⁵⁹ In any case, the risk of being excluded from patent protection constitutes an additional incentive for AI innovators to invest in so-called ‘explainable’ and transparent AI.⁶⁰

Another possibility is to look to the patenting practices in other fields of technology. For instance, WIPO’s background document on patents and emerging technologies points out that “deep learning technologies are non-deterministic: they involve some randomized initialization. Therefore, even the same training data and the same neural network architecture might lead to slightly different performance of the same machine learning model”. It then highlights the similarity of this non-deterministic character to that of biological materials, and mentions that “consideration might be given to the so-called reproducibility or plausibility of the claimed inventions based on the disclosure in a patent application”.⁶¹ Likewise READ indicates that “[p]articularly where the computer learns, the behaviour and hence a description of the computer is dynamic until training is terminated and is likely to be unpredictable”. He compares the challenges and requirements on sufficiency of disclosure for AI and machine learning inventions to that of the technical fields of chemistry and biology, and is of the opinion that many elements (like e.g. plausibility, the use of a depository for algorithms/datasets similar to the depository of micro-organisms under the Budapest Treaty, etc.), may be readily transposed to inventions based on AI and ML.⁶² The president of the EPO differs from opinion, however, and believes that a system of deposit is not suitable for algorithms because algorithms can be described in writing, unlike micro-organisms, while it will not always be necessary to disclose an entire algorithm.⁶³ Furthermore, he also points out that such system (and its administration/governance structure) would require international acceptance, which is currently lacking.⁶⁴

⁵⁶ M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 8.

⁵⁷ For instance, the Japan Patent Office has issued in January 2019 ten new case examples pertinent to artificial intelligence-related technology to Annex A of its Examination Handbook for Patent and Utility Model. On page 8-27, one can find several concrete examples regarding the application of the disclosure requirements to AI-related inventions. The main takeaways for the disclosure requirement are that, when filing AI patent applications in Japan, one should disclose a “certain relation, such as a correlation among the among the multiple types of data in the description or in view of the common general technical knowledge” which the AI-invention might make. It also requires for certain AI-inventions disclosure of test results or other proof of validation of the model is required “unless an estimation result by AI can be a substitution for an evaluation on a product that has actually been made”. See: JPO, *Patent Examination Case Examples pertinent to AI-related technologies*, p. 1, 4, 8-27, available at https://www.jpo.go.jp/e/system/laws/rule/guideline/patent/ai_jirei_e.html;

⁵⁸ See also in this sense: J. ALLAN e.a., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, Luxembourg, Publications Office of the European Union, 2020, p. 113 and 120.

⁵⁹ X., *Report from the IP5 Expert round table on artificial intelligence*, Munich, 31 October 2018, p. 3, par. 11, available at https://www.fiveipoffices.org/material/ai_roundtable_2018_report/ai_roundtable_2018_report. Nonetheless, applicants will still need to ensure that the claims are accurate and supported by a clear description.

⁶⁰ See e.g. B. HIGGINS, “The Role of Explainable Artificial Intelligence in Patent Law”, o.c., p. 1-6; A. WELLER, “Transparency: Motivations and Challenges” in W. SAMEK et al. (eds), *Explainable AI: Interpreting, Explaining and Visualizing Deep Learning*, Cham, Springer International Publishing, 2019, p. 23-40.

⁶¹ Standing Committee on the Law of Patents, *Background document on patents and emerging technologies*, Geneva, WIPO, 2019, p. 18, §72.

⁶² H. READ, “Artificial intelligence and machine learning: sufficiency and plausibility”, 12 June 2019, available at <https://www.appleyardlees.com/artificial-intelligence-and-machine-learning-sufficiency-and-plausibility/>. This author represents, so far, a minority position. See also: S. JONES, “Patentability of AI and machine learning at the EPO”, *Kluwer Patent Blog*, 21 December 2018, available at <http://patentblog.kluweriplaw.com/2018/12/21/patentability-of-ai-and-machine-learning-at-the-epo/>.

⁶³ See also in this sense: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 113 and 120.

⁶⁴ President of the EPO, *Update of legal aspects of artificial intelligence and patents*, Munich, EPO, 23 October 2020, §34.

The above questions relating to the patentability of AI-related innovation remain quite contentious.⁶⁵ As a result, it is often difficult to predict the outcome of the patenting process in a particular case, while also the direction patent offices should take remains debated. In general, it can therefore be concluded with regard to patent law that the EPC will enable patent protection for the technical developments underlying AI and machine learning and that existing law is sufficient.⁶⁶ Obviously, the applicable requirements need further clarification which will take time and case law in order to be further developed (e.g. T 161/06 and the upcoming decision in G 1/19).⁶⁷ This should not be surprising as AI-technology itself is also still developing.⁶⁸ If the EPO case law does not provide the necessary clarifications in due time, there may be a need for legislative intervention, whereby a harmonised solution at the international level is preferable.⁶⁹

2.1.3. Conclusions

Taking into account the above, one can discern that both copyright and patent law offer intellectual property protection for AI-related technology. On the one hand, copyright offers a relatively clear avenue for protection of the source code, object code and GUI of AI-software. On the other hand, the patentability of AI-systems under the regime of computer-implemented inventions is less clear, due to the exclusion of mathematical methods as patentable matter. Stakeholders are urging the EPO to provide more guidance in this regard, which could be useful in order to warrant a harmonised solution. It may, however, be good policy to wait for patent cases to emerge to identify additional issues that require a regulatory response, whereby the requisite technical character of an invention should be maintained.

2.2. IP-Protection for Data

In general, AI-systems require a substantial amount of data in their training and operational phase. These data may be subject to third-party rights, and AI-developers may therefore need to acquire (contractual) permission to access and use those data. Moreover, and in order to ensure data adequacy and data quality, AI-developers often clean and annotate the original datasets. These activities themselves may give rise to new rights. Cleaned or annotated data may indeed be a valuable resource for future users of the same or a different AI-system.⁷⁰ In this part, we will therefore discuss how 'data' can be protected. Exceptions in relation to text and data mining will be discussed later in the context of possible copyright infringement by AI-systems.

⁶⁵ Moreover, in a situation where binding ethical guidelines in relation to AI would have been adopted, one can ask the question whether "non-ethical" AI should be excluded from patentability under Article 53(a) of the EPC? This article specifies that "European patents shall not be granted in respect of inventions the commercial exploitation of which would be contrary to "ordre public" or morality; such exploitation shall not be deemed to be so contrary merely because it is prohibited by law or regulation in some or all of the Contracting States".

⁶⁶ A. SANDYS, "Patentable or not? Regulating AI inventions for a digital future", *JUVE Patent* 24 July 2020, <https://www.juve-patent.com/news-and-stories/legal-commentary/patentable-or-not-regulating-ai-inventions-for-a-digital-future/>; O. BALDUS, "A Practical Guide on How to Patent Artificial Intelligence (AI) Inventions and Computer Programs within the German and European Patent System: Much Ado about Little", *EIPR* 2019, 41, no. 12, p. 750-754.

⁶⁷ Taking into account the rapidly increasing number of patent applications related to AI-inventions, additional guidance stemming from EPO case law can be expected in the coming years. See e.g. X., *WIPO Technology Trends 2019 – Artificial Intelligence*, Geneva, WIPO, 2019, p. 13-15

⁶⁸ Standing Committee on the Law of Patents, *Background document on patents and emerging technologies*, Geneva, WIPO, 2019, p. 16, §62.

⁶⁹ See in this sense e.g. European Parliament Resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics, 2018/2088(INI), para. 136; European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL), para. 18. See also: A. SANDYS, "Patentable or not? Regulating AI inventions for a digital future", *JUVE Patent* 24 July 2020, available at <https://www.juve-patent.com/news-and-stories/legal-commentary/patentable-or-not-regulating-ai-inventions-for-a-digital-future/>

⁷⁰ M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 9.

2.2.1. Definition of Data(base)

Before discussing two possible avenues of legal protection for data, it is important to consider what is understood by 'data'. Data and information are often used interchangeably, while they are, strictly speaking, not synonyms (see also *infra*). Data can be combined to form or contains information and the following classification, provided by SWINNEN who was inspired by ZECH, may prove to be illustrative of how different categories of 'information' may all fall under a common denominator of 'data'.⁷¹

- Semantic information: this notion refers to the content of information, i.e. the information *per se*, that what can be deduced from data, actual or potential knowledge regarding an individual or other objects.
 - o Semantic information is currently not protected under (intellectual) property law as it does constitute a 'good' under Belgian property law, due to the fact that information *per se* / mere data cannot be exclusively controlled.⁷² Moreover, information *per se*/mere data should not be the object of (intellectual) property which would be socially undesirable and contrary to the freedom of information.⁷³
- Syntactic information: this notion refers to information that has been represented by a certain amount of symbols, signs, numbers, letters or code. In other words, information that has been formalized in a certain way (e.g. text or source code). Digitalised data are an example of syntactic information.
 - o Whether or not syntactic information can be the object of property rights, can be discussed, but it is currently generally accepted that e.g. digital data as such cannot be 'owned' under current Belgian property law.⁷⁴ Such information can however be protected through intellectual property rights and the data subject rights under the GDPR.⁷⁵ The extent of such protection is limited as in those cases the information needs either to meet the validity requirements for IP protection (e.g. originality or novelty/inventive step/..., see *infra*) or needs to be personal data. Especially machine-generated data will usually not be able to fulfil these requirements. The only options for protection of such data are the database *sui generis* right or trade secret protection. These will be further discussed below.
- Structural information: this notions refers to information contained in a certain physical carrier or in a wider sense information represented by the structure of a physical object. In other words, information that has been incorporated into a certain physical carrier or object. The information can be external to the carrier (e.g. the text contained in a book or the digital data

⁷¹ See H. ZECH, "Information as Property", *JIPITEC* 2015, p. 192-197; K. SWINNEN, "Eigendom van data? Reculer pour mieux sauter", *TPR* 2019, p. 73-75 en 87-91.

⁷² F. DE VISSCHER et al., "Rights in Data", *ICIP - Ing. Cons.* 2020, p. 361-363 and 367.

⁷³ SWINNEN and ZECH argue nonetheless that semantic information regarding the technical functioning of an object can be protected through patents. This argument should however be nuanced as a patent does not reserve the technical knowledge which emanates from it for its owner, but the *application* of such knowledge. On the contrary, in order to obtain a patent, a patent applicant needs to disclose the invention "sufficiently clear and complete for it to be carried out by a person skilled in the art". In other words, patent law exactly imposes on patentees to actively share the technical knowledge included in their invention, i.e. the relevant semantic information for this discussion, in order to enable further technological progress (e.g. through workarounds). Patents do hence, at most, protect indirectly technical semantic information then contain.

⁷⁴ This may, however, change in the future as Art. 3.55 of the new Belgian Civil Code defines 'goods' as 'all objects which can be appropriated, including property rights', whereby article 3.54 stipulates that goods can both be tangible and intangible (e.g. digital data). See also: F. DE VISSCHER e.a., "Rights in Data", *o.c.*, p. 364.

⁷⁵ F. DE VISSCHER et al., "Rights in Data", *o.c.*, p. 365 and 367.

on a data carrier (e.g. a USB-stick) or 'internal' (e.g. the information that a book has 100 pages stems from the structural fact that it has 100 pages).

- Structural information is currently legally protected through ownership. Someone can 'own' a book or a data carrier and can enforce the related rights. Furthermore, such physical carriers (and the digital data they contain) may also be protected under various intellectual property regimes, assuming the validity requirements are fulfilled.

In this context it is also interesting to take a closer look at the definition of database in the Database Directive.⁷⁶ Article 1 §2 defines database as meaning "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (see also Article I.13,6° CEL) In the context of this report, we would like to focus on two elements of this definition; (i) the requirement that it consists of works, data or other materials, and; (ii) the requirement that it is arranged in a systematic or methodical way.

A database should contain 'works, data or other materials'. The explanatory memorandum of the database-directive (arguably) seems to imply that these terms should be interpreted broadly by stating that the content of a database can be "information in the widest sense of that term".⁷⁷ This seems to be corroborated by case law from various European countries which accepts that a wide variety of information products is covered by the definition.⁷⁸ In addition, 'data' and 'other materials' do not have to be protected by copyright themselves (e.g. some official public documents).⁷⁹ Hence, a collection of materials in the public domain can possibly constitute a database.⁸⁰

The term works is understood to refer to copyrightable works.⁸¹

The term 'data' has not yet been defined by the CJEU. The only (and implicit) guidance the CJEU gave on this term is that the nature of the data is not relevant.⁸² Authors understand this rather vague term as to include any data (or information) that is understandable to humans.⁸³ BYGRAVE points out that *data* in everyday discourse is used as a synonym for *information*, but (that e.g. in the field of informatics the two are not considered synonyms (see supra).⁸⁴ In his well-written article, BYGRAVE e.g. refers to the definition of data by the International Organisation for Standardization (ISO): "a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means". This definition makes clear that the term 'data' has a representational function and should be

⁷⁶ Directive 96/9/EC of the European parliament and of the council of 11 March 1996 on the legal protection of databases, OJ L 77/20, 27 March 1996

⁷⁷ E. DERCLAYE, "What is a Database? A Critical Analysis of the definition of a database in the European Database Directive and suggestions for an international definition", *JWIP* 2002, p. 999; P.B. HUGENHOLTZ, "Database directive-commentary" in T. DREIER and P.B. HUGENHOLTZ (ed.), *Concise European Copyright Law*, Alphen aan den Rijn, Wolters Kluwer, 2016, p. 390. Both authors refer to the explanatory memorandum but I didn't succeed to find it online.

⁷⁸ See for a long list of examples: E. DERCLAYE, "Intellectual property rights on information and market power-comparing European and American protection of databases", *IIC* 2007, p. 283 (e.g. lists of financial data, as confirmed by French case law: DC Com Nanterre, 16 May 2000, *PR Line v. Newsinvest*, *JCP E* 2002, 223); P.B. HUGENHOLTZ, "Database directive-commentary", o.c., p. 390.

⁷⁹ *Ibid.*, p. 389 Regarding databases containing official public documents: the CJEU specifically confirmed that they can be a protected database in the *Apis-Hristovich*-case: CJEU 5 maart 2009, no. C-545/07, ECLI:EU:C:2009:132, *Apis-Hristovich v. Lakorda*, §69-72.

⁸⁰ I. STAMATOUDI and P. TORREMANS, *EU Copyright law: a commentary*, Cheltenham, Edward Elgar, 2014, p. 302.

⁸¹ E. DERCLAYE, "What is a Database? A Critical Analysis of the definition of a database in the European Database Directive and suggestions for an international definition", *JWIP* 2002, p. 989-990.

⁸² CJEU 9 November 2004, C-444/02, ECLI:EU:C:2004:697, *Fixtures v. OPAP*, §23 (*a fortiori*).

⁸³ I. STAMATOUDI and P. TORREMANS, *EU Copyright law: a commentary*, o.c., p. 302.

⁸⁴ L. BYGRAVE, "The data difficulty in database protection", *EIPR* 2013, p. 26-27.

distinguished from what it signifies. Data are something artificial, but intelligible. They communicate information. Or as DERCLAYE states: “Once deciphered by an individual, data become information to that individual.”⁸⁵

It thus remains to be seen how (and if ever) the CJEU will define this term. BYGRAVE argues that, keeping in mind the functional interpretation applied by the CJEU, it will probably choose for an ISO-definition oriented interpretation.⁸⁶ One can however disagree with this position as ‘formalised information’ can hardly be the only envisaged subject-matter of protection. Moreover, restricting the meaning of the word ‘data’ to its informatics-meaning is precisely at odds with the functional interpretation. The CJEU regards a database as a system with a function of *information storage and processing*.⁸⁷ This then leads to the suggestion that the CJEU (implicitly) already chose to understand data as used in everyday discourse and not in a technical understanding. This can, furthermore, be corroborated by the fact that the recitals are drafted in such a way that information and data seem to have been used as synonyms or at least, that it is not clear that a strict distinction has been applied or that there was an intention to do so (see e.g. recital 10 & 12 vs. recital 21 Database Directive).⁸⁸ Nonetheless, this remains a topic of discussion.⁸⁹

The term ‘other materials’ is understood to include things which are not works or data: e.g. sound recordings or non-original photographs that could be protected by neighbouring rights.⁹⁰ Apart from those things, this term can virtually encompass everything.⁹¹

These elements of a database should be *arranged in a systematic and methodical way*. Recital 21 of the Database Directive adds that it is not necessary for the materials to be physically stored in an organized manner, while the explanatory memorandum excludes the “mere stockage of quantities of works or materials in electronic form”. The CJEU further clarified that the methodical arrangement-requirement implies that “the collection [...] includes technical means such as electronic, electromagnetic or electro-optical processes, [reference to rec. 13 Database Directive], or other means, such as an index, a table of contents, or a particular plan or method of classification, to allow the retrieval of any independent material contained within it”.⁹² So far, this requirement has not been much debated.⁹³ Some further useful insight is provided by DERCLAYE who enumerates what shouldn’t be considered ‘a systematic or methodical arrangement’, according to her. First, she suggests to exclude strictly personal arrangements. On the contrary, the arrangement should (at least) be understandable by other people with skill in the art, related to a particular database. Second, she suggests to exclude ‘haphazard collections’. This was also

⁸⁵ E. DERCLAYE, “What is a Database? A Critical Analysis of the definition of a database in the European Database Directive and suggestions for an international definition”, o.c., p. 1004.

⁸⁶ L. BYGRAVE, “The data difficulty in database protection”, o.c., p. 31.

⁸⁷ CJEU 9 November 2004, C-444/02, ECLI:EU:C:2004:697, *Fixtures v. OPAP*, §27-28.

⁸⁸ Just to indicate that the word ‘data’ is not uniformly used in international legal documents, the additional examples of the General Data Protection Regulation (GDPR) and the Cybercrime Convention (CC) (Council of Europe) are given. The GDPR seems to choose to use data and information as synonyms; see. e.g. art. 4.1 GDPR: “Personal *data* means any *information*...” whereas the CC explicitly refers to the ISO-definition. In the Explanatory Report to the CC, one can read “the definition of computer data builds upon the ISO-definition of data...” See: Explanatory report to the Convention on Cybercrime (Council of Europe), 23 November 2001, ETS 185, p. 5.

⁸⁹ K. SWINNEN, “Eigendom van data? Reculer pour mieux sauter”, o.c., p. 90; R. FISHER et al., *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases – Annex 1: In-depth analysis of the Database Directive, article by article*, European Union, 2018, p. 65.

⁹⁰ P.B. HUGENHOLTZ, “Database directive-commentary”, o.c., p. 389.

⁹¹ I. STAMATOUDI and P. TORREMANS, *EU Copyright law: a commentary*, o.c., p. 302; A. QUAEDVLIEG, “Onafhankelijk, geordend en toegankelijk: het object van het databankenrechten in de richtlijn”, *Informaticarecht/AMI* 2000, p. 177-179.

⁹² CJEU 9 November 2004, C-444/02, ECLI:EU:C:2004:697, *Fixtures v. OPAP*, §30.

⁹³ Some doctrine even contents itself by only requiring that the arrangement shows any kind of ‘organisation’ or that some objective standards have been used. See M.M.M. VAN EECHOU, “De ontsporing van het begrip databank. Enige bedenkingen bij HVJEU Freistaat Beieren/Verlag Esterbauer”, *Informaticarecht/AMI*, p. 26, (further references in footnote 7). Note that a requirement of using ‘objective standards’ can be at odds with the requirement of an ‘original’ arrangement for copyright protection. A chronological arrangement can hardly be considered original.

suggested by Advocate-General STIX-HACKL in her conclusion to the *Fixtures v. OPAP*-case where she suggested to “exclude random accumulations of data and ensure that only planned collections of data are covered, that is to say, data organised according to specific criteria.”⁹⁴ Third, DERCLAYE addresses the relation with the originality-requirement (see *infra*). While a database arranged in a very personal manner (e.g. based on preference and taste) might well be original, it will probably fail to be arranged systematically.⁹⁵ Taking into account all of the above, it is remarkable to note that BUYERS argues that “it is improbable that such [training] datasets would reach the level of organisation equivalent to a classically ordered database”.⁹⁶ After all such (training) dataset will likely surpass the threshold of ‘mere stockage’, while often being organised in such way to achieve optimal training results, abstaining from being a strictly personal arrangement or haphazard collection.⁹⁷

To conclude, it is very important to be precise about what one understands by ‘data’ as different concepts will lead to different possible types of protection. If data is used as a broad concept, possibly encompassing works, trademarks, designs,..., those respective protective regimes can apply to those ‘data’. Should data, however, be used in a more strict meaning, limited to ‘raw’ data, there is no legal protection available except via database rights or trade secret protection (i.e. contractual limitations).⁹⁸

2.2.2. Database Protection

As mentioned above, Belgian (intellectual) property law does not provide a legal or statutory title for ownership of data ‘as such’.⁹⁹ At most, curated data libraries could become protected, under certain circumstances, by the database copyright or *sui generis* right.¹⁰⁰

A database can enjoy copyright protection if it constitutes the author's own intellectual creation by reason of the selection or arrangement of their contents (Article 3 §1 Database Directive, Article XI.186 CEL). Such copyright protection does not extend to the contents of such database and should not interfere with any rights subsisting in the contents themselves (e.g. copyright) (Article 3, §2 Database Directive, Article XI.306 CEL).¹⁰¹ The latter implies that, for instance, works or trademarks included in a database will continue to be protected by copyright, neighbouring rights or, respectively, trademark law.¹⁰²

⁹⁴ Opinion of the Advocate General STIX-HACKL in case C-444/02, 8 June 2004, ECLI:EU:C:2004:339, §40.

⁹⁵ However, depending on the circumstances at hand, such a database might be arranged systematically. See: E. DERCLAYE, “What is a Database? A Critical Analysis of the definition of a database in the European Database Directive and suggestions for an international definition”, *o.c.*, p. 991-994; J. JENKINS, “Database rights’ subsistence: under starter’s orders”, *JiPLP* 2006, 470, footnote 129.

⁹⁶ J. BUYERS, *Artificial Intelligence – The Practical Legal Issues*, Somerset, Law Brief Publishing, 2018.

⁹⁷ This statement is even more remarkable taking into account the position of a renowned scholar as HUGENHOLTZ who, oppositely, argues that even unsorted data on a hard disk would still qualify as a database if combined with database management software that enables the retrieval of specific stored data: P.B. HUGENHOLTZ, “Database directive-commentary”, *o.c.*, p. 390.

⁹⁸ K. SWINNEN, “Eigendom van data? Reculer pour mieux sauter”, *o.c.*, p. 69; M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, *o.c.*, p. 10; T. MARGONI, “Artificial Intelligence, Machine learning and EU copyright law: Who owns AI?”, *Create Working Paper Series* 2018, p. 8, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299523.

⁹⁹ K. SWINNEN, “Eigendom van data? Reculer pour mieux sauter”, *o.c.*, p. 68.

¹⁰⁰ Art. 3 and 7 Database Directive.

¹⁰¹ See also Art. 10, §2 TRIPS Agreement: “Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself”

¹⁰² T. MARGONI, “Artificial Intelligence, Machine learning and EU copyright law: Who owns AI?”, *o.c.*, p. 8.

The scope of the copyright-protection is limited to the structure of the database (see Recital 15 Database Directive).¹⁰³ Article 3, §1 Database Directive (Article XI.18 CEL) thus actually requires that the structure of the database is ‘the author’s own intellectual creation’ by ‘reason of the selection or arrangement of the contents’. Whether the structure can be considered as *the author’s own intellectual creation* depends on whether the originality-threshold, as developed by the CJEU, is met. In the *Football Dataco I*-case, the CJEU stated that a database enjoys copyright protection when the selection or arrangements of the contents amounts to an original expression of the creative freedom of its author. This means that the author should have expressed his creative ability by making free and creative choices, reflecting his “personal touch”.¹⁰⁴

Such original expression should happen through the *selection or arrangement* of the contents of the database. In other words, the creative and personal expression should be found in:

- Either the *selection*: the choosing of the contents of the database, the editing thereof.
- or the *arrangement*: the decision on how to present or structure the contents of a database.¹⁰⁵

Note that neither selection nor arrangement implies the creation of data. Hence, creation falls outside the scope of the database copyright-protection. This has also been explicitly denied by the CJEU by referring to the goal of the directive, which is to stimulate the production of databases, not to stimulate the creation of data (see also Recitals 9, 10 & 12 Database Directive).¹⁰⁶ Hence, any originality expressed through the creation of the data is irrelevant in this regard.¹⁰⁷

HUGENHOLTZ points out that “... an arrangement of data based on objective criteria, such as alphabetical ordering [is not creative]”.¹⁰⁸ Hence, the structure itself of a database should demonstrate a subjective choice.¹⁰⁹ In its *Football Dataco I*-ruling the CJEU also provided some further useful guidance by adding in paragraph 39 that “that criterion [of originality] is not satisfied when the setting up of the database is dictated by technical considerations, rules or constraints which leave no room for creative freedom”.¹¹⁰ At the same time, it is reiterated that this has to be balanced with the “systematic and methodical arrangement”-requirement from the database-definition (*supra*).

In an AI-context, it can be imagined that the database copyright protection will generally not be of great relevance, as the selection of data in (training) data sets is often determined by technical or functional prerequisites, leaving not much space for subjective creativity.

¹⁰³ G. VANDERSTICHELE, “Het oorspronkelijkheids criterium in het auteursrecht op databanken” (annotation of CJEU, 1 March 2012, C-604/10 *Football Dataco and others v. Yahoo UK*), *IRDI* 2013, p. 91; I. STAMATOUDI and P. TORREMANS, *EU Copyright law: a commentary*, o.c., p. 308.

¹⁰⁴ CJEU 1 March 2012, C-604/10, ECLI:EU:C:2012:115, *Football Dataco and others v. Yahoo UK*, §37-38 and §45. It thus confirmed (and explicitly referred to) its earlier jurisprudence on the originality-threshold in copyright. This interpretation has been criticised by some authors for lacking a clear legal basis: F. BRISON, M.-C. JANSSENS, P. MAEYAERT and H. VANHEES, “Evoluties binnen het recht van de intellectuele eigendom (2009-2010)”, *IRDI* 2011, p. 176. Their criticism has, however, been refuted persuasively by G. VANDERSTICHELE, “Het oorspronkelijkheids criterium in het auteursrecht op databanken”, o.c., p. 90-96.

¹⁰⁵ G. GLAS, “Kanttekeningen: Originaliteit, niets meer en niets minder”, *IRDI* 2012, 3; G. VANDERSTICHELE, “Het oorspronkelijkheids criterium in het auteursrecht op databanken”, o.c., p. 91.

¹⁰⁶ CJEU 1 March 2012, C-604/10, ECLI:EU:C:2012:115, *Football Dataco and others v. Yahoo UK* §32-36; E. DERCLAYE, “Database rights: success or failure? The chequered yet exciting journey of database protection in Europe” in C. GEIGER, *Constructing European Intellectual Property: achievements and new perspectives*, Cheltenham, Edward Elgar Publishing, 2013, p. 349-350.

¹⁰⁷ I. STAMATOUDI and P. TORREMANS, *EU Copyright law: a commentary*, o.c., p. 309.

¹⁰⁸ P.B. HUGENHOLTZ, “Database directive-commentary”, o.c., p. 393. He also gives an example: a list of someone’s *favourite* (subjective) restaurants may be eligible for copyright protection, but not a list of the most *expensive* (objective) ones.

¹⁰⁹ Vice versa, the possible originality (or the lack thereof) in the contents is irrelevant in this context. See: CJEU 1 March 2012, C-604/10, ECLI:EU:C:2012:115, *Football Dataco and others v. Yahoo UK*, §30-32.

¹¹⁰ CJEU 1 March 2012, C-604/10, ECLI:EU:C:2012:115, *Football Dataco and others v. Yahoo UK* §39.

The database sui generis-right accrues to the maker of the database and is triggered when a qualitatively and/or quantitatively substantial investment has been made in obtaining, verifying or presenting the contents of a database (Article 7 Database directive; Article XI.306 CEL).¹¹¹ In summary, even databases of unprotected facts could become the object of a proprietary right that extends to the database contents insofar the aforementioned (de minimis) substantial investment can be proven.¹¹²

Firstly, and with regard to the obtaining of the contents, this means that the investment should be aimed at obtaining data, i.e. seeking out existing independent materials and collecting them in the database, not creating them. A (near-)simultaneous addition of newly created data is, however, eligible for protection if a separate investment can be proven. Next to that, the majority of the doctrine considers that the recording of (pre-existing) facts can be understood as ‘obtaining’ of the contents. Secondly, investments in verification of the contents should be investments in the objective, non-discretionary checking, correcting or updating of the information to be or already included in a database. Also considered relevant are situations where the creation and verification of data are inseparable, as long as the respective investments are separable.¹¹³ Finally, investments in the presentation of contents are understood as investments in making the contents individually accessible (e.g. establishing processes to enable the localisation of content) and/or arrange them systematically or methodically.¹¹⁴ Also here, as it also goes for obtaining and verification, if the investment in presenting the contents is inseparable from investment in the creation of the materials, the right cannot be established.¹¹⁵ If they are separable, sui generis-protection could arise.^{116 117}

Hence, if cleaned or annotated data take the form of a database, and the making of this database entailed a substantial investment (either in financial or human resources, for example), the cleaned or annotated dataset could be subject to the sui generis-right. Although the sui generis-right does not enter into play when an investment is made in the creation of data, it could be argued that in the specific case of cleaned or annotated datasets it can be considered that the investment is not made in the creation but rather in the verification or presentation of the data.¹¹⁸ Similarly, it is currently understood that (sole source) collections of machine/sensor-generated data fall outside of the scope of database protection as the relevant investment will often have been directed towards the creation, rather than the obtaining of the data.¹¹⁹

In principle, when data(bases) are protected by the database copyright or the sui generis-right, any temporary or permanent reproduction of these data or, respectively, the extraction and/or reuse of a substantial part of the data contained in a protected database would need the authorisation

¹¹¹ The maker of the database is being defined as the natural or legal person who takes the initiative and the risk of investing in the database (Art.XI.1.17, 2°CEL). This rules out sui-generis protection for databases entirely generated by AI-systems, without any investment of human origin.

¹¹² T. MARGONI, “Artificial Intelligence, Machine learning and EU copyright law: Who owns AI?”, o.c., p. 8.

¹¹³ E.g.: CJEU, 9 November 2004, C-338/02, ECLI:EU:C:2004:696, *Fixtures Marketing v. Svenska Spel*, §50 (a contrario), See: J. JENKINS, “Database rights’ subsistence: under starter’s orders”, *JIPLP* 2006, p. 475-476 & 479.

¹¹⁴ J. JENKINS, “Database rights’ subsistence: under starter’s orders”, o.c., p. 476 & 480.

¹¹⁵ A. MASSON, “Creation of Database or Creation of data: Crucial choices in the matter of database protection”, *EBLR* 2006, p. 1072; E. DERCLAYE, “Intellectual property rights on information and market power-comparing European and American protection of databases”, o.c., p. 285.

¹¹⁶ J. JENKINS, “Database rights’ subsistence: under starter’s orders”, o.c., p. 476-477 & 479.

¹¹⁷ For a further discussion and additional sources: T. GILS, *Blockchain and law: an analysis of blockchain technology under the database directive 96/9*, KULeuven, 2017, p. 34-43, available at <https://papers.ssrn.com/abstract=3737360>

¹¹⁸ M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, Luxembourg, Publications Office of the European Union, 2020, 9

¹¹⁹ K. SWINNEN, “Eigendom van data? Reculer pour mieux sauter”, o.c., p. 90 ; R. FISHER et al., *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases*, European Union, 2018, p. vi-vii, 20-22, 30,110-115; M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 10, footnote 30.

of the rightholder (Article XI.307 CEL, unless an exception applies (see *infra* for text and data mining exception).

In cases where cleaned and annotated datasets incorporate individual works (e.g. pictures deserving copyright protection) or other protected subject-matter (substantial part of a database deserving *sui generis* protection), it will depend on the specific case whether the cleaned or annotated dataset (or even the trained system) is considered as a derivative work/subject-matter.¹²⁰ In cases where individual works or other protected subject-matter are not *per se* reproduced (i.e. where only information about those is included), one could in principle conclude that the final results should not be considered as a derivative work.

2.2.3. Trade Secret/Contractual Protection¹²¹

Where a collection of (cleaned or annotated) data does not reach the (*de minimis*-) investment threshold under the Database-directive (see *supra*), AI-developers will probably rely on trade secrets to protect their investments.¹²²

According to Article I.17/1, 1° CEL, a trade secret means “information that meets all the following requirements:

- it is secret in the sense that it is not, as a whole or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the communities usually dealing with the type of information in question;
- it has commercial value because it is secret;
- it has been subject to reasonable steps by the person lawfully in control of the information to keep it secret, taking into account the relevant circumstances”.

In view of this definition, it is accepted that any type of information can be protected as a trade secret,¹²³ regardless of its object and/or nature (technical, commercial, organisational, etc.), how it has been expressed (oral, written, etc.) and/or its medium (paper, digital, etc.). Thus, mere data may, in principle, be protected as a trade secret provided that it meets the conditions set out by law.

As one could expect, the secrecy-requirement of the relevant data is essential and must be established for as long as the holder intends to benefit from trade secret protection. The data must not only be confidential (i.e. not generally known or easily accessible) from the outset, but it must also remain so in time, in particular through the “reasonable steps” taken by the holder to that effect. Such “reasonable steps” can be contractual (e.g. contracts concluded with any person likely to come into possession/have knowledge of the trade secret), digital (e.g. encryption measures, password, etc.) and/or physical (e.g. expressly identifying information as confidential, storing it in restricted areas, training staff, adopting specific measures to control the entry/exit of visitors, etc.). As soon as the data become public, it automatically loses its trade secret status and, therefore, will no longer be protected as such.

Furthermore, the condition of the commercial value of the trade secret – whether actual or potential – is also essential. Any data can indeed only be protected as a trade secret if it (is likely to) give(s) the holder a substantial advantage likely to improve its competitive position.¹²⁴ This

¹²⁰ See also; T. MARGONI, “Artificial Intelligence, Machine learning and EU copyright law: Who owns AI?”, *o.c.*, p. 8-15.

¹²¹ This part is based on F. DE VISSCHER et al., “Rights in Data”, *o.c.*, p. 373-378.

¹²² Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *OJ L 157*.

¹²³ See Recital 14 of Directive 2016/943: “It is important to establish a homogenous definition of a trade secret without restricting the subject matter to be protected against misappropriation”

¹²⁴ H. VANHEES, “De nieuwe wettelijke regeling betreffende de bescherming van bedrijfsgeheimen”, *RW 2018-2019*, p. 1644-1645.

excludes trivial, current, generally-known information and/or information acquired in the normal course of business. The threshold of the value necessary for any data to qualify as a trade secret will obviously vary according to the sector of activity, the holder's financial capabilities or position on the market, etc. In other words where the unlawful acquisition, use or disclosure of data is likely to harm the interests of the organisation lawfully controlling it, meaning that it undermines that organisation's scientific or technical potential, business or financial interests, strategic positions or ability to compete, such data should be considered to have commercial value.

If applicable, data which are protected by trade secret, will be protected for as long as they are secret (which can be very long). Moreover, it should be highlighted that the rights a trade secret holder has, are negative rights. This means that a trade secret holder can only oppose the unlawful acquisition, use and/or disclosure of its trade secrets (see Article XI.332/2-4 CEL, including exceptions which allow certain uses of trade secrets, even without the trade secret holder's consent).

In practice this means that parties will, in the majority of cases, rely on contracts to regulate access, use and reuse of compilations of (cleaned and/or annotated) datasets or trained models.¹²⁵ Parties can in principle freely deal with mere data and establish some form of 'de facto' ownership of data or a set of data related rights. These contracts are subject to general contract law and need to comply with mandatory rules and rules of public order, if applicable.

2.2.4. Conclusion

Data can be protected in a number of ways. Especially when understood broadly, it cannot be excluded that data may be protected by e.g. copyright. When interpreted more strictly, data(bases) may be protected via the sui generis database right or via trade secrets (i.e. via contractual limitations). In the course of our research, we have not found any indications showing that there would be a genuine need to increase the number of possible protection mechanisms for data. On the contrary, scholars seem to agree that the existing toolkit of trade secret protection, contract and technological protection measures offers data producers ample means of securing de jure or de facto exclusivity.¹²⁶

3. The Applicability of Intellectual Property Regimes on AI-Output

As has been widely reported in the media, AI is being used to generate a diverse range of 'output'.¹²⁷ Recent advances in AI techniques have allowed machines to reach a level of autonomy that could make the human contribution trivial to the creative or inventive process. We may consequently be entering into an era where machines will not only *assist* humans in the creative process but *create or invent* all by themselves. The application of intellectual property regimes to the outputs assisted or generated by AI is a complex question, in particular for: copyright (part 3.1.), other sui generis or neighbouring rights (part 3.2.) and patent law (part 3.3.). Trademark/design law poses less of a challenge and will briefly be discussed (part 3.4.). We will

¹²⁵ M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 9.

¹²⁶ AIPPI, "Resolution on IP Rights in data", 14 October 2020, p. 2 ("Without prejudice to existing rights, mere data should not be eligible for protection by a new specific IP right such as a new sui generis right"); B. HUGENHOLTZ, 'Against Data Property' in H. ULLRICH, P. DRAHOS, & G. GHIDINI (Ed.), *Kritika: Essays on Intellectual Property* (Vol. 3), Cheltenham, Edward Elgar, 2018, p. 48-71; J. DREXL, "Designing Competitive Markets for Industrial Data – Between Propertization and Access", *JIPITEC* 2017, p. 257-292. *A contrario*, see C. DUCUING, "'Data rights in co-generated data': The ground-breaking proposal under development at ELI and ALI", *CITIP Blog*, 5 November 2020, available at <https://www.law.kuleuven.be/citip/blog/data-rights-in-co-generated-data-part-1/>. This author discusses the Principles for the Data Economy currently under development at the European Law Institute and American Law Institute.

¹²⁷ For an overview, see: M. IGLESIAS, S. SHAMUILA and A. ANDERBERG, *Intellectual Property and Artificial Intelligence: A Literature Review*, o.c., p. 12.

also look into the ownership of AI-assisted/generated output (part 3.5.) and examine IP-infringements by AI-systems (part 3.6.).

As a preliminary remark, the following distinction is clarified. When the term “AI-assisted” is used, we refer to outputs that are the result of a process where humans employed AI-systems as a tool. Oppositely, when the term “AI-generated” is used, we refer to outputs that have been created, produced,... entirely by AI-systems without any significant human intervention. It is generally assumed that fully autonomous creation or invention by AI does not exist at this moment, and will not exist for the foreseeable future. AI-systems should therefore primarily be viewed as sophisticated tools in the hands of human operators.¹²⁸

3.1. Copyright

Certain AI-systems available today can create – or can be used as a technical aid to create – output that could satisfy the conditions for copyright protection (see *infra*) if they had been created entirely by humans.¹²⁹ A feature common to many of these outputs is that there is still human intervention (to some extent), be it by a programmer, by a person using or training the AI-system through data input or by somebody who modifies and/or selects certain specific output deemed ‘worthy’ to be disclosed to the public. If such human(s) were to have created the output at issue without the assistance of an AI-system, there would be little doubt that copyright protection would be available to them.

Indeed, such output (e.g. music, novels, paintings etc.) will likely fall within the ‘literary, scientific and artistic domain’ (Art. 2 Berne Convention)¹³⁰ and will often constitute an actual, concrete creation or expression of an idea, hence copyright could apply.¹³¹ However, given the intervention of AI in these (and other) cases, the matter is less straightforward.¹³² After all, Belgian copyright law, just as most copyright legislation across EU Member States, is very much dependent on human-centred concepts, for: (i) the conditions for protection (e.g. originality); (ii) the beneficiary of protection (i.e. authorship); and (iii) the rights granted (economic, but more specifically moral rights).¹³³ This human-centred focus is also present in the *acquis communautaire*, although arguably to lesser extent due to the lack of regulation on moral rights.

In the following paragraphs, we will first elaborate upon the conditions for protection (part 3.1.1.). Once this has been done, the study will discuss authorship/ownership of AI-assisted output (part 3.1.2.) as well as other restrictions under copyright (part 3.1.3.).

3.1.1. Condition for Protection: Originality

This anthropocentric approach also applies for the definition of originality. Although the concept of originality is not clearly defined in European law, several directives link originality to natural

¹²⁸ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 6, 78 and 116; See J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., §23 and §32.

¹²⁹ See J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., §18 for an extensive list of examples of such outputs and related sources. This chapter has also served as important source for this part.

¹³⁰ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p.78.

¹³¹ Cass. 17 February 2017, *IRDI* 2017, 135. For some background on the concept of ‘works’, we refer to O.

¹³² Interestingly, VANHERPE (*ibid.*) points out legal scholarship regarding the question of computer authorship already spans several decades. See e.g. K.F. Jr. MILDE, “Can a Computer Be an Author or an Inventor”, *J Pat Off Soc’y* 1969, p. 378-405; T.L. BUTLER, “Can a Computer Be an Author? Copyright Aspects of Artificial Intelligence”, *Comm/Ent L*, 1981, p. 707; P. SAMUELSON, “Allocating Ownership Rights in Computer-Generated Works”, *U Pitt L Rev* 1986, p. 1185-228; US Congress, Office of Technology Assessment, “Intellectual Property Rights in an Age of Electronics and Information”, April 1986.

¹³³ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 69.

persons or human attributes.¹³⁴ More importantly, both the Software and Database Directives (as well as the Term Directive in relation to photographs) refer to the ‘author’s own intellectual creation’ as the sole criterion to consider when assessing originality.¹³⁵

Most importantly, however, the interpretation of this criterion has been harmonised to a considerable degree by the case law of the CJEU, often later confirmed by the Belgian Court of Cassation. In summary, the condition of originality entails that a work needs to be an intellectual creation of its author(s) reflecting the personality of the author and expressing his/her free and creative choices in the production of the work.¹³⁶ By making certain choices, the author applies his “personal touch” to the work.¹³⁷ Under Belgian copyright law, the subjective component of the originality criterion (i.e. the author’s personality) is thus of paramount importance.¹³⁸ To sum up, these courts refer to the ‘authors’ intellectual creation’, ‘the free creative choices’, ‘the authors’ personality’, or ‘the author’s personal touch’ as requirements for the emergence of a copyright-protected work.¹³⁹ Interestingly, Advocate General TRSTENJAK affirmed explicitly in her opinion in the Painer-case (C-145/10) that “...only human creations are therefore protected, which can also include those for which the person employs a technical aid, such as a camera”. Also Advocate General SZPUNAR stated that “the origin of and justification for copyright, in the form of both moral and property rights, lies in the special relationship between the author and his work. Thus, where there is no author, there is no copyright, in the form of either moral or property rights”.¹⁴⁰

In recent articles and public presentations, European scholars have debated the possible protection of AI-generated output under current European and national legislation in the context of this humanist approach to copyright law. Most authors logically conclude that, under present law, AI-generated output will not be eligible for copyright protection.¹⁴¹ This is because output created solely by machines cannot be considered original in the sense of copyright law since they will lack the human attributes required by case law. AI-systems remain machines and cannot as

¹³⁴ For instance, the Resale Directive arguably points to *persons* (“artists”, Article 2 of Directive 2001/84/EC of the European Parliament and of the Council of 27 September 2001 on the resale right for the benefit of the author of an original work of art, OJ L 272) and the Copyright Term Directive points to *human attributes* (“personality”, 16 of Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version) OJ L 372).

¹³⁵ Art. 3 of the Database Directive, Article 1(3) of the Software Directive, and Article 6 of the Copyright Term Directive on photographs.

¹³⁶ CJEU, 16 July 2009, no. C-5/08, ECLI:EU:C:2009:465, *Infopaq/Danske Dagblades Forening*, §37-39 and §45.; CJEU 22 December 2010, no. C-393/09, ECLI:EU:C:2010:816, *BSA/Ministerstvo kultury*, §46; CJEU 23 January 2014, no. C-355/12, ECLI:EU:C:2014:25, *Nintendo/PC Box*, §21; CJEU 13 November 2018, no. C-310/17, ECLI:EU:C:2018:899, *Levola/Smilde*, §36-40. See also: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 69-75.

¹³⁷ CJEU 1 December 2011, no. C-145/10, ECLI:EU:C:2011:798, *Painer/Standard*, §92 and §99; Cass. 31 October 2013, RW 2013-2014, 1464; Cass. 17 March 2014, ICIP 201, no. 2, 251; 4; Cass. 14 December 2015, ICIP 2016, 193. The CJEU does not seem to require that the author’s creativity or personality (“personal stamp”) be objectively discernible in the resulting expression (the output). See: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 73-74.

¹³⁸ The objective component being that a certain minimum level of (human) intellectual work is required. See: F. GOTZEN and M.-C. JANSSENS, *Wegwijs in het intellectueel eigendomsrecht*, o.c., 37.

¹³⁹ Note that the actual required level of creativity is in practice low. See: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 74.

¹⁴⁰ Opinion AG SZPUNAR 25 October 2018, no. C-469/17, ECLI:EU:C:2018:870, *Funke Medien/Bundesrepublik Deutschland*, § 60.

¹⁴¹ For Belgium: B. MICHAUX et al., “Copyright in Artificially-Generated Works”, *ICIP* 2019, p. 224-225; F. GOTZEN and M.-C. JANSSENS, “Kunstatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie”, *A&M* 2019, p. 331-332; F. VEHAR and T. GILS, “I’m sorry AI, I’m afraid you can’t be author (for now)”, *JiPLP* 2020, vol. 15, no. 9, p. 720-721; J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., §21 and §23. See also: D. GERVAIS, “The Machine As Author”, *Iowa Law Review* 2019, vol. 105, p. 2062, 2098-2101; J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 70.

such develop a ‘personality’, which is a typical human attribute and which can then also not be reflected in its output.¹⁴²

On the other hand, these scholars also often indicate that AI-assisted output may well end up being protected as long as a human contributed decisively to the originality of the output in question, imprinting it with his/her ‘personal touch’ through free and creative choices.¹⁴³ In relation to such AI-assisted works, the most important question hence relates to the requisite degree of human intervention in order to be able to be eligible for copyright protection. Who would be the relevant human for this purpose, will be discussed in the next part. Furthermore, it is asserted that such AI-assisted output should enjoy the same modalities of protection (economic rights, moral rights, term of protection, exceptions and limitations and initial ownership) as applicable to purely human-generated output.¹⁴⁴

In the context of AI-assisted output, the relevant creative choices can occur at various levels and in various phases of the creative process: conception/preparation, execution, and redaction of the output.¹⁴⁵ Even creativity occurring solely at the conceptual or preparatory stage of a work might suffice for a finding of originality. This is in line with the Software Directive prescient inclusion of “preparatory design material” in the definition of a “computer programme”, which clarifies that computer-generated computer code will qualify as a copyright-protected computer programme if it is based on preparatory design work reflecting creative choices by a human author.¹⁴⁶ There must, however, always be an causal link between the author’s creative act (the exercising of their creative freedom) and the expression thereof in the form of the work produced. In summary, as long as the output reflects creative choices by a human being at any stage of the production process, an AI-assisted output is likely to qualify for copyright protection. This is true even if the AI-system has played a significant or even predominant role in the entire creative process.¹⁴⁷ ALLAN et al. further clarify that with regard to AI-assisted output relevant (creative) choices may be: design choices in the conception phase, some calibration choices in the execution phase, and the editing and post-production choices at the redaction phase.¹⁴⁸ Finally, it should be stressed, as evident from the above, that economic investment cannot, as such, justify copyright protection.¹⁴⁹

¹⁴² B. MICHAUX et al., “Copyright in Artificially-Generated Works”, o.c., p. 224; F. VEHAR and T. GILS, “I’m sorry AI, I’m afraid you can’t be author (for now)”, o.c., p. 721. This exclusion from copyright protection for AI-generated works may, however, lead one to reflect upon the very nature of (human) originality/creativity. See e.g. J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., §23.

¹⁴³ B. MICHAUX et al., “Copyright in Artificially-Generated Works”, o.c., p. 221-224; F. GOTZEN and M.-C. JANSSENS, “Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie”, o.c., p. 329-330. These authors include some references to (French) case law and existing jurisprudence to corroborate this point. Moreover, these authors also indicate that this debate (including the element of the relative unpredictability of computer creations) is actually a rather old one (going back to scholarly debates in Germany in the 1950s).

¹⁴⁴ AIPPI, “Resolution: Copyright in artificially generated works”, 2019, p. 3 available at https://www.aippi.dk/wp-content/uploads/2019/11/Resolution_Copyright_in_artificially_generated_works_English.pdf

¹⁴⁵ CJEU 1 December 2011, no. C-145/10, ECLI:EU:C:2011:798, *Painer/Standard*, §90-91; A. Q. RAMALHO, “Originality Redux: An Analysis of the Originality Requirement in AI-Generated Works”, *AIDA* 2019, p. 7.

¹⁴⁶ Art. 1(1), second sentence Software Directive. See recital 7 of the same directive: “Whereas, for the purpose of this Directive, the term ‘computer program’ shall include programs in any form, including those which are incorporated into hardware; whereas this term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage”.

¹⁴⁷ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 75-76. These authors introduce the new notion of *general authorial intent* in this context. This implies that it is sufficient that the author has a general conception of a work before it is expressed, while leaving room for unintended expressive features which will not break the creative link between author and output.

¹⁴⁸ See in detail: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 78-82.

¹⁴⁹ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 71.

3.1.2. Authorship/Ownership of AI-assisted Output

On European level, both the Software Directive and the Database Directive define authorship on the basis of the natural person(s) or group(s) of natural persons who created the work.¹⁵⁰

Authorship is primarily a matter of national law. Belgian copyright law, as opposed to copyright law in many other European jurisdictions, explicitly stipulates that the original copyright holder is 'the natural person who created the work' (Art. XI.170 CEL). This excludes the possibility that legal persons could be regarded as the original author, which also follows from the requirement of an 'intellectual' creation, which is something only physical persons can do.¹⁵¹ In addition, Art. XI.170 CEL clearly refers to a 'natural person', excluding all other kinds of virtual persons, including AI-systems.¹⁵² With regard to Belgium, this is an additional argument to exclude AI-generated output from copyright protection.

With regard to AI-assisted output, there are few human actors which may be eligible to claim copyright, insofar as they contributed decisively to the (originality of the) final work and their creative choices/personal touch is discernible in the output: e.g. the programmer of the AI-system, the user/operator, the owner,...¹⁵³ Below we will discuss some of these possibilities. We will also address this point more generally in part 3.5. Ownership of AI-Generated Output.

First of all, the programmer/owner of the copyrights in AI-software will not as such be entitled to the copyrights on the AI-assisted output.¹⁵⁴ Copyright protection should, however, not be excluded by default for the programmers who draw up functional specifications for an AI-system that are so detailed that the AI-system would in practice not have the possibility to change or turn away from its objective and the available means, so that the 'personal touch' of the programmer is reflected in the work generated by means of the AI-system.¹⁵⁵ The programmer should however be able to demonstrate that his/her specifications/instructions contributed directly to the final original result.¹⁵⁶ In the UK, AI-programmers can possibly enjoy (a sort of) copyright protection under the computer-generated works regime if they are "the person by whom the arrangements necessary for the creation of the work are undertaken".¹⁵⁷

For a user/operator of an AI-system, it is required that he/she contributes decisively to the originality of the work in question, by e.g. having set the parameters, improving or modifying the work. Moreover, it cannot be excluded that a user, by selecting the data that are used to train or feed an AI-system, contributes decisively to the (originality of the) output, which may lead to copyright protection, implying that such user could be regarded as a (co-)author.¹⁵⁸ In that context, the mere selection of an output from multiple AI-generated outputs will not by itself give rise to copyrights.¹⁵⁹ Only if the person making the selection, or another person, also improves or

¹⁵⁰ Art. 2 Software Directive, Art. 4 Database Directive.

¹⁵¹ F. GOTZEN and M.- C. JANSSENS, *Wegwijs in het intellectueel eigendomsrecht*, o.c., p. 43.

¹⁵² B. MICHAUX et al., "Copyright in Artificially-Generated Works", o.c., p. 221.

¹⁵³ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 79

¹⁵⁴ B. MICHAUX et al., "Copyright in Artificially-Generated Works", o.c., p. 221-222: "[...] there is no reason to attribute Copyright ownership of the final work to a person who has only coded the program – that is, who has written the program in a language that can be understood by the machine."

¹⁵⁵ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 74.

¹⁵⁶ B. MICHAUX et al., "Copyright in Artificially-Generated Works", o.c., p. 222.

¹⁵⁷ Art. 9(3) UK CDPA. Such a work is protected for a shorter period of 50 years (Art. 12(7) UK CDPA). No moral right protection applies (Arts 79, 81 UK CDPA regarding right to paternity and integrity respectively). See also: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 87-88.

¹⁵⁸ B. MICHAUX et al., "Copyright in Artificially-Generated Works", o.c., p. 221-224

¹⁵⁹ A selection of multiple works from AI-assisted/-generated works may be eligible for database copyright protection if the selection falls under the definition of database (art.I.13,6° CEL) and it is the 'own intellectual creation' of an author (Art. XI.18 CEL).

modifies the output (after generation by the AI), imbuing it with their personal touch and originality, such person may be considered a (co-)author and be entitled to copyrights on the final work.¹⁶⁰ In other words, the AI-operator should manipulate the AI-system to such extent that it assists in expressing its personal creativity.¹⁶¹

If more than a single author is involved in the process, and the authors collaborate (e.g. a developer and a user), this will lead to co-authorship, even if the creative contributions occur at different stages of the creative process. Valid authorship or co-authorship claims by developers of AI-systems are likely to arise primarily in situations where developers and users collaborate closely on an AI production and where the developer played a significant creative role in a specific process. In many if not most cases, however, the developers of AI-systems will not collaborate in a material way with the users on generating *specific* outputs, meaning that no concerted creative effort will be present.¹⁶²

In borderline cases, stakeholders and courts will thus be confronted with the need to precisely determine the relative importance of all human and AI contribution(s) in order to be able to make a correct copyright classification of an output and the related attribution of author-/ownership. Evidently, this is a legal situation that may cause difficulties and raises the question of whether it is still a contemporary approach to focus on the human intellect. One could therefore ask the question if the legislator should intervene and (i) issue guidance concerning the elements that should be taken into account when determining the relative importance of the author's contribution vis-à-vis other authors and the AI-system (or whether this should be left to the courts); (ii) open up the possibility for attributing copyright to AI-generated works (to a certain extent); or (iii) establish a new sort of (statutory) protection. This will be discussed later during the project.

A final relevant topic which relates to the authorship/ownership of AI-assisted output is the issue of copyfraud. Proving or enforcing authorship or copyright ownership of a work is sometimes difficult in practice. For this reason, Belgium, just like other EU-countries, provide for a rule that establishes a (rebuttable) presumption of authorship, in that the person indicated on or with the published work as the author is deemed to be the author, unless proven otherwise (Art. XI.170, second sentence CEL). The Berne Convention and Enforcement Directive validate such legal presumptions, and allow the person whose name "appear[s] on the work in the usual manner" to instigate infringement procedures.¹⁶³ Evidently, rules like these might be abused in cases where AI-generated/ assisted outputs that do not meet the standards of copyright protection are published and falsely attributed to a natural or legal person. After all, these "work-like but authorless" AI-creations may be considered as a work *de facto* even though they are not works *de jure*.¹⁶⁴ This opens the possibility for copyright trolls to abuse the presumption of authorship in order to extort other authors and claim copyright protection.¹⁶⁵ Defendants will then have the onerous task to argue why the work should not be protected by copyright (e.g. because it is entirely generated by AI). As explained above, copyright protection is indeed only available if there is sufficient creative human intervention, but disproving a claim for copyright protection in relation

¹⁶⁰ B. MICHAUX et al., "Copyright in Artificially-Generated Works", o.c., p. 223; F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 329.

¹⁶¹ F. VEHAR and T. GILS, "I'm sorry AI, I'm afraid you can't be author (for now)", o.c., p. 722

¹⁶² J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 84-85. These authors also point out that co-authorship claims from AI-developers will also be unlikely for commercial reasons as they will not want to burden customers with downstream copyright claims.

¹⁶³ Art. 15(1) Berne Convention; Art. 5 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (as corrected in OJ L 157) ("Enforcement Directive").

¹⁶⁴ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 334;

¹⁶⁵ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 87, 117-118.

to AI-assisted/-generated output with certainty will be very difficult in practice, especially if there is no transparency with regard to the level of human/AI-contribution.¹⁶⁶ In view of the possibility of such abuses, it may therefore be considered to revise the legal presumption of authorship.

3.1.3. Other Restrictions Under Copyright: Moral Rights, Term of Protection and Exceptions

The way in which copyright protection is designed in Belgium, on an EU level and by the Berne Convention, presupposes the involvement of a human actor. Copyright provides an author not only with economic rights but also with moral rights (e.g. right to paternity or integrity). Granting a machine such rights (in their current form) would constitute an aberration.¹⁶⁷

Furthermore, the term of protection of copyright (life plus 70 years after the death of the author, art. XI.166 CEL) cannot be applied with regard to an AI-system.¹⁶⁸

Finally, certain copyright exceptions only apply if the author is acknowledged and/or if an equitable remuneration is paid to such author.¹⁶⁹

3.2. Sui Generis/Related Rights¹⁷⁰

AI-generated and AI-assisted output which would not be eligible for copyright protection may be able to enjoy protection under various related right-regimes. The major difference between related rights and copyright in this context is that related rights do not require originality or authorship. On the contrary, and apart from the performers' related right, these related rights have in common that they reward economic or entrepreneurial expenditure rather than human creativity. By the same token, most related rights may vest directly in legal persons to whom the entrepreneurial activities are to be attributed. At first sight, therefore, these related rights more easily accommodate AI-assisted outputs than copyright law with its focus on human creativity. We will discuss various possibilities briefly below. We will first address sui generis database right (part 3.2.1.) followed by rights of phonogram and film producers (part 3.2.2.), broadcasters (part 3.2.3.) and publishers of press publications (part 3.2.4.). A major drawback regarding the approach of protecting AI-generated/-assisted outputs via related rights, is that such rights do not exist for every category of AI-generated work.¹⁷¹

3.2.1. Sui Generis Database Right¹⁷²

Interestingly, the Database Directive defines the owner of the database right as the "maker of a database" (art. 7 Database Directive). According to Recital 41 Database Directive and art. XI.1.17, 2° CEL, this is "the (natural or legal) person who takes the initiative and the risk of investing", in

¹⁶⁶ J. VANHERPE, "AI and IP – a tale of Two Acronyms", o.c., §44. A similar remark can be made in relation to patent protection. This author furthermore points out that the possibility of such abuse may be a reason to not ban AI-generated output to the public domain, because users of creative AI-systems will then be incentivized to remain silent on the involvement of AI-systems in the creation of output. One can imagine that this could be remedied by an obligation on users to disclose the use of AI-systems in the creative process, but enforcing such transparency obligations is often complicated.

¹⁶⁷ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 331. See also F. DE ROUCK, "Moral Rights & AI Environments: The Unique Bond Between Intelligent Agents and Their Creations", *JiLP* 2019, p. 299-304. This author argues that the moral rights provided to human authors under the international copyright regime may serve as inspiration for EU legislators in developing new policies to safeguard the link between intelligent agents and their creations.

¹⁶⁸ B. MICHAUX et al., "Copyright in Artificially-Generated Works", o.c., p. 225; J. VANHERPE, "AI and IP – a tale of Two Acronyms", o.c., §20

¹⁶⁹ See under Belgian law: Arts. XI.190(1), and XI.191/1(5) CEL.

¹⁷⁰ This part is based on J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 88-94.

¹⁷¹ F. VEHAR and T. GILS, "I'm sorry AI, I'm afraid you can't be author (for now)", o.c., p. 723

¹⁷² See also part 0

other words: the human database producer. This rules out sui-generis protection for databases entirely generated by AI-systems, without any investment of human origin. Moreover, only nationals or residents of EU Member States, or companies and firms formed in accordance with the law of a Member State and having their registered office, central administration or principal place of business within the EU, may benefit from the sui generis right.¹⁷³

Nonetheless, and in absence of an originality or authorship-requirement, it is possible that all sorts of AI-assisted outputs which qualify as “databases”, including the database of pharmaceutical properties of molecules, weather reports and sports data generated by AI may be protected. As mentioned before, the substantial investment requirement allows the costs of developing and implementing AI technology to be factored in, and therefore does not seem to present an unsurmountable obstacle to protection.

Under Belgian law, some authors discuss protection via the sui generis database right in relation to two rather specific situations.¹⁷⁴ Firstly, they discuss the possibility that the selection of data which are used to train or feed an AI-system may not only be protected by copyright (if the selection is ‘original’) but also by the sui generis right if such selection entails a substantial quantitative or qualitative investment (Article XI.306 CEL, see supra). Secondly, the final output produced by the AI-system may also be covered by the sui generis right which could cover the above-mentioned selection of training data if the AI-assisted/-generated output corresponds to a substantial part of the database for qualitative reasons. This is, however, rather unlikely.

There are nevertheless various major challenges with the feasibility of this approach for the protection of AI-assisted/-generated outputs, e.g. the question remains whether more traditional types of works apart from data/information compilations could be covered by the database producer right.¹⁷⁵ In any event, such protection does not cover the data contained in the database nor new works generated from a database, except, in unlikely situations.

3.2.2. Rights of Phonogram and Film Producers

The Rental and Lending Rights Directive¹⁷⁶ and the InfoSoc Directives harmonise the related right of phonogram producers (Art. XI.209-XI.210 CEL).¹⁷⁷ Producers of “phonograms” (i.e. sound recordings) enjoy rights of reproduction, distribution and communication to the public.¹⁷⁸ The Directives do not define the notions of “phonogram” and “phonogram producer”. From their legislative history, it transpires that these definitions can be derived from the 1960 Rome Convention and the 1996 WIPO Performances and Phonograms Treaty (WPPT), the two main international treaties on the protection of related rights.

The Rome Convention defines a “phonogram” as an “exclusively aural fixation of sounds of a performance or of other sounds”, and a “producer of phonograms” as “person who, or the legal entity which, first fixes the sounds of a performance or other sounds”.¹⁷⁹ The WPPT provides for

¹⁷³ Art. 11 Database Directive.

¹⁷⁴ B. MICHAUX et al., “Copyright in Artificially-Generated Works”, o.c., p. 222-223 and 226-228.

¹⁷⁵ Recital 17 Database Directive; J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 94.

¹⁷⁶ Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version).

¹⁷⁷ B. MICHAUX et al., “Copyright in Artificially-Generated Works”, o.c., p. 226-227.

¹⁷⁸ See Arts. 9(1)(b) Rental and Lending Rights Directive and 2(c) and 3(2)(b) InfoSoc Directive.

¹⁷⁹ Art. 3(a) and (c) Rome Convention.

similar, albeit slightly different definitions.¹⁸⁰ With digital technology in mind, the WPPT adds a definition of “fixation”, which is absent from the Rome Convention. Fixation is defined as “the embodiment of sounds, or of the representations thereof, from which they can be perceived, reproduced or communicated through a device”. In the case of computer-generated or computer-assisted music production, the notion clearly extends to sounds directly recorded on a computer hard drive or other digital equipment.

The phonographic right is triggered by the act of “fixation” of sounds in a recording medium. No act of human authorship is needed, nor does the phonogram right require originality or any other threshold prerequisite. As the diplomatic records of the Rome Convention reveal, even a simple recording (by means of a tape recorder) of “bird songs” suffices.¹⁸¹

As Advocate General SZPUNAR explains in his opinion in the Pelham case: “[a] phonogram is not an intellectual creation consisting of a composition of elements such as words, sounds, colours etc. A phonogram is a fixation of sounds which is protected, not by virtue of the arrangement of those sounds, but rather on account of the fixation itself. [...]. Moreover, in the case of a phonogram, there is no requirement for originality, because a phonogram, unlike a work, is protected, not by virtue of its creativeness, but rather on account of the financial and organisational investment.”¹⁸²

The phonographic rights vests in the “producer” of the phonogram. The international conventions define a “phonogram producer” in similar, but not identical ways/ Based on the definition in the Rome convention, a phonogram producer may either be a natural person or a legal entity. The WPPT’s definition is more elaborate. A “phonogram producer” is “the person, or the legal entity, who or which takes the initiative and has the responsibility for the first fixation of the sounds of a performance or other sounds, or the representations of sounds”. The WPPT’s definition makes clear that the definition focuses on the entrepreneurial activity of the person or legal entity “taking the initiative and having the responsibility” for the recording, rather than on the physical person that actually makes the first recording.

In light of the phonogram right’s absence of a requirement of human authorship or originality, and its rationale of rewarding economic or entrepreneurial activity, this right will fairly easily allow protection for certain AI output. In practical terms, all that is required, is that the AI-generated or -assisted output at issue qualifies as a “phonogram”, in other words: a recording of sounds. This opens the door to a wide variety of AI produced audio output, ranging from the generation through AI of electronic dance music to the generation through AI of aural translations.

In respect of such audio recordings generated by AI, the phonographic right will be allocated to “the person, or the legal entity, who or which takes the initiative and has the responsibility for the first fixation of the sounds of a performance or other sounds, or the representations of sounds”. This will in most cases be the user of the AI software, not the developer, since it is the user that triggers the act of fixation of the sounds by activating the AI-system.

Similarly, the Rental and Lending Rights Directive and the InfoSoc Directive also provide for the right of “producers of the first fixations of films”, generally known as the film producer’s right.¹⁸³ This film producer’s right has, however, no history in the Rome Convention. Its origin can be traced to German law that traditionally protects non-original moving pictures (so-called Laufbilder) under

¹⁸⁰ Art. 2 WPPT: (b) “phonogram” means the fixation of the sounds of a performance or of other sounds, or of a representation of sounds, other than in the form of a fixation incorporated in a cinematographic or other audio-visual work; (c) “fixation” means the embodiment of sounds, or of the representations thereof, from which they can be perceived, reproduced or communicated through a device; (d) “producer of a phonogram” means the person, or the legal entity, who or which takes the initiative and has the responsibility for the first fixation of the sounds of a performance or other sounds, or the representations of sounds.

¹⁸¹ WIPO Guide to the Rome Convention, WIPO 1981, p. 22.

¹⁸² Opinion AG SZPUNAR 12 December 2018, no. C-476/17 ECLI: EU:C:2018:1002, Pelham GmbH v Hutte, §30.

¹⁸³ Art. 9(1)(c) Rental and Lending Rights Directive; Art. 2(d) and 3(2)(c) InfoSoc Directive.

related rights.¹⁸⁴ Note that a motion picture will normally (also) qualify as an original film work or audiovisual work protected by copyright, and that the copyright will usually be assigned to the film producer. The practical importance of having a separate related right is that it accords a minimum of legal protection to producers of *non-original* films.

Also the film producer's right does not require originality or provide for any other threshold requirement. As a consequence, it allows protection of all sorts of video content generated by AI-systems, varying from surveillance videos, to drone footage, to satellite imagery, to video content automatically generated for media channels.

Although the Directives are silent on the issue of ownership of the film producer's right, it may be assumed that the allocation rule of the phonographic right applies here *mutatis mutandis*. In other words, the right will belong to the person or legal entity, who or which takes the initiative and has the responsibility for the first fixation of the film. In case of AI generated audio-visual output this will in most cases be the user of the AI software – not the developer.

In summary, these ancillary rights may arise for the producer of the first recording of a phonogram/the first fixation of a film. As this right aims to protect the investment and the effort in ensuring such first recording/fixation, it is not constrained by the originality threshold and does not require human intervention in the creation of the work itself. Hence, in theory, a person could be entitled to such producer's right if he employs an AI-system producing music or films and he ensures the first recording or fixation of said final work, even if there is no human intervention in the 'creative' process.¹⁸⁵

3.2.3. Rights of Broadcasters

In line with the Rome Convention, the Rental and Lending Rights Directive and the InfoSoc Directive also accord related rights to "broadcasting organisations" in respect of their broadcasts (see also art. XI.215 and XI.216 CEL).¹⁸⁶ Again, the Directives leave the definitions to the Rome Convention. The latter defines "broadcasting" as "the transmission by wireless means for public reception of sounds or of images and sounds",¹⁸⁷ but does not provide a definition of "broadcasting organisation." Apparently, this notion was considered self-explanatory.

Like the phonogram right, the related right of broadcasting organisations does not require any creative activity to trigger protection, nor does it provide for any other threshold requirement. All that is needed is an act of "broadcasting" of audio or audiovisual content by a "broadcasting organisation." Whereas the scope of the Rome Convention is limited to traditional "wireless" broadcasting, the Rental and Lending Rights Directive also protects broadcasts by cable or satellite.¹⁸⁸

Likewise, the broadcasters' related right can easily give rise to protection of AI-assisted output if the preconditions of the right are met, in other words if a broadcast is automatically produced and transmitted by an AI-system. Note that computer-assisted radio broadcasting has been a common phenomenon for some time, while "artificial DJ's" are reportedly now making inroads into music radio.¹⁸⁹

¹⁸⁴ Art. 95 German Copyright Act.

¹⁸⁵ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", *o.c.*, p. 333 and 334. These authors rightly note that the scope of protection of this right is nonetheless rather limited (no moral rights limited to the specific first fixation and primarily aimed at preventing illegal reproductions).

¹⁸⁶ Art. 13 Rome Convention. See also Art. 14(3) TRIPS.

¹⁸⁷ Art. 3(f) Rome Convention.

¹⁸⁸ See Art. 7(2) Rome Convention; Art. 8(3) Rental and Lending Rights Directive.

¹⁸⁹ See: R.J. STINE, "Radio Streamlines Workflow With Artificial Intelligence", available at <https://www.tvtechnology.com/news/radio-streamlines-workflow-withartificial-Intelligence>.

3.2.4. Rights of Publishers of Press Publications

Article 15 of Directive 2019/790 on copyright and related rights in the Digital Single Market (CDSM Directive) obliges the Member States to grant certain exclusive rights to “publishers of press publications”.¹⁹⁰ Like the film producer’s right, this new related right has its origin in Germany.¹⁹¹ The right is meant to protect European newspaper publishers against online news aggregators that allegedly undermine the newspaper’s business model. The CDSM Directive provides a detailed definition of “press publication”. This is “a collection composed mainly of literary works of a journalistic nature, but which can also include other works or other subject matter, and which: (a) constitutes an individual item within a periodical or regularly updated publication under a single title, such as a newspaper or a general or special interest magazine; (b) has the purpose of providing the general public with information related to news or other topics; and (c) is published in any media under the initiative, editorial responsibility and control of a service provider.”¹⁹² Similar to the related rights previously discussed the press publisher’s right does not require originality, and thus leaves room for content generated by AI that otherwise fits this definition. For example, a blog generated by AI on sports news would probably qualify for protection, as long as it is published under the imprint of a European press publisher.¹⁹³ Recital 56 (in fine) which excludes “websites, such as blogs, providing information as part of an activity that is not carried out under the initiative, editorial responsibility and control of a news publisher” from the scope of protection does not seem to preclude such finding. After all, the news publisher will have decided to use an AI-system for blog generation, implying that the activity by the AI-system is indeed carried out under the initiative, editorial responsibility and control of the news publisher.¹⁹⁴

3.3. Patent Law

AI plays an important role in innovation processes and may have the potential to increasingly marginalise human ingenuity and human input in new inventions. AI has already been used to come up with technical inventions that, if made by humans, could, in principle be patentable.¹⁹⁵ As in the case of copyright, the patentability of inventions generated by AI raises several questions for patent law. Most importantly, should inventions entirely generated or assisted by AI-systems be granted patents? To whom should inventorship be awarded for such AI-generated inventions? For the sake of the argument, we will first address the issue of inventorship (part 3.3.1.), followed by the patentability of AI-assisted inventions and related issues (part 3.3.2).

3.3.1. Inventorship

For AI-assisted/-generated inventions, the question of inventorship arises. Who should be listed as the inventor of such new asset? Neither European, nor Belgian patent law provide for a definition of inventorship, although there is a presumption that it belongs to a ‘natural person’.¹⁹⁶

¹⁹⁰ Art. 15 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

¹⁹¹ Art. 87f German Copyright Act.

¹⁹² Art. 2(4) CDSM Directive.

¹⁹³ Note that the press publisher’s right is not available for publishers that are not established in an EU Member State. See Art. 15(1) CDSM Directive.

¹⁹⁴ What the exclusion does exclude from protection, is the situation where an AI-system would start generating press publications and publish them online without being linked to any kind of existing news publisher. This, however, seems currently very unlikely, if not impossible.

¹⁹⁵ See also: J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., §26-27

¹⁹⁶ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 101-103; K. VANHALST et al., “Inventorship of inventions made using Artificial Intelligence”, *ICIP 2020*, nr.2, p. 397-399 and 403. These authors indicate that it could be a “quick-win” for the legislator to explicitly clarify in Belgian patent law, just as in copyright law, that an inventor must be a natural person.

Indeed, a number of provisions of patent law would simply make no sense if we were to accept AI inventorship.¹⁹⁷

First, many patent laws stipulate that, in principle and in similar vein as under copyright law, the ‘inventor’ is the first owner of an invention, except in an employment context, where (under the laws of some countries) the employer may be deemed to be the first owner.¹⁹⁸ Since AI-systems do not have legal personality, they arguably cannot be the bearer of ownership rights, nor can they be an employee as such.¹⁹⁹ Given that those are the only two available options, such systems cannot be considered ‘inventors’ under patent law as it currently stands.

Another argument against AI inventorship may be drawn from the inventor’s moral right of attribution. Every inventor has the right to be mentioned as such and all patent applications must designate the inventor.²⁰⁰ This moral right may become meaningless when the application of the concept of inventorship is extended to AI-systems.²⁰¹ More specifically, this right fulfils a reward function, allowing the inventor to build on his or her reputation by being named in the patent application as the “creator” or “parent” of the invention.²⁰²

The fact that inventorship is reserved for humans, was explicitly confirmed by the EPO in the two DABUS-decisions. In the autumn of 2018, a number of patent applications were filed for two of DABUS’ inventions.²⁰³ The prosecution file for both patent applications indicated DABUS as the alleged inventor and clarified that Dr Thaler (inventor of DABUS) obtained the right to the inventions as a successor in title – being the employer and/or the owner of the machine.²⁰⁴ The EPO, however, refused both applications and held that the formal requirement for patent applications to designate the inventor(s) as set by the EPC (Article 81 *jo* Rule 19.1) refers to a

¹⁹⁷ E.g. Art. XI.9 CEL refers to the scenario where multiple persons have independently invented something, while Art. XI.10 CEL talks about entitlement claims being open to persons. See also S. YANISKY-RAVID and X. LIU, “When Artificial Intelligence Systems Produce Inventions: an Alternative Model for Patent Law at the 3A Era”, *Cardozo Law Review* 2018, p. 2230 available at <https://ssrn.com/abstract=2931828>.

¹⁹⁸ See Art. 60 EPC. The corresponding provision under Belgian law is Art. XI.9 CEL. See regarding employee output under Belgian law Arts XI.187 and XI.296 CEL.

¹⁹⁹ K. VANHALST et al., “Inventorship of inventions made using Artificial Intelligence”, *o.c.*, p. 398; N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, European Patent Office, February 2019, p. 10-11 available at [http://documents.epo.org/projects/babylon/eponet.nsf/0/3918F57B010A3540C125841900280653/\\$File/Concept_of_Inventorship_in_Inventions_involving_AI_Activity_en.pdf](http://documents.epo.org/projects/babylon/eponet.nsf/0/3918F57B010A3540C125841900280653/$File/Concept_of_Inventorship_in_Inventions_involving_AI_Activity_en.pdf).

²⁰⁰ See e.g. also Art. 4(A) Paris Convention for the Protection of Industrial Property, 20 March 1883, as amended. This is the oldest international convention on industrial property rights.. See also respectively Arts. 62 and 81 *jo*. 90 and Rule 19.1 of the Implementing Regulation EPC. The corresponding provisions under Belgian law are Arts XI.13 and XI.16(1), 7° CEL. Note that these provisions require that e.g. the name and address of the inventor is provided. See also N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, *o.c.*, p. 8.

²⁰¹ N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, *o.c.*, p. 23-25, 27.

²⁰² K. VANHALST et al., “Inventorship of inventions made using Artificial Intelligence”, *o.c.*, p. 403-404. These authors point out that it could be possible, in theory, to talk about the “reputation” of an AI-system, much like the reputation of a trademark. However, so long as the AI-system does not have legal personality, it cannot benefit from its increased reputation within the legal system. As a result, the ultimate beneficiary of an AI’s reputation build-up would be the undertaking behind the AI entity. The personal reward function would then be reduced to commercial benefits for the company in question.

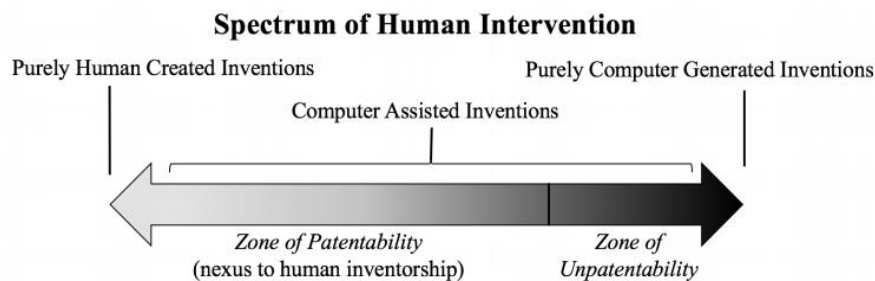
²⁰³ DABUS is a neural network-based system comprising two artificial neural networks. The first neural network, made up of a series of smaller neural networks, has been trained with general information from various knowledge domains. This first network generates novel ideas in response to self-perturbations of connection weights between neurons and component neural nets therein. A second “critic” artificial neural network monitors the first neural network for new ideas and identifies those ideas that are sufficiently novel compared to the machine’s pre-existing knowledge base. The critic net also generates an affective response that in turn injects/retracts perturbations to selectively form and ripen ideas having the most novelty, utility, or value. See: <https://artificialinventor.com/dabus/>. See also: EP application 18275163.6 and UK patent application GB1816909.4, both filed on 17 October 2018. The substantively equivalent US patent application is available at www.artificialinventor.com/wp-content/uploads/2019/07/Fractal-Container-Application.pdf and EP application 18275174.3 and UK patent application GB1818161.0, both filed on 7 November 2018. The substantively equivalent US patent application is available at www.artificialinventor.com/wp-content/uploads/2019/07/Neural-Flame-Application.pdf.

²⁰⁴ See EPO Decisions 27 January 2020 re patent applications 18275163.6 and 18275174.3, §1-5, available at register.epo.org.

human being, not a machine.²⁰⁵ Since the patent applications filed for DABUS' inventions designate DABUS as the inventor, both applications were affected by a formal deficiency and the patents were therefore refused – even before the analysis of the substantive requirements for patentability (novelty, inventive step and industrial applicability) took place.²⁰⁶ At the time of writing, appeal proceedings before the EPO are still ongoing.²⁰⁷

As apparent, the EPO employed a rather formal argument to refuse the application.²⁰⁸ Substantively speaking, Belgian case law provides more guidance as to the requirements to be considered an inventor. As such, the Supreme Court clarified that entitlement vests in “anyone who has actually contributed to the invention by his intellectual and creative input”.²⁰⁹ A similar definition has been adopted by both lower and higher courts, specifying that a “substantial contribution to the invention” is required (in the sense of actual intellectual or creative input), which is assessed “in light of the conceptual value of the claimed invention”.²¹⁰ This can be considered in line with the case law of the Boards of Appeal of the EPO, referring to the inventor as someone “who has performed the creative act of invention.”²¹¹ SHEMTOV summarises this as follows in his comparative study: (human) inventorship may arise in case of a contribution to the invention(/inventive concept) that transcends the purely financial, abstract or administrative level and that is aimed at conceiving the claimed invention.²¹²

Similarly as under copyright law, the distinction between AI-generated and AI-assisted output will be relevant. To illustrate this, we can use the following framework, proposed by MCLAUGHLIN.²¹³ This framework analyses the spectrum of human intervention to distinguish between patentable computer(/AI)-assisted and unpatentable and computer(/AI)-generated inventions (see supra). According to the scale, when a computer-assisted invention lacks sufficient human intervention to constitute a connection (cf. ‘nexus’) to human inventorship, the computer-assisted invention enters a zone of unpatentability.²¹⁴ Although being unpatentable, it remains free to be protected in other areas of law such as trade-secret law. This framework is illustrated in the figure below taken from MCLAUGHLIN.



²⁰⁵ EPO Decisions 27 January 2020 re patent applications 18275163.6 and 18275174.3, §23-30, available at register.epo.org.

²⁰⁶ EPO Decisions 27 January 2020 re patent applications 18275163.6 and 18275174.3, §35-37. Note also that the EPO stated that names given to things (such as AI entities) cannot be equated with names of natural persons, which form part of their personality and enable them to exercise their rights.

²⁰⁷ The Statement of Grounds of Appeal filed on behalf of Dr. Thaler on 27 May 2020 is available online at register.epo.org/application?documentId=E4T32W3C7876DSU&number=EP18275163.

²⁰⁸ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 100.

²⁰⁹ Cass. 18 November 2016, no. C.14.0316N.N, *Ayal v. Katoen Natie*.

²¹⁰ See e.g. Court of Appeal Antwerp, 11 April 2016, *IRDI* 2016/2, p. 166; Comm. Court Brussels, 24 February 2017, *IRDI* 2017/3, p. 221; Comm. Court Antwerp, 18 October 2013, *IRDI* 2014/1, p. 381.

²¹¹ See e.g. EPO Boards of appeal, case J 7/99, point 2, and case J 8/82, points 9 and 13.

²¹² N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, o.c., p. 19-21.

²¹³ M. MCLAUGHLIN, ‘Computer-Generated Inventions’, 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097822.

²¹⁴ See also J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 102-103.

In order to establish whether an AI-assisted invention is patentable or not in a certain situation, the general rules on inventorship should be applied. In other words, the actual contribution of each individual will need to be assessed. Inventorship regarding an invention created with the aid of an AI-system should not be viewed differently than inventions which came about using other tools (e.g. a computer or calculator, using certain assays or markers etc.). In summary, the contribution of each individual to “the invention” should be assessed in light of the inventive concept. If such contribution surpasses the purely financial, abstract or administrative level and is aimed at conceiving the claimed invention, such individual should be able to claim (co-)inventorship. Also here, different actors may be eligible to claim (co-)inventorship.²¹⁵ Below we will discuss some of these possibilities. We will also address this point more generally in part 3.5. Ownership of AI-Generated Output.

For instance, designing or programming an AI-system with a specific problem in mind whereby it is used to design a particular type of product or process and the resulting patentable invention is of the type of product or process intended, may well enable AI-designers/-programmers to claim inventorship. This will obviously depend on the concrete circumstances and the inventive concept, but it should not be excluded a priori. A similar reasoning could apply with regard to the individuals selecting the data or the source of the data used to train an AI-system.²¹⁶

Similarly, if an individual uses an AI-system to design a particular type of product or process, regardless of the fact whether the resulting output was intended or not, such AI-user may well be able to claim inventorship if his contribution meets the requirements. In such case, it can be argued that the contribution of the human consists in deliberately using an AI-entity in order to achieve a certain result. The human is the one identifying the technical problem and the means to solve it; the AI-system is merely a tool to arrive at the solution. Both the initiation of and the intent for the result therefore lies with the human. Moreover, identifying the patentable invention amidst the (unintended) results generated by an AI-system, could accordingly suffice to be attributed inventorship. A similar reasoning could apply for the individuals generating or selecting the data or the source of the data which is used as input for a trained AI-system algorithm.

In this regard, ALLAN et al. point out that it may be advisable not to focus on exactly how much of the inventive activity, if any, is attributable to an AI-system, for two reasons. First, the AI-system’s “inventiveness” may well be derivative of the person(s) who programmed and/or supervised or directed the AI-system. Second, if a human person made an inventive contribution to an invention that meets patentability criteria, the fact that part of the inventive activity can be attributed in whole or in part to an AI-system should not prevent the invention from being patented as long as there is a sufficient nexus between the invention and the applicant (see supra).²¹⁷

In summary, and in the words of SHEMTOV: “When it comes to a human actor that uses an AI-system, whose identity may be inconsequential to the invention process, who simply uses a machine learning technique developed by another, the inventor may be the person who ‘tooled’ the AI-system in a particular way in order to generate the inventive output. Hence, under such circumstances the person that carries out the intelligent or creative conception of the invention may be the one who geared up the AI-system towards producing the inventive output, taking decisions in relation to issues such as the choice of the algorithm employed, the selection of

²¹⁵ See in detail: K. VANHALST et al., “Inventorship of inventions made using Artificial Intelligence”, o.c., p. 399-402 and 407-408.

²¹⁶ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 105

²¹⁷ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 104-105.

parameters and the design and choice of input data, even if the specific output was somewhat unpredictable”.²¹⁸

Just as for copyright, this is a legal situation that may cause difficulties and raises the question of whether it is still a contemporary approach to focus on the human intellect. One could therefore ask the question if the legislator should intervene and (i) issue guidance concerning the elements that should be taken into account when determining the relative importance of the inventor’s contribution vis-à-vis other inventors and the AI-system (or whether this should be left to the courts); (ii) open up the possibility for attributing patent protection to AI-generated inventions (to a certain extent); or (iii) establish a new sort of (statutory) protection. This will be discussed later during the project.

3.3.2. Patentability of AI-assisted output

In principle, nothing prevents the granting of patents for AI-assisted inventions (and strictly speaking also not for AI-generated inventions), provided they entail patentable subject-matter and comply with the formal requirements set by patent offices.²¹⁹ According to Articles 52 *jo* 54-57 EPC, art. XI.3 *jo* art. XI.6-7 CEL, patents can be granted for any inventions that may have an industrial application, are new and involve an inventive step. In addition, Article 83 EPC/Article XI.18 CEL stipulates that “an application shall disclose the invention in a manner for it to be carried out by a person skilled in the art” (see *supra*). For this part, we will focus on the novelty (part A) and inventive step (part B). Sufficiency of disclosure has already been discussed in part 2.1.2. and the reasoning outlined there, can be applied *mutatis mutandis* on AI-assisted output.²²⁰

A. Novelty

This section explores issues regarding the application of the novelty requirement under the EPC to AI-assisted (or generated) outputs as inventions.²²¹ This part of the analysis can be brief since there appear to be few significant novelty-related challenges associated with such outputs for our purposes. Still, there are few issues to explore.

The basic rules for novelty under the EPC is that an invention is new only if it does not form part of the “state of the art” available to the public “by means of a written or oral description, by use, or in any other way, before the date of filing of the European patent application” (Article 54, §1-2 EPC, Article XI.6, §1-2 CEL) To defeat novelty, a single item of the state of the art must contain the elements of a claim in the application and enable the person skilled in the art (PSA) to “practice the technical teaching which is the subject of the document, taking into account also the general knowledge at that time in the field to be expected of him”.²²² In contrast, for inventiveness or inventive step (discussed below), elements of prior art may be combined.²²³

It should also be made clear at the outset that determining novelty can always be a difficult process, whether AI is involved or not: “The requirement of novelty ... is becoming increasingly

²¹⁸ N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, *o.c.*, p. 35.

²¹⁹ VANHALST et al. point out that an exclusion from patentability merely because an invention was made using a certain amount of AI would be detrimental to innovation as well as form an unjustified discrimination against a specific technology, which would infringe the technological neutrality of patent law (Art. XI. 3 CEL). See: K. VANHALST et al., “Inventorship of inventions made using Artificial Intelligence”, *o.c.*, p. 402 and 406

²²⁰ See also: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, *o.c.*, p. 111-113.

²²¹ See Arts. 54 and 55 EPC; Art. XI.6-7 CEL.

²²² EPO, “Guidelines for Examination, Part G, Chapter VI, 4”, 2020 available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_vi_4.htm.

²²³ EPO, “Guidelines for Examination, Part G, Chapter VII, 6”, 2020, available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_vii_6.htm.

difficult to meet and determine with any great level of certainty.”²²⁴ The role of AI in this field means that several parallel changes are happening. More data can be parsed by AI-systems used by patent applicants or by patent offices. AI can assist inventors in myriad ways in selecting the most relevant data for humans to work with. AI-systems can also be used by patent offices to analyse more potentially relevant prior art faster. Applicants can perhaps use this same feature to modify or even “broaden” claims in an application. Thus far, those are essentially *quantitative* changes to the amount of data that an AI-system might be able to process during a patent application or examination process as compared to a human examiner. Admittedly, an experienced human examiner might, however, perform a much more targeted search and thus need to process much less data to arrive at their conclusion.

One possibly *qualitative* change that this quantitative change (and the related analytical approach) might induce is worth noting, however. It is that the novelty assessment will be increasingly performed by AI-systems. As EBRAHIM explains: “Unlike past technological advancements in tools for the invention process, artificial intelligence technology ushers in a form of omniscience in the patent-prosecution process and disintermediates the patent-prosecution process. The move toward automation and predictive analytics in patent prosecution will undoubtedly decrease reliance on patent legal judgment. In economic terms, artificial-intelligence technology reduces the transaction costs of acquiring patents.... Therefore, the economic impact of artificial-intelligence technologies will reshape patent law from a policy perspective. The danger in artificial-intelligence technology, particularly predictive analytics that can make predictions from large data sets, is the complex and opaque effects on interactions”.²²⁵

ALLAN et al. therefore recommend to maintain a level of technical capability at patent offices that matches the technology available to (most) patent applicants.²²⁶

Concerns regarding patent numbers potentially rising to undesirable levels (due to AI-assisted/-generated inventions) are also being somewhat met by projects attempting to algorithmically create and publicly publish all possible new prior art so that any of such output would no longer be patentable by others.²²⁷ However, the EPO guidelines indicate in G-IV, section 2 that “Subject-matter can only be regarded as having been made available to the public, and therefore as comprised in the state of the art pursuant to Art. 54, §1 EPC, if the information given to the skilled person is sufficient to enable him, at the relevant date (see G-VI, 3) and taking into account the common general knowledge in the field at that time, to practice the technical teaching which is the subject of the disclosure (see T 26/85, T 206/83 and T 491/99)”.²²⁸ Consequently, it has therefore been argued that for the ‘All Prior Art’-prior art lacks the required enabling disclosure.²²⁹

B. Inventive step

Article 56 EPC/Article XI.7 CEL requires that an invention shall not be obvious to a ‘person skilled in the art’ (“PSA”) taking into account the ‘state of the art’. The ‘person skilled in the art’ is a key issue for AI-generated inventions. The EPC itself does not give a definition of a ‘person skilled in the art’, but this notion has been interpreted through case-law and various guidelines. Guideline

²²⁴ J. WILD, “Artificial Intelligence and the Future of the Patent System”, *IAM (blog)*, 11 July 2018, available at <https://www.iam-media.com/law-policy/artificial-intelligence-and-future-patent-system>.

²²⁵ T. EBRAHIM, “Automation & Predictive Analytics in Patent Prosecution: USPTO Implication & Policy”, *Georgia State University Law Review* 2019, vol. 35, no. 4, p. 118 available at <https://readingroom.law.gsu.edu/gsulr/vol35/iss4/5>.

²²⁶ J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 106-107.

²²⁷ See the ‘All Prior Art’-project by Alexander REBEN (<https://areben.com/project/all-prior-art/>).

²²⁸ EPO, “Guidelines for Examination, Part G, Chapter IV, 2”, 2020, available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_iv_2.htm.

²²⁹ B. BERMAN, “‘All prior art’ algorithm won’t stop bad patents or actors”, *IP CloseUp* 6 June 2016, available at <https://ipcloseup.com/2016/06/06/all-prior-art-algorithm-wont-stop-bad-patents-or-actors/>.

G-VII, 3 stipulates the following: “[t]he person skilled in the art is presumed to be a skilled practitioner in the relevant field of technology, who is possessed of average knowledge and ability and is aware of what was common general knowledge in the art at the relevant date. He is also presumed to have had access to everything in the ‘state of the art’, in particular the documents cited in the search report, and to have had at his disposal the means and capacity for routine work and experimentation which are normal for the field of technology in question...”. This guideline further states that “there may be instances where it is more appropriate to think in terms of a group of persons, e.g. a research or production team, rather than a single person...”.²³⁰

In the context of AI-systems, it has been argued that the possible use of AI as a tool (if its use was common in the field in question) needs to be taken into account when assessing the inventive step.²³¹ One effect of inventions involving AI and machine learning may thus be an increase in the level of skills and knowledge of the skilled person and thus an increase in the level of inventive step required. After all if, at some point in the future, the use of AI-powered inventive machines becomes commonplace in certain (or even all) sectors of technology, the PSA-standard will evolve into a PSA using such an AI-powered inventive machine.²³²

Raising the bar for inventive step and ensuing patentability is not without problems, as highlighted by two scholars. BLOK argues that “the toughest problem may be how to determine the capabilities of a normal artificial intelligence tool, and more in particular, how examiners, patent attorneys and patent judges can establish whether the average skilled person equipped with that tool could and would create a specific product or process. Determining the reach of artificial intelligence is particularly difficult, because the output of an artificial intelligence application is hard to predict”.²³³ VANHERPE, on her turn, points out that “[t]aken to its logical extreme, this argument could shake the very foundations of our patent system. Indeed, if the ‘artificially superintelligent’ PSA is capable of inventive step, everything becomes obvious, leaving no more room for patentable inventions. This conclusion may seem quite drastic, because it is. We therefore need to start thinking about alternatives and/or supplements to the current non-obviousness analysis – and maybe even to the patent regime as such as a way to provide incentives to innovation”.²³⁴

3.4. Trademark/Design Law

For the purpose of this part, we will consider whether AI-systems can generate signs or designs that may be eligible for trademark (part 3.4.1.) or design protection (part 3.4.2.). We will also briefly touch upon some other effects that may occur as a consequence of the application of AI-systems in the trademark/design domain (part 3.4.3.). As opposed to the wealth of scholarship on AI and copyright/patent law, the interface between AI and trademark law has been explored considerably less.

3.4.1. Trademark Protection for AI-Generated/-Assisted Output

In this part, we will examine the object of the protection (part A) as well as formal requirements (part B). We will end this part with a short conclusion (part C).

²³⁰ EPO, “Guidelines for Examination, Part G, Chapter VII, 3”, 2020, available at https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_vii_3.htm.

²³¹ See in detail: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 107-110.

²³² J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., §32; K. VANHALST et al., “Inventorship of inventions made using Artificial Intelligence”, o.c., p. 402.

²³³ P. BLOK, “The inventor’s new tool: artificial intelligence – how does it fit in the European patent system?”, *EIPR* 2017, vol. 39, no. 2, p. 69-73.

²³⁴ She refers extensively to R. ABBOTT, “Everything is Obvious”, *UCLA L. Rev.* 2018, p. 3-52, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3056915#.

A. Object of Protection: a Trademark

Both the EU Trademark Regulation (TMR)²³⁵ as well as the Benelux Convention on Intellectual Property (BCIP) state that trademarks may consist of any signs, in particular words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, provided that such signs are capable of (a) distinguishing the goods or services of one undertaking from those of other undertakings; and (b) being represented on the register in a manner which enables the competent authorities and the public to determine the clear and precise subject matter of the protection afforded to its proprietor (Article 4 TMR and Article 2.1 BCIP).

These provisions are usually understood to result in three requirements. A trademark needs to consist of (i) a sign (ii) which can be represented graphically, and (iii) which has a distinctive character.²³⁶ The CJEU has further elaborated these requirements in its case law. For instance, in its *Sieckmann*-judgment, it stated that a trade mark may consist of a sign which is not in itself capable of being perceived visually, provided that it can be represented graphically, particularly by means of images, lines or characters, and that the representation is clear, precise, self-contained, easily accessible, intelligible, durable and objective.²³⁷ These additional requirements are of particular importance for olfactory, sound and colour marks. The questions that arise in relation to these substantive requirements would, however, be no different if an AI-system was used to create trademarks as none of the requirements imply the (creative) intervention of a human.

Neither do the absolute and relative grounds for refusal seem to include a ground that would render an AI-generated trademark “un-trademarkable” because of the fact that it would have been generated by an AI-system (Article 7 & 8 TMR and Article 2.2bis & 2.2ter BCIP).

B. Formal Requirements?

As the substantive requirements do not seem to entail any real issue, we will now briefly discuss if there are formal requirements that would necessarily imply the intervention of a human actor in order to validly obtain trademark protection and own a trademark.

One needs, however, to recognize that there is a fundamental difference with copyright and patent law in this respect, as trademark law does not really have an equivalent actor to the author or inventor. There is no first ‘*trademark-er*’. Rather the TMR/BCIP refer to the ‘applicant’ for a trademark or the ‘proprietor’ of trademark who are typically not the persons who came up with the trademark sign. Nonetheless, these notions, just like the author and inventor, are also clearly aimed at legal or natural persons. For instance, Article 19 TMR contains a reference to the seat or domicile of the proprietor of a trademark, Article 53 TMR refers to ‘the name of the person requesting renewal’, while art. 55 TMR refers to ‘a change of the name or address’ of the proprietor of a trademark.²³⁸ All of these provisions refer to features that AI-systems currently do not have, as they do not have legal personality.

C. Conclusion

Current trademark law does not seem to prevent companies from using AI-systems to generate trademarkable signs or assist humans in designing such signs, while applying for those trademarks in name of the company, rather than indicating the AI-system as the applicant/proprietor. Should the AI-system itself be indicated as the applicant, it remains rather unclear what the outcome

²³⁵ Regulation 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark, OJ L 154/1, p. 1-99.

²³⁶ J. PILA and P. TORREMANNS, *European Intellectual Property Law*, Oxford, Oxford University Press, 2016, p. 367-374.

²³⁷ CJEU, 12 December 2002, no. C-273/00, ECLI:EU:C:2002:748, *Sieckmann*, §55.

²³⁸ Art. 2.31 BCIP refers, for instance, to a transfer of trademark between companies.

would/should be as trademark law does not feature a specific human-tailored actor, as opposed to the author or inventor from copyright/patent law. In summary, trademark law does not share their anthropocentric nature.

3.4.2. Design Protection for AI-Generated/-Assisted Output AI

Both the EU Regulation 6/2002 on Community designs (CDR), as well as the BCIP state that models and designs for products designs are eligible for protection if they are new and have individual character (Article 4.1 CDR; Article 3.1 BCIP).²³⁹

Novelty means that no identical design should have been made available to the public before the date of filing of the application for registration or the date on which the design for which protection is claimed has first been made available to the public, in case of an unregistered community design (Article 5 CDR, Article 3.3.1 BCIP).²⁴⁰ A design shall be considered to have individual character if the overall impression it produces on the informed user differs from the overall impression produced on such a user by any design which has been made available to the public before the date on which the design for which protection is claimed has first been made available to the public (unregistered community design) or before the date of filing of the application for registration or, if a priority is claimed, the date of priority (community design). In assessing the individual character, the degree of freedom of the designer in developing the design shall be taken into consideration (Article 6 CDR, Article 3.3.2 BCIP).

Although these substantive requirements of novelty and individual character by themselves do not seem to necessarily exclude the possibility of AI-generated designs, the additional guidance in relation to the assessment of individual character introduces the notion of 'designer'. In the same vein, Article 14.1 CDR clearly states that the right to the community design shall vest in the designer or his successor in title.²⁴¹ Interestingly, the BCIP does not contain an equivalent provision. Article 3.7.1 BCIP does, however, mirror Article 15.1 CDR which grants the designer the right to claim to become recognised as the legitimate holder of the community design if an unregistered community design was disclosed or claimed by, or a registered community design was applied for or registered in the name of a person who was not entitled to the design. Furthermore, Article 14.3 CDR and Article 3.8 BCIP refer to employees creating designs on behalf of an employer. Finally, Article 18 CDR contains the (moral) right of the designer to be cited as such before the EUIPO and in the register. Various other articles of both laws also refer to the designer, the successors in title, the applicant for or the proprietor of the design.

To conclude, one can infer from the provisions cited above that the creation of a design eligible for protection under current design law implies some (creative) intervention from a human (i.e. the designer), similar to the situation in patent and copyright law. Likewise, AI-assisted designs should be able to enjoy design protection if they fulfil the validity requirement of novelty and individual character.

3.4.3. Other Topics under Trademark/Design Law

Apart from the issues identified under the previous point, some other trademark/design-relevant topics may also come into play as AI-systems increasingly become commonplace.

²³⁹ The CDR defines design as "the appearance of the whole or a part of a product resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself and/or its ornamentation". Product is understood as "any industrial or handicraft item, including inter alia parts intended to be assembled into a complex product, packaging, get-up, graphic symbols and typographic typefaces, but excluding computer programs" (art. 3 CDR). The BCIP uses similar definitions.

²⁴⁰ Art. 5.2 adds that designs will be deemed identical if their features differ only in immaterial details.

²⁴¹ J. PILA and P. TORREMANS, *European Intellectual Property Law*, o.c., p. 497.

First of all, online platforms, smart home devices and smart appliances increasingly intervene in the purchasing process, thereby minimizing (or possibly even eliminating) consumer participation in the purchasing decision. Such systems provide personalized product recommendations and may influence brand and default purchase preferences of consumers. Through these recommendations (and possibly e.g. showing low-cost alternatives when a consumer is looking for products of a certain brand), AI-systems may misdirect consumers and influence the distinctive character of trademarks. In the same sense, AI-systems may have an impact on how examiners and courts think about “likelihood of confusion” and the “average consumer”.²⁴²

On the other hand, trademark offices can use AI-systems as a powerful tool in their evaluations of trademark applications. For instance, the EUIPO employs AI-based technology (eSearchplus) to search for similar-looking trademarks and designs.²⁴³ Likewise, in 2019 WIPO launched an AI-powered image search technology that makes it faster and easier to establish the distinctiveness of a trademark in a target market.²⁴⁴ Trademark owners, on their turn, can use such image recognition technology to scan the internet in search for counterfeit goods or companies abusing their trademark(s).

3.5. Ownership of AI-Generated Output²⁴⁵

As explained above, intellectual property law as it currently stands in principle does not allow for AI- systems to be recognised as either an author or an inventor, due to their lack of both physical and legal personhood as well as their (currently) largely instrumental nature.²⁴⁶ Even if an AI-system would transcend its status as a tool and create or innovate in a more autonomous way, it could be argued that an AI-system – being a machine – does not need any reputational or financial incentive to do so and that allocating any IP rights to it would be devoid of any real purpose.²⁴⁷

The next issue is then whether the intervention of a creative and/or inventive AI excludes *any* kind of human authorship or inventorship (and thus ownership) in relation to the output at issue. As explained above, it does not as long as there is a physical person who commands the AI and maintains the requisite level of control over its output.²⁴⁸ In such a case, IP rights may fulfil their role of protecting the interests of the human creators as well as provide an indirect incentive for future creation and/or innovation.²⁴⁹ However, if there is no sufficient causal relationship between the (in)actions of a creative and/or inventive human and the end result – in other words, if the AI becomes more than an assisting tool wielded by a human –, the argument in favour of a human author and/or inventor becomes rather untenable. What exactly constitutes ‘sufficient’ control may be tough to establish, given the wide spectrum that exists between different types of AI,

²⁴² R. KEEN et al., *Artificial Intelligence (AI) and the Future of Brands: How will AI Impact Product Selection and the Role of Trademarks for Consumers?*, International Trademark Association, October 2019, available at <https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/AI-and-the-Future-of-Brands-Report-2019-010-18.pdf>.

²⁴³ See in this regard: https://euipo.europa.eu/ohimportal/nl/key-user-newsflash/-/asset_publisher/dIGJZDH66W8B/content/thanks-to-user-feedback-image-search-now-improved-in-tmview-and-eSearch-plus.

²⁴⁴ See: https://www.wipo.int/pressroom/en/articles/2019/article_0005.html.

²⁴⁵ Based on J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., §33-44.

²⁴⁶ The European Parliament adopted a resolution in which it clearly states that “in this connection, [...] it would not be appropriate to seek to impart legal personality to AI technologies and points out the negative impact of such a possibility on incentives of human creators”. See: European Parliament Resolution, 2020/2015(INI), Intellectual Property Rights for the development of artificial intelligence technologies, 20 October 2020, §13.

²⁴⁷ See for instance D. GERVAIS, “The Machine As Author”, o.c., p. 2053-2106 (rejecting “arguments in favor of protection of machine productions by copyright for several reasons, not the least of which is that machines need no legal or financial incentives to run their code”).

²⁴⁸ See parts 3.1.1. and .3.3.1

²⁴⁹ S.F. HEDRICK, “I “Think,” Therefore I Create”, *NYU Journal of IP and Ent. Law* 2019, vol. 8, no. 2, p. 337 and 440.

between output that is merely AI-assisted and output that is purely AI-generated (see *supra*).²⁵⁰ The black box nature of some AI-systems can further complicate matters.²⁵¹ What level of human intervention is required for a sufficient original and/or an inventive contribution to arise, will hence be particularly tricky and will often require a case-by-case analysis.²⁵² Different categories of people involved in AI-systems may stake a claim in this regard. Moreover, and importantly, these categories will also be relevant in the context of AI-generated output, which we will now discuss jointly for copyright and patent law as similar reasonings apply.

First in line are the programmer(s)²⁵³, designer(s)²⁵⁴ and/or producer(s) of the AI-system – or, in many cases, the legal entity that employs them (hereinafter collectively referred to as ‘AI creators’). By creating the AI-system itself, these actors play a substantive role in the production of AI-generated output.²⁵⁵ Put simply: without them, no AI-system and without AI-system, no AI-generated output. Regardless of the analogy with chance creations/innovations, the allocation of ownership rights to the creator sits uneasily (at least to a certain extent) with the unpredictable nature of AI-generated output.²⁵⁶ Indeed, it could be argued that the AI’s intervention cuts the requisite direct link between the programmer’s actions and the AI-generated output. While the AI creator’s choices and parameters define the AI-system, they do not define the ‘final form of the work’ as such.²⁵⁷ This argument gains in strength the more autonomous the AI algorithm becomes. Then again, a programmer who is somehow dissatisfied with the AI’s initial output may tweak the AI’s algorithm at a later stage, thus manipulating and shaping further output, as well as curate the AI output based on their own, personal (perhaps creative and/or innovative) choices. Could these be the steps necessary for a programmer to rightfully claim control over and, thus, ownership of the AI-system’s output?²⁵⁸ A generalised answer to this question is, at present, impossible to give.²⁵⁹

In any case, an economic argument against granting the creator ownership rights in AI-generated output is that this may lead to ‘double-dipping’.²⁶⁰ For example, this would be the case if the creator also holds ownership rights in a patent or multiple patents granted in relation to the AI-system or the copyright therein, or if the AI-system is acquired by a third party for a (presumably

²⁵⁰ F. GOTZEN and M.-C. JANSSENS, “Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie”, o.c., p. 327-328.

²⁵¹ J. VANHERPE, “AI and IP – a tale of Two Acronyms”, o.c., §36. See also: J. ALLAN et al., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, o.c., p. 82-83. These authors use their notion of “general authorial intent” to account for unpredicted or unexplainable output of an AI-system. They argue that as long as such output stays within the ambit of the author’s general authorial intent that such output can enjoy copyright protection.

²⁵² N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, o.c., p. 31.

²⁵³ See regarding a Chinese court decision in favour of this solution: P. SAWERS, “Chinese court rules AI-written article is protected by copyright”, 10 January 2020, available at www.venturebeat.com/2020/01/10/chinese-court-rules-ai-written-article-is-protected-by-copyright.

²⁵⁴ See in favour: M. SUMMERFIELD, “The Impact of Machine Learning on Patent Law, Part 3: Who is the Inventor of a Machine-Assisted Invention?”, 4 February 2018, www.blog.patentology.com.au/2018/02/the-impact-of-machine-learning-on.html.

²⁵⁵ G. GABISON, “Who Holds the Right to Exclude for Machine Work Products?”, December 2019, 23, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3498941; P. SAMUELSON, “Allocating Ownership Rights in Computer-Generated Works”, o.c., p. 1205; N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, o.c., p. 22.

²⁵⁶ P. SAMUELSON, “Allocating Ownership Rights in Computer-Generated Works”, o.c., p. 1209; S. YANISKY-RAVID and X. LIU, “When Artificial Intelligence Systems Produce Inventions: an Alternative Model for Patent Law at the 3A Era”, o.c., p. 2231-2232.

²⁵⁷ A. BRIDY, “Coding Creativity: Copyright and the Artificially Intelligent Author”, *Stan. Tech. L. Rev.* 2012, p. 25, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1888622.

²⁵⁸ cf. S.F. HEDRICK, “I “Think,” Therefore I Create”, o.c., p. 338-39, 343, 354, 362.

²⁵⁹ For an illustration of the differing opinions on this topic: J. OSHA et al., “AIPPI Summary Report on Inventorship”, 2020, p. 9-13.

²⁶⁰ This can also apply in relation to the moral right to be named as inventor: see K. VANHALST et al., “Inventorship of inventions made using Artificial Intelligence”, o.c., p. 404 and 406. See contra N.I. BROWN, “Artificial Authors: A Case for Copyright in Computer-Generated Works”, *Col. S.T.L.R.* 2018, vol. XX, p. 22-24.

rather significant) fee and the original and/or inventive output at issue postdates this transfer.²⁶¹ In both cases, the creator would obtain two separate sources of income for essentially the same thing. This would arguably be an unfavourable outcome. In addition, we must consider the user's right to data protection, as well as practical aspects, such as issues of enforceability. Enforcing ownership rights on the part of the AI creator would be problematic if the AI-system generates the output at issue after a third party has started using it. Indeed, knowing that ownership rights would be allocated to the creator, the subsequent user would have strong incentives not to report back on the (modalities of) creation of protectable output.²⁶² Effective enforcement of such rights would moreover risk negatively impacting potential users' incentives to purchase AI-driven systems.²⁶³

A similar claim to the AI-system's creator (especially the programmer who alters the algorithm in a way that influences future output) may be made by the AI's trainer who feeds data/input to the AI-system with the aim of achieving a certain result.²⁶⁴ Alternatively, also the user who has contributed substantially to the original/inventive elements of the AI-system's output at issue may claim ownership.²⁶⁵ An economic argument in favour of the latter solution is that this would incentivise the user to further distribute the AI-generated output.²⁶⁶ Again, however, it is unclear how much input (and ensuing influence on output) exactly would be required for them to be able to validly stake a claim in the output. Merely pressing the 'on'-button that brings the AI into action should be insufficient, while translating the AI's discoveries to a patentable technical teaching would arguably be enough, as well as making creative choices in the selection and editing of the AI's output.²⁶⁷ Then again, it might be near impossible to properly distinguish button-pushers from genuine user-authors/inventors in practice.²⁶⁸

The list of stakeholders continues with the investor²⁶⁹, the owner of the AI-system and/or the data used to train the algorithm, the publisher of the work²⁷⁰, the general public and even the government.²⁷¹ Moreover, some form of co-ownership may be envisaged between two or more

²⁶¹ P. SAMUELSON, "Allocating Ownership Rights in Computer-Generated Works", *o.c.*, p. 1207-1208; N. SHEMTOV, "A study on inventorship in inventions involving AI activity", *o.c.*, p. 31; S. YANISKY-RAVID and X. LIU, "When Artificial Intelligence Systems Produce Inventions: an Alternative Model for Patent Law at the 3A Era", *o.c.*, p. 2233.

²⁶² P. SAMUELSON, "Allocating Ownership Rights in Computer-Generated Works", *o.c.*, p. 1208.

²⁶³ G. GABISON, "Who Holds the Right to Exclude for Machine Work Products?", *o.c.*, p. 22-25.

²⁶⁴ B. MICHAUX et al., "Copyright in Artificially-Generated Works", *o.c.*, p. 221-224; N. SHEMTOV, "A study on inventorship in inventions involving AI activity", *o.c.*, p. 31.

²⁶⁵ G. GABISON, "Who Holds the Right to Exclude for Machine Work Products?", *o.c.*, p. 35; N.I. BROWN, "Artificial Authors: A Case for Copyright in Computer-Generated Works", *o.c.*, p. 37-39; P. SAMUELSON, "Allocating Ownership Rights in Computer-Generated Works", *o.c.*, p. 1201-1204; S.F. HEDRICK, "I 'Think,' Therefore I Create", *o.c.*, p. 344; W.M. SCHUSTER, "Artificial Intelligence and Patent Ownership", *Wash. & Lee L. Rev.* 2018, vol. 75, no. 4, p. 1950, 1988-91. See in detail: L. BUIJTELAAR and M. SENFTLEBEN, "Auteursrecht op robotcreaties? Een analyse op basis van de incentive theorie", *AMI* 2020, p. 77-93.

²⁶⁶ P. SAMUELSON, "Allocating Ownership Rights in Computer-Generated Works", *o.c.*, p. 1226; S.F. HEDRICK, "I 'Think,' Therefore I Create", *o.c.*, p. 345-346.

²⁶⁷ See regarding the possible originality of a selection process CJEU 16 July 2009, no. C-5/08, ECLI:EU:C:2009:465, *Infopaq/Danske Dagblades Forening*, §45. See also N. SHEMTOV, "A study on inventorship in inventions involving AI activity", *o.c.*, p. 22; P. SAMUELSON, "Allocating Ownership Rights in Computer-Generated Works", *o.c.*, p. 1201; P. BLOK, "The inventor's new tool: artificial intelligence – how does it fit in the European patent system?", *o.c.*, p. 73; S.F. HEDRICK, "I 'Think,' Therefore I Create", *o.c.*, p. 346;

²⁶⁸ cf. J. GRIMMELMANN, "There's No Such Thing as a Computer-Authored Work – And it's a Good Thing, Too", *Columbia Journal of Law & the Arts* 2016, p. 410-411.

²⁶⁹ cf. E. BONADIO and L. MCDONAGH, "Artificial Intelligence as Producer and Consumer of Copyright Works: Evaluating the Consequences of Algorithmic Creativity", *I.P.Q.* 2020, p. 124-125.

²⁷⁰ A. RAMALHO, "Will Robots Rule the (Artistic) World? A Proposed Model for the Legal Status of Creations by Artificial Intelligence Systems", *Journal of Internet Law* 2017, vol. 21, no. 1, p. 12-25.

²⁷¹ See e.g. S. YANISKY-RAVID and X. LIU, "When Artificial Intelligence Systems Produce Inventions: an Alternative Model for Patent Law at the 3A Era", *o.c.*, p. 2232-33. See also EPO Decisions 27 January 2020 re patent applications 18275163.6 and 18275174.3, para. 13 and in particular para. 33: "(...) The owner of an AI system may (...) own the output of that system, just as an owner of any machine may own the output of that machine. However, the question of ownership must be distinguished from the question of inventorship and from the rights connected herewith".

of the actors mentioned above, such as the user and the creator of the AI.²⁷² However, this would entail other theoretical and practical issues, such as (respectively) an unnecessary fragmentation of ownership rights and difficulties in proving (the extent of) the claims of wannabe right holders.²⁷³ It could even be argued that, in view of the ever-rising number of players involved, no individual entity can rightfully claim to have made a significant contribution ‘worthy’ of IP ownership.²⁷⁴

As of yet, therefore, no solution to the ownership conundrum appears to readily available. Moreover, it is unlikely that this question will be definitively resolved in the near future. It could even be argued that a catch-all solution would be both impossible and undesirable and that a case-by-case assessment of ownership claims will remain warranted.²⁷⁵ The void left by this uncertainty will likely be filled with contractual solutions between the relevant parties.²⁷⁶ As a result of unequal bargaining power, Coasean bargaining²⁷⁷ may be prevented and instances of unfair ownership and licensing arrangements are to be expected.²⁷⁸

Another solution could be to not allocate ownership in AI-generated output to anyone at all and instead allot such output to the public domain.²⁷⁹ Indeed, without a human author and/or inventor, how can any human actually be motivated to create and what would the point of granting any IP right be?²⁸⁰ Arguably, the relevant stakeholders can sufficiently protect their investment in AI-related innovation by relying on patent protection for the AI-system itself, first-mover advantage, trade secret law, contractual arrangements and technological protection measures as well as general civil liability and the law of unfair competition.²⁸¹ While proponents of additional IP protection will undoubtedly argue that additional protection is needed to incentivise R&D, no empirical evidence backing up this claim appears to be available to date.

As of yet, however, there is a pragmatic reason not to ban AI-generated output to the public domain, namely that it is (and will become) increasingly difficult to distinguish AI-generated output from AI-assisted output and humane creations. While this issue could in theory be remedied by requiring aspiring IP owners to disclose AI intervention in the creation and/or innovation process, the practical application of such a requirement will likely be problematic.²⁸² Indeed, the prospect having a work be banished to the public domain would provide stakeholders seeking a return on investment with strong incentives to keep quiet on this point. Thus, this could invite misleading

²⁷² E. BONADIO and L. MCDONAGH, “Artificial Intelligence as Producer and Consumer of Copyright Works: Evaluating the Consequences of Algorithmic Creativity”, *o.c.*, p. 124; N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, *o.c.*, p. 30.

²⁷³ N.I. BROWN, “Artificial Authors: A Case for Copyright in Computer-Generated Works”, *o.c.*, p. 34-35; P. SAMUELSON, “Allocating Ownership Rights in Computer-Generated Works”, *o.c.*, p. 1221-1224; S.F. HEDRICK, “I “Think,” Therefore I Create”, *o.c.*, p. 348.

²⁷⁴ S. YANISKY-RAVID and X. LIU, “When Artificial Intelligence Systems Produce Inventions: an Alternative Model for Patent Law at the 3A Era”, *o.c.*, p. 2235.

²⁷⁵ S.F. HEDRICK, “I “Think,” Therefore I Create”, *o.c.*, p. 347-48.

²⁷⁶ F. VEHAR and T. GILS, “I’m sorry AI, I’m afraid you can’t be author (for now)”, *o.c.*, p. 724-726.

²⁷⁷ See extensively W.M. SCHUSTER, “Artificial Intelligence and Patent Ownership”, *o.c.*, p. 1951-52, 1967-82.

²⁷⁸ cf. R. ABBOTT, “I Think, Therefore I Invent: Creative Computers and the Future of Patent Law”, *B.C. L. Rev.* 2016, p. 1117; S.F. HEDRICK, “I “Think,” Therefore I Create”, *o.c.*, p. 347.

²⁷⁹ See in this sense A.H. KHOURY, “Intellectual Property Rights for Hubots: On the Legal Implications of Human-like Robots as Innovators and Creators”, *Cardozo Arts & Ent LJ* 2017, p. 635-668; F. GOTZEN and M.-C. JANSSENS, “Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie”, *o.c.*, p. 334-345; G. GABISON, “Who Holds the Right to Exclude for Machine Work Products?”, *o.c.*, p. 22 and 41-43.

²⁸⁰ P. SAMUELSON, “Allocating Ownership Rights in Computer-Generated Works”, *o.c.*, p. 1224-1225.

²⁸¹ D. GERVAIS, “The Machine As Author”, *o.c.*, p. 2060; G. GABISON, “Who Holds the Right to Exclude for Machine Work Products?”, *o.c.*, p. 32-33, 39; N. SHEMTOV, “A study on inventorship in inventions involving AI activity”, *o.c.*, p. 24; S. YANISKY-RAVID and X. LIU, “When Artificial Intelligence Systems Produce Inventions: an Alternative Model for Patent Law at the 3A Era”, *o.c.*, p. 2222, 2252-2256.

²⁸² R. ABBOTT, “Everything is obvious”, *UCLA L. Rev.* 2018, p. 6, 34-35.

statements on authorship and/or inventorship of AI-generated output in the future.²⁸³ This is the crux of the matter: IP protection is (and, arguably, should only be) available if the creator is human, but disproving a claim for human authorship in relation to AI-generated output with certainty is nearly impossible. Therefore, as long as it is impossible to prove whether or not AI technology was used in the production of certain output, blindly refusing protection to AI-generated output may lead to unfair situations in practice.

3.6. Infringement of Intellectual Property Rights by AI-Systems

To conclude this part on intellectual property, we will briefly discuss the hypothesis of infringement of intellectual property rights by AI-systems. In this part, we will focus on copyright for two reasons; (i) the available legal literature discussing IP-infringement by AI-systems focuses on copyright, and (ii) considerations in relation to infringement by AI-generated/-assisted output under copyright can similarly apply under e.g. patent and trademark law. After all, this is essentially a discussion of extracontractual liability. We will briefly discuss IP-infringement through input (part 3.6.1.), IP-infringement through output (part 3.6.2.) and liability for IP-infringement (part 3.6.3.)

3.6.1. IP-Infringement Through Input: Training of AI-Systems

Data-driven AI-systems (e.g. machine learning) require vast amounts of data in order to learn, train and properly function. It cannot be excluded that such 'data' sensu lato are protected by copyright (for software) and/or database protection (see infra part 2.2. IP-Protection for Data). Consequently, the use of such data – even for training purposes – will in principle necessitate the prior authorisation of the copyright owner. There are, however, some exceptions which may come into play in the context of AI-systems.²⁸⁴

Firstly, there is the exception for temporary acts of reproduction which are transient or incidental and an integral and essential part of a technological process and whose sole purpose is to enable a lawful use of a work and which have no independent economic significance (art. 5.1 InfoSoc Directive, art. XI.189, §3 CEL). This has been further clarified by the CJEU in the two Infopaq-judgments.²⁸⁵ For instance, in the Infopaq I-judgement the CJEU held “that an act can be held to be ‘transient’ within the meaning of [Article 5(1) InfoSoc Directive] only if its duration is limited to what is necessary for the proper completion of the technological process in question, it being understood that that process must be automated so that it deletes that act automatically, without human intervention, once its function of enabling the completion of such a process has come to an end”.²⁸⁶ In the second Infopaq-judgement, the CJEU clarified that such acts have an independent economic significance if “[...] the acts of temporary reproduction lead to a change in the subject matter reproduced as it exists when the technological process concerned is initiated, because those acts no longer aim to facilitate its use, but the use of a different subject matter” (e.g. the output produced by an AI-system having been trained on existing works).²⁸⁷ Due to this strict interpretation, GOTZEN and JANSSENS conclude that is unlikely that all acts with the purpose of training an AI-system will meet the five cumulative conditions of the exception.²⁸⁸

²⁸³ R. ABBOTT, “I Think, Therefore I Invent: Creative Computers and the Future of Patent Law”, o.c., p. 1097-98; R. ABBOTT, “Everything is obvious”, o.c., p. 29.

²⁸⁴ F. GOTZEN and M.-C. JANSSENS, “Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie”, o.c., p. 335-336.

²⁸⁵ CJEU, 16 July 2009, no. C-5/08, ECLI:EU:C:2009:465, *Infopaq/Danske Dagblades Forening* (Infopaq I); CJEU, 17 January 2012, no. C-302/10, ECLI:EU:C:2012:16, *Infopaq/Danske Dagblades Forening* (Infopaq II).

²⁸⁶ CJEU, 16 July 2009, no. C-5/08, ECLI:EU:C:2009:465, *Infopaq/Danske Dagblades Forening* (Infopaq I), §64.

²⁸⁷ CJEU, 17 January 2012, no. C-302/10, ECLI:EU:C:2012:16, *Infopaq/Danske Dagblades Forening* (Infopaq II), §54.

²⁸⁸ F. GOTZEN and M.-C. JANSSENS, “Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie”, o.c., p.336

Secondly, one can envisage that certain actors (e.g. secondary schools or universities) may be able to rely on the exception for educational and scientific purposes (art. XI.191/1 CEL) in the course of their education of scientific activities (e.g. AI-related R&D).²⁸⁹ However, also here the (fact-specific) question arises as to the extent the output generated by an AI-system will also be covered by the exception.²⁹⁰

Thirdly, the future text- and data mining (TDM) exceptions, included in the CDSM Directive (which needs to be implemented by EU Member States by June 2021) may be of particular relevance for AI-developers/-users.²⁹¹ The material and personal scope of these provisions are, however, quite limited.²⁹² Art. 3 requires Member States to provide for an exception for reproductions and extractions made by research organisations and cultural heritage institutions in order to carry out, for the purposes of scientific research, text and data mining of works or other subject matter. Note that this exception is limited to research organisations and cultural heritage institutions and can only cover activities aimed at scientific research. Art. 4, on the other hand, does provide for a 'general' TDM-exception but only applies insofar "the use of works and other subject matter [...] has not been expressly reserved by their rightholders in an appropriate manner, such as machine-readable means in the case of content made publicly available online." Recital 18 CDSM Directive adds: "In the case of content that has been made publicly available online, it should only be considered appropriate to reserve those rights by the use of machine-readable means, including metadata and terms and conditions of a website or a service. Other uses should not be affected by the reservation of rights for the purposes of text and data mining. In other cases [e.g. offline], it can be appropriate to reserve the rights by other means, such as contractual agreements or a unilateral declaration." Hence, it is evident that rightholders can largely sideline this exception themselves.²⁹³

Several distinguished authors deem these TDM-exceptions to be insufficient.²⁹⁴ Moreover, this limited scope of the TDM-exception contrasts with the broader fair use exception under US copyright law and the broader exception for data analytics under Japanese copyright law.²⁹⁵ Hence, the Belgian legislator may wish to investigate to what extent it can broaden the wording of the TDM-exceptions.

²⁸⁹ See also art. XI.190, °5 CEL.

²⁹⁰ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 337.

²⁹¹ Arts 3-4 Dir. (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (CDSM Directive), OJ L 17 May 2019, nr. 130, 92. Note that recital 8 of this directive clarifies that text and data mining should be understood broadly. Furthermore, it is interesting to note that article 3 does not mention the Software Directive, leaving open the question whether TDM of e.g. source code is covered by the exception contained in article 3.

²⁹² F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 337

²⁹³ Note, moreover, that both exceptions also require the works should be lawfully accessible (art. 3.1 and 4.1 CDSM Directive).

²⁹⁴ See on this topic in detail e.g. C. GEIGER, G. FROSIO and O. BULAYENKO, "Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data?: Legal Analysis and Policy Recommendations", *IIC* 2018, p. 814-844; R. DUCATO and A. STROWEL, "Limitations to Text and Data Mining and Consumer Empowerment: Making the Case for a Right to "Machine Legibility"", *IIC* 2019, p. 649; E. ROSATI, "Copyright as an Obstacle or an Enabler? A European Perspective on Text and Data Mining and Its Role in the Development of AI Creativity", *Asia Pac Law Rev* 2019, p. 217; P.B. HUGENHOLTZ, "The New Copyright Directive: Text and Data Mining (Articles 3 and 4)", *Kluwer Copyright Blog*, 24 July 2019, www.copyrightblog.kluweriplaw.com/2019/07/24/the-new-copyright-directive-text-and-data-mining-articles-3-and-4/; S. FLYNN, C. GEIGER, J. PEDRO QUINTAIS, T. MARGONI, M. SAG, L. GUIBAULT and M.W. CARROLL, "Implementing User Rights for Research in the Field of Artificial Intelligence: A Call for International Action", *EIPR* 2020, pp. 393-398.

²⁹⁵ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 337. These authors explain that Japanese copyright allows for TDM for machine learning, as long as the use of the existing works only serves the machine learning process and there is no human perception of the work.

If no exception is found to be applicable in this regard and AI-developers/-users are not able to secure an (expensive) license for (training) data, it can be expected that they will either use old public domain data, look for data under open licenses or even infringe intellectual property rights hoping that the rightholders do not notice.²⁹⁶

3.6.2. IP-Infringement Through Output: Reproduction or Adaptation

The output created by or with the aid of an AI-system may infringe on the copyright of a third party. By way of example, an AI-system could create a song or painting containing original elements of pre-existing works, infringing the reproduction right of the owner of the copyright in the works at hand.²⁹⁷ If indeed such original elements can be found in the AI-output, the defence of entirely independent creation seems in any case nearly impossible due to fact that AI-systems require a great number of examples to learn, rendering it quite likely that the initial work featured among those examples.

A related remark is that a style or genre 'per se' cannot be protected under copyright. Consequently, an AI-system could create a Banksy- or Justin Bieber-like work, insofar no original elements from a specific work are copied.²⁹⁸ However, an additional limitation in this regard is the author's right of adaptation (art. XI.165, §1 CEL, art. 12 Berne Convention). This right entails that even significantly modified works keep enjoying protection under the copyright for the initial work, as long as the form of the initial work can be distinguished.²⁹⁹ Such adaptation may enjoy separate copyright protection, but still requires the prior authorization from the initial copyright owner in order to validly come into existence and to be exploited. The underlying question of whether such AI-assisted/-generated adaptation could be original, has been discussed above (see part 3.1. Copyright).

Finally, it is also possible that such AI-assisted/-generated output infringes upon the moral rights of attribution and integrity (art. XI.165, §2 CEL, art. 6bis Berne Convention).

The hypothesis of infringing AI-assisted/-generated output may lead to further contentious matters, such as whether or not relevant exceptions and/or limitations (should) apply (see previous point) and what role fundamental rights such as freedom of expression or commerce may play in such cases.³⁰⁰

3.6.3. Liability for Intellectual Property Infringement

When it is established that the intellectual property rights of a party have been infringed, the question as to who can be held liable will arise. In the absence of legal personality for AI-systems

²⁹⁶ See A. LEVENDOWSKI, "How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem" *Wash. L. Rev.* 2018, 579. This author points out that legal restrictions on datasets may contribute to the bias-problem in AI-systems. AI-developers will tend to use easy accessible data, avoiding data sets for which it is difficult to obtain a license. This may lead to situations in which developers prefer using less relevant datasets, as more relevant or representative datasets may be harder to obtain.

²⁹⁷ Similarly, it cannot be excluded that an "inventive machine" develops a process and/or product that could infringe a patent when put into practice, or devises a sign that is confusingly similar to a registered trademark, or a product that falls within the scope of a protected (un)registered design

²⁹⁸ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 338.

²⁹⁹ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 338

³⁰⁰ J. OSHA et al., o.c. , p. 1.

(which has been debated extensively³⁰¹) or applicable contractual arrangements, the different extracontractual liability regimes will come into play.³⁰²

In this regard, the distinction between AI-assisted and AI-generated output becomes more relevant again. In the hypothesis of infringing AI-assisted output, rightholders will be able sue the person (or group of persons) who contributed to the infringing output by having used the AI-system to create an infringing reproduction, perform an unauthorized communication to the public or having failed to sufficiently review the output for infringing material.³⁰³ In practice, it may be difficult to ascertain the extent of the responsibility of the different actors, but no indications have been found that this would be different from other complex situations involving technology (e.g. technology outsourcing projects).

The hypothesis of infringing AI-generated output is more difficult as no human can be held responsible 'per se' for the infringement, resulting in a situation where rightholders may have trouble seeking compensation for the damage incurred. This is, however, not a specific issue for intellectual property infringements but is a more general issue for all kinds of extracontractual liability. Therefore, GOTZEN and JANSSENS think that AI-generated copyright infringements do not need a regime distinct from the general principles of tort liability, at the moment.³⁰⁴

More generally, the issue of extracontractual liability for (autonomous) AI-systems has been the subject of many papers and studies, discussing the variety of existing regimes and drawing parallels to the liability for children, animals, defective things,... (art. 1382 etc. CCL).³⁰⁵ Another often-discussed regime in this regard is product liability (for a more detailed explanation, see part 3.2.4. – Liability for defective products).³⁰⁶ Part of the solution to this liability-conundrum may be the establishment of some kind of mandatory insurance for AI-systems, similar to the current mandatory insurance for motor vehicles. This should allow affected parties to easily obtain compensation, avoiding the need to identify the ultimate responsible party themselves.³⁰⁷ (For further information on insurance, see chapter 5 – Insurances.)

A final but specific topic in relation to intellectual property infringement is the possibility to apply for injunctions against intermediaries whose services are used by a third party to infringe on intellectual property rights.³⁰⁸ In the hypothesis of AI-systems generating and distributing infringing output, relevant intermediaries that can be addressed via such injunctions could be e.g.

³⁰¹ It is recalled that the European Parliament adopted a resolution in the meantime in which it clearly states that "in this connection, [...] it would not be appropriate to seek to impart legal personality to AI technologies and points out the negative impact of such a possibility on incentives of human creators". See: European Parliament Resolution, 2020/2015(INI), Intellectual Property Rights for the development of artificial intelligence technologies, 20 October 2020, §13

³⁰² Note that art. 2 Enforcement Directive states that its provisions apply "to any infringement of intellectual property rights" (own underlining), implying that rightholders need to be able to enjoy related measures, procedures and remedies also if the infringement is committed by an AI-system.

³⁰³ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p. 339.

³⁰⁴ F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p.339. On the other hand, they do foresee that e.g. the Enforcement Directive may have to be amended.

³⁰⁵ See for example: S. LOHSSE et al., *Liability for Artificial Intelligence and the Internet of Things*, Berlin, Nomos, 2019, 352 p.; J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort law and Damage Caused by AI Systems", in J. DE BRUYNE en C. VANLEENHOVE, *Artificial Intelligence and Law*, Antwerpen, Intersentia, 2021, p. 359-403; Expert Group on Liability and New Technologies, "Liability for Artificial Intelligence and Other Emerging Technologies", 2019, available at <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>. Also see further part 3.2.4.

³⁰⁶ J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort law and Damage Caused by AI Systems", o.c., p. 376-385.

³⁰⁷ European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL), para. 57-59; F. GOTZEN and M.-C. JANSSENS, "Kunstmatige Kunst – Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie", o.c., p.341

³⁰⁸ See art. 8.3 Infosoc Directive and art. XI.334, §1 CEL.

internet service providers or online and offline marketplace providers.³⁰⁹ It can, however, be envisaged that such intermediaries may be able to enjoy from the e-commerce exemptions, depending on the facts of the case (see parts 4.5.3. – Scope and intermediaries activities and 4.5.4. – Focus on liability exemption for hosting services).³¹⁰

4. Overview of the Identified Gaps

To conclude, we present a list of the gaps identified throughout the analysis. This overview follows the structure of the analysis and repeats some of its findings.

- IP-protection for AI-technology

Although AI-software may be eligible for copyright protection, the multiplicity of authors in a software programming context and the widespread use of open source software renders applying software copyright protection in practice not that evident.

With regard to the patentability of AI-systems, it was highlighted that there is already quite some guidance and case law, but that the application of the related principles in practice remains often unclear. It is asserted that only if (EPO) case law does not provide the necessary clarifications in due time, there may be a need for legislative intervention, whereby a harmonised solution at the international level is preferable.

In the context of assessing sufficiency of disclosure in the context of patentability, it could be useful to study the feasibility and usefulness of a deposit system (or similar legal mechanism) for AI algorithms and/or training data and models that would require applicants in appropriate cases to provide information that is relevant to meet this legal requirement, while including safeguards to protect applicants' confidential information to the extent it is required under EU or international rules.

- IP-protection for data

If data is used as a broad concept, possibly encompassing works, trademarks, designs,...., those respective protective regimes can apply to those 'data'. If data is used in a more strict meaning, limited to 'raw' data, there is no legal protection available except via database rights or trade secret protection (i.e. contractual limitations). No indications showing that there would be a genuine need to increase or extend the number of possible protection mechanisms for data were found.

The creation/obtaining distinction in the sui generis right remains a cause of legal uncertainty regarding the status of machine-generated data and could justify a revision or clarification of the rules on the sui generis database right.

- Copyright protection for AI-assisted/-generated output

Current copyright rules appear generally sufficiently flexible to deal with the challenges posed by AI-assisted outputs. There is, however, uncertainty concerning the elements that should be taken into account when determining the relative importance of an author's contribution vis-à-vis other authors and the AI-system.

Further empirical research into/monitoring of the risks of false authorship attributions by publishers of "work-like" but "authorless" AI productions (copyfraud), seen in the light of the general authorship presumption in Article 5 of the Enforcement Directive/art XI.170 CEL should be considered.

³⁰⁹ For offline market place providers: CJEU, 7 July 2006, no. C-494/15, ECLI:EU:C:2016:528, *Tommy Hilfiger Licensing LLC and others v Delta Center*, §30 and §37.

³¹⁰ Arts. XII.17-20 CEL.

Further empirical research into/monitoring of the role of alternative regimes to protect AI-generated outputs, such as trade secret protection, unfair competition and contract law, should be considered, taking into account that “authorless” AI-generated outputs will remain completely unprotected only in cases where no related right or sui generis right is available.

Related to the above and depending on the availability of strong economic arguments (which currently seem to be absent), it may be considered to attribute copyright to AI-generated works (to a certain extent) or establish a new sort of (statutory) protection.

- Sui generis/ related right protection for AI-assisted/-generated output

Further research into the extent related rights regimes potentially cover “authorless” AI-generated productions should be considered, similar to the rights available for audio recording, broadcasting, audio-visual recording, and news. In addition, the sui generis database right may offer protection to AI-generated/-assisted databases that are the result of substantial investment.

- Patent protection for AI-assisted/-generated output

Current patent law seems to be suitable to address the challenges posed by AI-technologies in the context of AI-assisted outputs. There is, however, uncertainty concerning the elements that should be taken into account when determining the relative importance of an inventor’s contribution vis-à-vis other inventors and the AI-system.

While the increasing use of AI-systems for inventive purposes does not seem to require material changes to the core concepts of patent law, the emergence of AI may have practical consequences for patent offices. Also, certain rules may in specific cases be difficult to apply to AI-assisted outputs and, where that is the case, it may be justified to make minor adjustments.

In the context of assessing novelty, patent offices should consider investing in maintaining a level of technical capability that matches the technology available to sophisticated patent applicants.

In the context of assessing the inventive step, it may be advisable to update the examination guidelines to adjust the definition of the PSA and secondary indicia so as to track developments in AI-assisted outputs and account for the related, potential elevation of the inventiveness-threshold.

For other challenges identified in this analysis arising in the context of AI-assisted inventions or outputs, it may be good policy to wait for cases to emerge to identify actual issues that require a regulatory response, if any. Related to the above and depending on the availability of strong economic arguments (which currently seem to be absent), it may be considered to attribute patent protection to AI-generated inventions (to a certain extent) or establish a new sort of (statutory) protection.

- Trademark/design protection for AI-assisted/-generated output

Current trademark law does not seem to prevent companies from using AI-systems to generate trademarkable signs or assist humans in designing such signs, while validly applying for those trademarks in name of the company, rather than indicating the AI-system as the applicant/proprietor. Should the AI-system itself be indicated as the applicant, it remains rather unclear what the outcome would/should be as trademark law does not feature a specific human-tailored actor, as opposed to the author or inventor from copyright/patent law.

As opposed to trademark law, protection under current design law implies some (creative) intervention from a human (i.e. the designer), similar to the situation in patent and copyright law. Likewise, AI-assisted designs should be able to enjoy design protection if they fulfil the validity requirement of novelty and individual character, while AI-generated designs will fall outside of the scope of design protection.

- Ownership of AI-generated output

Different categories of people involved in using AI-systems to produce creative or inventive output may stake a claim in the resulting intellectual property rights. Where copyright requires a decisive contribution in the originality of the work, patent law requires a substantial intellectual or creative contribution to the conception of the invention. What level of human intervention exactly constitutes a sufficient original and/or an inventive contribution may be tough to establish, given the wide spectrum of different types of AI and the difference between AI-assisted and AI-generated output. The black box nature of some AI- systems can further complicate matters. Currently, this will often require a case-by-case analysis. The other possibility is to not allocate ownership in AI-generated output and leave it to the public domain.

- Infringement of intellectual property rights

It can be expected that the development, training and use of AI-systems will trigger intellectual property infringements. In the course of the development and training phase of AI-systems, several exceptions may come into play depending on the actor involved. The most important remark in this regard is the limited scope of the TDM-exceptions in their current form. With regard to the output created by AI-systems, it is evident that if humans are involved in the creative process, those humans can incur liability if infringing material is indeed produced. Entirely autonomously generated infringing output presents more of an issue and relates to the larger discussion on extracontractual liability for damage caused by AI-systems. The hypothesis of infringing AI-assisted/-generated output may lead to further contentious matters, such as the role of fundamental rights in the context of intellectual property infringement, but it is too early to tell in which direction this will evolve.

CHAPTER 3 – CONSUMER AND MARKET (WP 3)

1. Introduction

AI challenges several traditional practices and principles of consumer protection law as well as competition law. Against this background, this chapter seeks to provide insights on how AI influences market structures and how competition law can regulate AI applications (part 2). It will also examine the impact of AI on consumer protection (part 3).

2. Competition Law (WP 3.1)

Once the applicable regulatory framework has been provided (part 2.1.) the study will analyse the impact of AI on competition (part 2.2.) as well as the influence on the structure and concentration of markets (part 2.3.). We will then proceed with an overview of AI-related competition issues (part 2.4.) and conclude with an overview of some gaps (part 2.5.).

2.1. Regulatory Framework

The main legal provisions regarding competition are included in the Treaty on the Functioning of the European Union (“TFEU”). Chapter 1 of the VII of the TFEU is the core regulation for competition. Two articles are of particular importance in this regard and constitute the starting point of the analysis.

Article 101 TFEU provides that:

1. The following shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market, and in particular those which:

(a) directly or indirectly fix purchase or selling prices or any other trading conditions;

(b) limit or control production, markets, technical development, or investment;

(c) share markets or sources of supply;

(d) apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(e) make the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

2. Any agreements or decisions prohibited pursuant to this Article shall be automatically void.

3. The provisions of paragraph 1 may, however, be declared inapplicable in the case of:

- any agreement or category of agreements between undertakings,

- any decision or category of decisions by associations of undertakings,

- any concerted practice or category of concerted practices,

which contributes to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefit, and which does not:

(a) impose on the undertakings concerned restrictions which are not indispensable to the attainment of these objectives;

(b) afford such undertakings the possibility of eliminating competition in respect of a substantial part of the products in question.

Article 102 stipulates that:

Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.

Such abuse may, in particular, consist in:

(a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions;

(b) limiting production, markets or technical development to the prejudice of consumers;

(c) applying dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage;

(d) making the conclusion of contracts subject to acceptance by the other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts.

Article 101 TFEU thus prohibits cartels and anti-competitive agreements. These are all agreements between companies that have as their object or effect the restriction of competition. Article 102 TFEU forbids any abuse of a dominant position by a company such as imposing unfair prices, unfair trading conditions or discrimination. Those legal rules have been transposed in the Belgian Code of Economic Law in the Articles IV.1 to IV.5.

It has already been mentioned that the EC issued a White Paper on AI in February 2020³¹¹ accompanied by a communication on a European Strategy for Data³¹² and a Report on the Safety and Liability Implication of AI.³¹³ The TFEU has been adopted long before the digital era. Therefore, it is important to identify the applicable competition law framework for AI-systems and, more importantly, determine whether those rules are sufficiently able to deal with the current and future challenges raised by AI.

The Commission is aware that the currently applicable legal framework is outdated and does not (adequately) address new (digital) evolutions. During the last years, for example, online platforms have risen in an unprecedented way and they are now playing an important role in digital markets. Against this background, the Commission issued a Proposal of a Digital Markets Act – DMA.³¹⁴ This Act addresses issues of competition and online platforms that are currently unregulated. The main purpose of the Act is to define the conditions for an actor to be qualified as a “gatekeeper”. Once a company is identified as such, the DMA imposes a set of obligations and prohibits certain unfair practices. These, for example, include the prohibition to discriminate in favour of own services, the obligation to ensure interoperability with its platform and the obligation to share, in compliance with privacy rules, data that is provided or generated through business users' and their customers' interactions on the gatekeeper's platform. In addition to those practices, gatekeepers

³¹¹ European Commission, “White Paper on artificial intelligence – A European approach to excellence and trust”, o.c.

³¹² European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data”, Brussels, 19 February 2020, COM(2020) 66 final available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

³¹³ European Commission, “Report from the Commission to the European Parliament, the Council, and the European Economic and Social Committee: Report on the safety and liability implication of artificial Intelligence, The Internet of Things and Robotics”, Brussels, 19 February 2020, COM(2020) 64 final, available at https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf.

³¹⁴ European Commission, “Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)”, COM/2020/842 final, 15 December 2020.

will continue to offer new and innovative services as they have always done but without taking advantage of unfair behavior.³¹⁵ The DMA Proposal shows the Commission's intent to update the legislation in order to provide an adequate and improved framework for the behavior of new market players. However, the DMA Proposal is only at the proposal stage and is not yet final.

2.2. The Influence of AI on Competition

AI can have a positive effect on competition as it can result in both static and dynamic efficiencies.

First, companies are always seeking for the 'next best thing' to increase the quality of their product or to reduce the cost of their production. With the emergence of big data and data mining algorithms, it is easier for companies to better comprehend the consumers' preferences and adapt their offer and strategies accordingly.³¹⁶ The use of predictive analytics enables firms to create a product that suits the consumer's interests and needs. Data can also enable companies to better target customers and anticipate trends before they even occur³¹⁷. The incorporation of AI-systems in the supply chain also allows for savings. The company will rely on AI-systems if it is deemed profitable after a cost-benefit analysis. This will result in the reduction of expenses for the company.³¹⁸

Consumers will be offered products of better quality that fit their interests. Moreover, the reduction of the production cost can be translated into a reduction of the purchase price for the consumer. Other AI-applications can be used by consumers to facilitate their purchasing decisions (i.e. search engines, recommendation of products or price comparators). Those digital tools eventually help consumers making the most rational choice.³¹⁹

Finally, there is no doubt that AI may foster innovation. Considering that AI has capacities exceeding human abilities, AI allows for more innovation. What was deemed impossible a few years ago is now becoming possible by using AI. Artificial intelligence is able to do what human can but in a faster, more efficient and cheaper way. Moreover, AI can also be self-learning and act independently from any human intervention. Innovation is beneficial for the consumer as well as for competition itself.³²⁰

In digital markets which are characterised by a high concentration, innovation is a very effective mean to challenge the established balance of powers.³²¹ Big data and data-based skills result in the market being more transparent. Therefore, a company is able to compare its own offer to the ones available on the same market. As such, companies have an incentive to stand out from competitors and innovation is an effective way to do it. Companies are under constant pressure to innovate. For that reason, they have incentives to develop non-traditional products or services that will appeal to consumers.³²²

³¹⁵ Europe fit for the Digital Age: new online rules for platforms, available at https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-platforms_en.

³¹⁶ See Y. POULLET, "Titre 1 - Le phénomène de l'IA, son intérêt et ses acteurs", in *Le RGPD face aux défis de l'intelligence artificielle*, Bruxelles, Éditions Larcier, 2020, p. 15-46.

³¹⁷ I. FORRESTER, "Disruptive innovation and implications for competition policy", EUI Working Papers LAW 2018/14, 2018, p. 10.

³¹⁸ For example, see C. WONG, Z.X. GUO and S.Y.S LEUNG, "Fundamentals of artificial intelligence techniques for apparel management applications, in *Optimizing decision making in the apparel supply using artificial intelligence : from production to retail*, Woodhead Publishing, 2013, p. 13.

³¹⁹ OECD, "Algorithms and Collusion: Background Note by the Secretariat", 9 June 2017, DAF/COMP(2017)4, p. 13 available at <http://www.oecd.org/competition/algorithmscollusion-competition-policy-in-the-digital-age.htm>.

³²⁰ G. GURKAYNAK, "Competition Law Consequences of Artificial Intelligence", in *The Academic Gift Book of ELIG, Attorneys-at-Law in Honor of the 20th Anniversary of Competition Law Practice in Turkey*, March 2018, p. 303.

³²¹ P. I. COLOMO, "Restriction on Innovation in EU Competition Law", LSE Working Papers, n°22, 2015, p. 17.

³²² G. GURKAYNAK, "Competition Law Consequences of Artificial Intelligence", o.c., p. 301-302.

These evolutions may eventually converge towards the rise of disruptive innovation. Disruptive innovation “introduces a different package of attributes from the one that customers historically value. However, those attributes may not all surpass those the traditional product has but adds values enough of the old features that consumers still need and draw attention to them”.³²³ To qualify an innovation as being disruptive, the size of the leap that the innovation represents is irrelevant. Breakthrough innovations are not necessarily disruptive. Disruptive innovation is a manner of penetrating the value network. The disruptive product or service will appeal to consumers because of its added value. At that stage, clients do not see the product as a substitution for the product of the value network. Therefore, companies established in the value market do not feel threatened in first instance. But at some point, however, the disruptor will unexpectedly set a foothold into the value network.³²⁴

2.3. The Impact of AI on the Structure and Concentration of Markets

In the following parts, the influence of AI on the structure and concentration of markets is examined. This in the first place implies an analysis on how data can have a competitive advantage (part 2.3.1.) followed by an examination as to how AI may increase market concentration (part 2.3.2.). It will also be assessed how the use of AI affect transparency (part 2.3.3.).

2.3.1. Data as a Competitive Advantage

The strategies of companies can be based on predictions made by algorithms. Those algorithms are fed and trained with data. In other words, the functioning of AI is only possible if the company possesses the fundamental requisite input, namely data. The quality of the data collection, which depends on four factors (i.e. volume, veracity, variety, velocity), will determine the accuracy of the predictions.³²⁵

Data constitute a competitive advantage for companies. Even if data are non-exclusive, non-ubiquitous and non-rivalrous, the accumulation of data may itself be a competitive advantage. Moreover, data have their own feedback effect. This means that the more data owned by the company, the more accurate it's AI predictions will be. This in turn will allow the company to attract more customers. With more clients, the company will be in a position to collect more data which can be used again to improve the predictions. A company benefiting from market power will thus maintain its dominance via an ongoing collection of data. Consequently, it is challenging to dethrone the market leader. In addition, there is no level playing field for companies wishing to be active on the market. Data may create a market entry barrier for potential competitors that do not benefit from the competitive advantage resulting from a critical mass of data. Data can thus be used as a tool for companies to outperform competitors. The DMA Proposal imposes an obligation

³²³ H.-F. WEI, “Does Disruptive Innovation “Disrupt” Competition Law Enforcement? The Review and Reflection”, 30 December 2016, p. 5 available at <https://www.ftc.gov.tw/upload/636d4e6f-2570-4b26-b746-d0904c18e2db.pdf>.

³²⁴ See J. DREXL, “Anti-competitive stumbling stones on the way to a cleaner world: Protecting competition in innovation without a market”, Max Planck Institute for Intellectual Property and Competition Law Research Paper, n°12-08, 2012, p. 4; C.M. CHRISTENSEN, M. E. RAYNOR, and R. MCDONALD, “What Is Disruptive Innovation?”, *Harvard Business Review*, December 2015, available at <https://hbr.org/2015/12/what-is-disruptive-innovation>; J.L. BOWER and C. M. CHRISTENSEN, “Disruptive Technologies: Catching the Wave”, *Harvard Business Review*, January-February 1995, available at <https://hbr.org/1995/01/disruptive-technologies-catching-the-wave>; H.-F. WEI, “Does Disruptive Innovation “Disrupt” Competition Law Enforcement? The Review and Reflection”, 2016, p. 5 available at <https://www.ftc.gov.tw/upload/636d4e6f-2570-4b26-b746-d0904c18e2db.pdf>; T. SCHREPEL, “Chapitre 2 - L'innovation de rupture: de nouveaux défis pour le droit de la concurrence”, in *L'innovation prédatrice en droit de la concurrence*, Bruxelles, Bruylant, 2018, p. 108- 113; A. DE STREEL and P. LAROUCHE, “Disruptive Innovation and Competition Policy Enforcement”, OECD DAF/COMP/GF(2015)7, p. 4-9.

³²⁵ E. CALVANO and M. POLO, “Market Power, Competition and Innovation in Digital Markets: A Survey”, *Information Economics and Policy* 2019, p. 15.

on gatekeeper to share its data under certain circumstances. This measure clearly illustrates that the European legislator is aware of the importance of data and their competitive advantage.³²⁶

Although the DMA Proposal seems to provide interesting proposals of solutions, it should not be overestimated. The data sharing and interoperability obligations are only imposed in specific situations and does not solve every problem identified in relation with data.³²⁷

One way of acquiring data is through mergers. For this reason, competition authorities cannot overlook the consequence of a concentration of data when assessing merger operations. For this reason, the Commission should pay extra attention to the accumulation of data within competitors.³²⁸ The merger considered between two Big Data companies must trigger the alarm bell and lead to closer scrutiny by the Commission that must take data into account in its merger assessment.³²⁹

When analysing a merger proposal, the Commission assesses the concentration of market power by looking at the market shares and other factors such as imminent entry of competitors or consumer bargaining power. The goal is to examine if, after the merger, there will still be competitive pressure on the merged entity. If the merger seems anti-competitive, the parties can then demonstrate that the merger also creates positive effects which can make up for the negative ones.³³⁰ EU competition law is traditionally based on a static approach focusing on how the merger will modify the structure of the relevant market and change market power. This neoclassic static test is well-suited for a control solely based on price competition.³³¹ The data owned by the firm does not intervene in the measurement of market power. In the era of big data, data and data-linked skills are significant competitive advantages and critical resources required to innovate in the high-tech industry.³³² Given the importance of data, it must be taken into account when assessing the undertaking's market power.³³³

2.3.2. Concentration

The use of AI may also increase market concentration. The most affected sectors are online and digital markets. These are the ones most frequently relying on AI. Those markets are already characterized by their high concentration. Indeed, those markets are often considered 'winner takes all' markets in which the competition occurs *for* the market and not *in* the market due to network effects. The digital sector is thus a competitive environment in which direct and indirect network effects play a major role. On the one hand, the direct network effect implies that a product becomes more valuable and attractive for consumers when it is increasingly used/bought.

³²⁶ European Commission, "The Digital Markets Act: ensuring fair and open digital markets", available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

³²⁷ See Centre on Regulation in Europe (CERRE), "The European proposal for a digital markets act: a first assessment", Assessment Paper, January 2021.

³²⁸ E. ARGENTESI, P. BUCCIROSSI, E. CALVANO, T. DUSO, A. MARRAZZO and S. NAVA, "Merger Policy in Digital Markets: An Ex-Post Assessment", Deutsches Institut für Wirtschaftsforschung Discussion Paper, 2019, p. 11.

³²⁹ See M. BOURREAU and A. DE STREEL, "Big tech acquisitions: competition and innovation effects and EU merger control", CERRE, issue paper, February 2020.

³³⁰ M.L. KATZ and H.A. SHELANSKY, "Merger Policy and Innovation: Must Enforcement Change to Account for Technological Change?", in A. B. JAFFE, J. LERNER and S. STERN (eds.), *Innovation Policy and the Economy*, The MIT Press, 2005, p. 120.

³³¹ W. KERBER, "Competition, Innovation, and Competition Law: Dissecting the Interplay", MAGKS Joint Discussion Paper Series in Economics, n°42-2017, 2017, p. 4.

³³² M.E. STUCKE and A.P. GRUNES, "Big Data and Competition Policy", Oxford, Oxford University Press, 2016, p. 8, available at: https://www.researchgate.net/publication/308970973_Big_Data_and_Competition_Policy.

³³³ In the *Microsoft/LinkedIn* case, the combination of data was only a secondary concern while in *Google/DoubleClick*, the Commission looked into the potential foreclosure based on the combination of Google and DoubleClick's datasets. Commission decision of 6 December 2016, M.8124, *Microsoft/LinkedIn*, § 339; Commission decision of 11 March 2008, COMP/M.4731, *Google/DoubleClick*, §. 359.

The indirect network effect, on the other hand, typically occurs in multisided platforms in which the increase of users on one side of the platform boosts the value that a distinct group of actors places on joining that same platform. Network effects can raise entry barriers to a point where it has a foreclosing effect because it prevents competitors to enter the market. In the end, companies are competing to be the first ones acquiring certain market power. Once this threshold is reached, it will be hard to challenge the dominant company.³³⁴

The emergence of big data and AI has the consequence that market actors compete for data obtained from the consumers. One indication is the widely adopted method referred to as the so-called 'free of charge for the consumer' model. It illustrates that the monetary side is often not decisive. In reality, the ultimate goal is to attract a large number of users through a zero-price policy. Once this is done, the firm may either directly sell the user's data to advertisers or use the data to improve its product and keep its customers. In sum, the starting point of the value chain is data and AI.³³⁵

2.3.3. Transparency

The proliferation of data and the development of AI-systems able of processing data increase the transparency in a market. Actors possessing these resources can have a proper and better understanding of the consumer's expectations as well as of a competitor's behavior. Although transparency may be a positive factor, it also facilitates the anti-competitive conduct by a company. AI increases the transparency of marketplaces. As a result, the undertakings active on the market are able to improve their decision-making process. In this regard, "[i]t is widely recognized that algorithms, by virtue of their self-learning nature, their ability to find patterns and to create data trends, are tools that assist business operations and also generate and improve commercial strategies more efficiently than ever. As a matter of fact, by using patterns and data trends, suppliers are able to respond more rapidly than ever to their customers' needs, which results in significant improvements in the allocation of resources, and thus lowers production costs and generates supply-side efficiencies. In turn, this supply-side efficiency allows companies to lower their prices, and therefore leads to the creation of consumer welfare".³³⁶

2.4. AI-Related Competition Issues

Companies consider the growing aptitudes of AI as promising tools. Today, companies (already) use commercial AI-applications for a variety of reasons. The progress and forecast that AI provides for economic actors and for society as a whole, however, comes with great risks. The fundamental question is whether these risks can be prevented and mitigated by the applicable legal framework. Although not only competition law should prevent those risks, it may enable competition authorities to hold someone liable when a company resorts to AI capable of making an independent decision.³³⁷

Two major risks related to, for instance, the use of pricing algorithms are algorithmic collusion on the one hand (part 2.4.1.) and price discrimination on the other hand (part 2.4.2.). As AI-technologies are continuously improving, a growing number of companies are relying on AI and algorithmic pricing to make commercial decisions. Pricing algorithms are algorithms capable of autonomously setting the prices of goods offered by a company.³³⁸ Those algorithms will fix prices

³³⁴ P.I. COLOMO, "Restriction on Innovation in EU Competition", o.c.

³³⁵ E. CALVANO and M. POLO, "Market Power, Competition and Innovation in Digital Markets: A Survey", o.c.

³³⁶ G. GURKAYNAK, "Competition Law Consequences of Artificial Intelligence", o.c., p. 301-302.

³³⁷ K. GARYALI, "Is the competition regime ready to take on the AI decision maker ?", CMS Law available at <https://cms.law/en/gbr/publication/is-the-competition-regime-ready-to-take-on-the-ai-decision-maker>.

³³⁸ N. PETIT, "Algorithmes tarifaires et droit européen de la concurrence", in *L'Europe au présent!*, Bruxelles, Bruylant, 2018, p. 167.

after considering various factors such as the supply, the demand, the anticipated trends, the consumer's preferences and the competitors' prices. Moreover, as soon as some companies rely on those technologies, they benefit from a more efficient decision-making process³³⁹. Consequently, other firms will be tempted to acquire that technology as well to stay in the market and sustain the competitive pressure.

2.4.1. Collusion by Algorithms

The notion of a collusion commonly refers to “any form of coordination or agreement among competing firms with the objective of raising profit to a higher level than the non-cooperative equilibrium”.³⁴⁰ The collusion can result either from an explicit oral or written agreement or from a tacit one. A tacit collusion refers to the situation in which the companies that are involved in the collusion are interdependent but have not made an explicit agreement to create such interdependence. At that stage, it is important to make a *summa divisio* between the two ways in which companies can deploy AI. On the one hand, the role of the algorithms can be to facilitate the anti-competitive conduct in which companies are taking part. In such a case, the reliance on AI is (merely) aiding collusion (part A.). The use of algorithms by itself can, on the other hand, also create a new threat to competition (part B.). The interaction of algorithmic pricing agents may result in a situation that is detrimental to competition. This outcome can arise even without any human intervention.³⁴¹ The applicable framework (part C.) as well as the attribution of liability (part D.) are also examined.

A. The Use of AI to Facilitate Collusion

In order to be viable, a collusive agreement needs to fulfil three conditions. Firstly, the companies must agree on a common policy that they all have to adhere to. This means that in the context of pricing algorithms, companies will align their pricing strategies by determining a focal point. Secondly, the companies involved in this arrangement must be able to monitor the other's behaviour to control that each and every company sticks to the agreed common policy. Finally, companies must be able to punish the participant that deviates from the focal point.³⁴²

Tacit collusion was a concept rarely encountered in practice. Indeed, it is very difficult to achieve tacit collusion between humans. Artificial intelligence facilitates this practice.

When AI is used to aid collusion, “[t]he algorithms are mere ‘intermediaries’ to the ‘per se’ illegality of the agreed upon-actions of the human agents”.³⁴³ Nowadays, we observe multiple companies operating in the same market. Each of these companies offers heterogeneous products and services at different prices. It means that there is much information to take into account when companies want to enter into an agreement. It is also harder to monitor compliance with the agreement among a large number of participants.

Algorithms assist humans to negotiate and enforce the agreement. Artificial intelligence is able to find the focal point and dissuade participants from deviating from this equilibrium. The common policy of collusive companies can be found by the algorithm itself. For example, companies can rely on the same person to conceive their pricing algorithm. Those firms will *in fine* thus use parallel algorithms. Companies can also rely on algorithms to spot the unilateral modification by a

³³⁹ G. GURKAYNAK, “Competition Law Consequences of Artificial Intelligence”, o.c., p. 294-295.

³⁴⁰ OECD, “Algorithms and Collusion: Background Note by the Secretariat”, o.c., p. 17.

³⁴¹ *Ibid*, p. 5.

³⁴² *Ibid*, p.17.

³⁴³ N. SINGH, “Virtual competition: Challenges for Competition Policy in an algorithm driven market”, 11 September 2018, available at: <http://competitionlawblog.kluwercompetitionlaw.com/2018/09/11/virtual-competition-challenges-competition-policy-algorithm-driven-market/>.

competitor who wishes to signal to others its willingness to collude.³⁴⁴ Computing power has no problem dealing with a large amount of real-time information. Based on that information, a monitoring algorithm can find a focal point, detect when a participant deviates from it and trigger immediate retaliation.

B. Collusion Solely Achieved by Algorithms

Tacit price collusion, in economic literature, occurs “when there is no express coordination or agreement between firms, but they recognise competitive behaviour in the market and change their strategies accordingly”.³⁴⁵ AI and self-learning algorithms may also allow for the alignment of prices between companies without the implementation of any explicit agreement (tacit collusion) nor of any human instructions to do so³⁴⁶. In such a scenario, competition authorities cannot attribute the infringement of competition law to any executive of the company as algorithms reach the anti-competitive equilibrium without any human person even being aware of it.

C. Applicable Competition Law Regulations

Collusion, either explicit or tacit, is prohibited under Article 101 TFEU. The question already arose to which extent Article 101 TFEU, which is traditionally dealing with anti-competitive agreements, is an appropriate tool to prevent algorithmic collusion. On the one hand, when algorithms are used to implement traditional anti-competitive agreements and facilitate their enforcement, Article 101 TFEU is fully applicable. A major challenge for competition authorities is then to understand the (proper) functioning of AI-systems and how these aid the implementation of the agreement. On the other hand, the application of the TFEU to collusion achieved without human intervention is more controversial. Indeed, there are limitations to the extent to which the TFEU is relevant to tackle those collusions. We address those limitation below.

The concepts used in Article 101 TFEU constitute an obstacle to its application to algorithmic collusion. In order to be applicable, Article 101 TFEU requires competition authorities to detect an agreement or at least, when no formal agreement has been taken, detect concerted practices between competitors. Despite the lack of definition in the TFEU, case law requires “a concurrence of wills”³⁴⁷ or “concordant intentions from both parties of the agreement”.³⁴⁸ When companies rely on pricing algorithms, however, they can reach an agreement without any contact taking place between them.

Anti-competitive practices prohibited by Article 101 TFEU is also possible without any contact between companies. It occurs when a company makes unilateral price modifications as an indication for competitors of its willingness to collude. Competitors receiving that indication will have to follow such behaviour to express their adherence to the pricing strategy.³⁴⁹ Despite the fact that contact is not a requisite for an infringement of Article 101 TFEU, the mere finding that several companies adopt a similar pricing strategy cannot, by itself, demonstrate the existence of an agreement between them. Indeed, market conditions may justify that companies have rationally decided to act in such a way without any intention to distort competition. This case law is understandable as it would make little sense to reproach a company making rational choices after considering the market conditions. Nonetheless, this cases law makes it challenging to reveal tacit

³⁴⁴ OECD, “Algorithms and Collusion: Background Note by the Secretariat”, o.c., p. 27-28.

³⁴⁵ M. ZAMINDAR and P. MUCHHALA, “Artificial Intelligence and Market Regulation: The Way Forward for the CCI”, *The RMLNLU Law Review Blog*, 17 July 2020 available at <https://rmlnlulawreview.com/2020/07/17/artificial-intelligence-and-market-regulation-the-way-forward-for-the-cci/>.

³⁴⁶ See E. CALVANO, G. CALZOLARI, V. DENICOLO and S. PASTORELLO, “Artificial intelligence, algorithmic pricing and collusion”, December 2019, available <https://ssrn.com/abstract=3304991> or <http://dx.doi.org/10.2139/ssrn.3304991>.

³⁴⁷ Case T-41/96, *Bayer AG v Commission*, 26 October 2000, ECR II-3383, §173.

³⁴⁸ N. PETIT, “Algorithmes tarifaires et droit européen de la concurrence”, o.c., p. 169.

³⁴⁹ Case AT.39850, *Container Shipping*, 7 July 2016, C(2016) 4215, §§37-39.

collusion when the collusive equilibrium reached is the sole result of self-learning algorithms' functioning.

Another possibility would be to consider that companies using algorithms to align their pricing strategies would be qualified as a collective dominant position. In that way, competition authorities could rely on the prohibition under Article 102 TFEU to restrict this behavior. A collective dominant position refers to the situation in which "from an economic point of view, several firms present themselves or act together on a specific market, as a collective entity".³⁵⁰ The company using algorithms to collude would constitute a single economic entity. However, the application of Article 102 TFEU requires companies to have a position of market dominance and that they abuse that established market power.

D. The Attribution of Liability

If competition authorities decide that algorithmic collusion constitutes a violation of the TFEU, the question will eventually be who to held liable for it. In case undertakings rely on AI to negotiate, monitor or enforce an agreement already entered into by the company's executives, competition authorities may forbid this behaviour. Indeed, Article 101 TFEU applies conventionally and the companies involved in the agreement will be held liable for infringing competition law.³⁵¹

When a decision is taken by algorithms acting independently from any human instruction, the question of liability is more challenging. To avoid impunity, responsibility should be attributed to the company that has deployed the algorithms or to the manufacturer of the algorithm. Note, however, that imposing liability for parties involved in the AI supply chain (e.g. producer of software,...) is not straightforward. Several challenges exist under the Product Liability Directive such as the question whether software can be qualified as a product or when an AI-system is defective. The problem is also that self-learning algorithms are by nature unpredictable. Imposing liability upon the seller of the AI-technology or the company using that technology may thus result in someone being held liable for something that was impossible to foresee. Liability has to be assessed on a case-by-case basis by considering whether, in light of the facts at hand, "any illegal action could have been anticipated or predetermined by the individuals who benefit from the algorithm".³⁵²

However, the question of the attribution of liability is a general question raised by the use of AI and not an issue specific to competition law. This has been expressed by Margrethe Vestager in a 2017 speech when she said that "so as competition enforcers, I think we need to make it very clear that companies can't escape responsibility for collusion by hiding behind a computer program (...) They may not always know exactly how an automated system will use its algorithms to take decisions. What businesses can – and must – do is to ensure antitrust compliance by design. That means pricing algorithms need to be built in a way that doesn't allow them to collude. Like a more honourable version of the computer HAL in the film 2001, they need to respond to an offer of collusion by saying "I'm sorry, I'm afraid I can't do that".³⁵³

2.4.2. Personalised Pricing

The second major anti-competitive practice that is made possible by using AI is price discrimination. In the past, companies generally adopted a single price strategy, whereby every customer could purchase the same product at a same price. This is typically what happens in 'brick-

³⁵⁰ N. PETIT, "Algorithmes tarifaires et droit européen de la concurrence", o.c., p.171.

³⁵¹ G. GURKAYNAK, "Competition Law Consequences of Artificial Intelligence", o.c., p. 296-297.

³⁵² OECD, "Algorithms and Collusion: Background Note by the Secretariat", o.c., p. 38.

³⁵³ M. VESTAGER's speech on algorithms and competition, 16 March 2017.

and-mortar' shops. Once we have discussed how AI can be used to set up personalised pricing (part A.), the applicable regulatory framework will also be discussed (part B.).

A. The Use of AI to Set up Personalised Pricing

With the evolution of commercial techniques, companies are given the possibility to easily adapt the prices depending on the state of the market. This is called "dynamic pricing". It refers to the practice of "adjusting the prices to change in demand and supply often in real time not implying any kind of discrimination between consumers".³⁵⁴ When the change in prices is based on factors such as the stock available or the demand, AI only facilitates optimal and rational decision-making by the companies. Those decisions could have been made less efficiently but (still) without the use of AI and prices changed manually. Yet, AI can be used as a facilitator when it monitors the market's conditions and automatically adjusts prices.

Nowadays, with the emergence of big data and the development of algorithms able of processing a huge quantity of data, companies cannot only anticipate which good consumers could be interested in but also obtain information regarding the value they attach to that specific good. If companies are able to predict the maximum price that each potential customer is willing to pay for a specific good, they can align their prices accordingly. Algorithms allow for the processing of a large volume of data, the deduction of customer's willingness to pay and the instant adaptation of prices on that basis.³⁵⁵

On the one hand, if companies apply a single price policy, some consumers may be underserved.³⁵⁶ With personal pricing, a particular good is available to each consumer at the price he/she was willing to pay for it. "Firms collect extensive consumer data online and use pricing algorithms to engage in so-called "perfect price discrimination". This behaviour consists in charging each consumer his or her exact willingness to pay, enabling the firm to capture the entire consumer surplus. While perfect price discrimination has been considered a highly theoretical concept, it is not unconceivable that new technologies can at least enable firms to estimate consumers' willingness to pay and to charge prices accordingly"³⁵⁷.

Companies will only provide the good at the reserve price - that is the highest price a buyer is willing to pay for the good - if the reduction of the price for low-end consumers is compensated by the increase of the price for high-end customers. In this scenario, low-end customers are the ones that would not be able to afford the good if it were provided at the single price. By contrast, the high-end consumers are the consumers who were willing to pay a higher price than the single price to obtain the good. In the end, some people who could not buy the good at a single price benefit from a lower price as a result of price discrimination (low-end customers). For those who were willing to pay more than the single price, they will have access to the good at a higher price in a situation of price discrimination (high-end customers).

On the other hand, personal pricing creates a perception of unfairness among consumers. This may result in the loss of consumer trust in companies relying on AI. That is because "[p]ersonal pricing can essentially be seen as a form of price discrimination in which individual consumers are charged different prices based on their personal characteristics and conduct. Personalised pricing thus results in consumers paying each a different price, generally as a function of their willingness to pay, with implications for consumer welfare".³⁵⁸ The degree of discrimination depends on the

³⁵⁴ OECD, "Personalised pricing in the Digital Era: Background note by the Secretariat", 12 October 2018, DAF/COMP(2018)13, p. 9 available at [https://one.oecd.org/document/DAF/COMP\(2018\)13/en/pdf](https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf).

³⁵⁵ N. PETIT, "Algorithmes tarifaires et droit européen de la concurrence", *o.c.*, p. 168.

³⁵⁶ OECD, "Personalised pricing in the Digital Era: Background note by the Secretariat", *o.c.*, p. 5.

³⁵⁷ *Ibid.*

³⁵⁸ *Ibid.*

volume of data available to the firm. The more data a company possess, the more accurate its estimation of the consumer's willingness to pay will be. By using AI, firms do not only access the data freely provided by consumers but also observed and inferred data. As a result, it is easier to estimate the precise willingness of consumers to pay and proceed to perfect discrimination.

In addition to the availability of data, personal pricing is only possible if buyers cannot resell the goods to one another party otherwise consumers benefiting from low prices would buy and resell to others.³⁵⁹

B. Current Competition Law Legislation

When it comes to personalized pricing in competition law, the relevant provisions are included in Article 102 TFEU forbidding any abuse of dominance. A company has a dominant position when it detains market power enabling it to behave independently from its competitors. The mere fact that a company has market power, however, is itself not illegal. A competition authority will have to assess whether a company uses such position of power to engage in anti-competitive practices. The abuses can be either exclusionary (i.e. when its purpose is to remove a rival from the market) or exploitative (i.e. when its purpose is to harm consumers). Either way, the practice must fit one of the categories of abuses listed in Article 102 TFEU.³⁶⁰

Finally, in order to conclude in an infringement of Article 102 TFEU, competition authorities should make a balance between the positive and negative effects of a company's conduct on competition. Abuse of dominance could still be accepted to the extent that it brings static or dynamic efficiencies that have countervailing effects. It has been proven difficult to qualify the practice in which companies rely on AI to infer the consumer's willingness to pay and align their prices accordingly as an abuse contained in Article 102 TFEU.³⁶¹

Despite the fact that Article 102 TFEU explicitly lists discrimination as an abusive practice,³⁶² the TFEU uses terms that will restrict its application to AI. The Article only refers to the discrimination by a company's towards its trading partners, and not towards consumers. The only way in which personalized pricing would enter that type of abuse is if it is part of a predatory pricing strategy of the dominant firm. The firm would charge less to a competitor's consumers to capture them and the competitor would not be able to align its prices without incurring losses.

If the abuse of discrimination cannot be applied, personalized pricing could be considered as an exploitative abuse because it harms consumers. Consumers who pay more are at a disadvantage compared to those who pay less. In order to do that, one must demonstrate that personalized pricing constitutes excessive or unfair pricing. Indeed, it results in high-end consumers being charged a higher price that cannot be justified by a differentiation in the cost of providing those consumers with that good.³⁶³

This situation was analysed in the *Asnef Case*.³⁶⁴ Although this case dates from before the digital age, it concerns an exchange of data between undertakings. As such, the insights gained from this case may be relevant. In the case, the sharing of data between banks allowed the latter to apply higher rates for loans granted to persons profiled as "bad payers". This case eventually made it to the Court of Justice that held that, in order to judge whether a price is excessive under competition law, "it is the beneficial nature of the effect on all consumers in the relevant markets that must be

³⁵⁹ *Ibid.*, p. 13.

³⁶⁰ *Ibid.*, p. 28; Art. 102 TFEU.

³⁶¹ *Ibid.*

³⁶² TFEU, Art. 102, c).

³⁶³ OECD, "Personalised pricing in the Digital Era: Background note by the Secretariat", o.c., p. 26-28.

³⁶⁴ Case C-238/05, *Asnef-Equifax v. Asociación de Usuarios de Servicios Bancarios (Ausbanc)*, ECLI:EU:C:2006:734.

taken into consideration, not the effect on each member of that category of consumer”.³⁶⁵ From that case law, we understand that discriminatory pricing will only be considered an exploitative abuse if it diminishes consumer welfare in general. It is therefore not sufficient that some consumers pay more due to the personalised prices. Article 102 will only apply if the discrimination allows the supplier to appropriate all the surplus to the exclusion of consumers.³⁶⁶

2.5. Overview of the Identified Gaps

There is no doubt that the widespread integration of artificial intelligence into business practices is beneficial on various levels. The generalised use of algorithms by undertakings allows for a more efficient decision-making process and business models and encourages innovation. However, the use of AI by undertakings fundamentally modifies market conditions (i.e. the importance of data, transparency, concentration, high frequency trading, automated price adjustments,...). More importantly, firms might use AI to indulge in anti-competitive practices. Those new risks are inherent to the rise of AI and should not be disregarded. As established above, AI facilitates certain potentially anti-competitive behaviours.

Competition law is based on rules issued at the European level. These rules must provide the answers to the risks generated by the use of artificial intelligence. It is true that, as explained above, European competition law rules were made before the digital age. These rules may, therefore, appear obsolete when faced with the current challenges posed by artificial intelligence. However, this does not mean that an overhaul of European rules is necessary. Competition law is flexible enough to adapt to those new challenges. The current wording does not address current technologies, but it is not impossible to remedy this without changing the whole applicable regime. Indeed, it would be sufficient to adopt guidelines that would encourage a more extensive interpretation of the current rules in order to bring new technologies within their scope. At the very least, situations in which algorithms are used by undertakings to facilitate anti-competitive practices must enter the scope of competition law and be prohibited. Another solution is to edit specific rules, applicable to algorithms and the way they function. However, when it comes to competition law, there are permanent concerns that the introduction of additional rules might end up having a result it was not intended to. If a new regulatory framework is introduced, the negative and the positive effects that it could have must be assessed. Although there are gaps in the enforcement of the current competition rules when it comes to AI, over-regulation is not desirable either.

Finally, it must be recalled that there are no empirical data to this date providing evidence of such anti-competitive behaviour achieved solely by the functioning of algorithms, without any human intervention. Nevertheless, the constant evolution of technologies does not rule out that possibility in the future.

Against this background, the following points are also relevant and will be covered in the following studies.

- The sharing of data (although addressed in the DMA Proposal) but in need for a final legislative framework.
- The qualification of both the collusion made solely by algorithms and the price discrimination against consumers as infringements of competition law.
- The attribution of liability when the infringement of competition law is made by the use of AI without any human intervention.

³⁶⁵ *Ibid.*, § 70.

³⁶⁶ OECD, “The regulation of personalised pricing in the digital era - Note by Marc Bourreau and Alexandre de Stree”, 21 November 2018, DAF/COMP/WD(2018)150, p. 8, available at [https://one.oecd.org/document/DAF/COMP/WD\(2018\)150/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)150/en/pdf).

3. Consumer Protection (WP 3.2)

3.1. Introduction

This part of the study focuses on the application of consumer protection rules in the Belgian legal order³⁶⁷ to AI-systems.³⁶⁸ In this regard, the study considers the applicable legal rules from two different perspectives. Firstly, consumer protection rules are analysed in the case where they apply to AI as the object of the contract concluded between an undertaking and a consumer (part 3.2.). Secondly, consumer protection rules are examined in the case where AI is used to conclude a contract with a consumer (part 3.3.). It should also be kept in mind that AI-technology can also be used to contribute to consumer protection. For instance, public authorities might develop and deploy AI-tools to automatically detect a wide range of commercial practices which are forbidden by consumer protection law and/or to automate the issuance of warnings to undertakings that behave illegally. Although this is not the focus of the study, it seems relevant to highlight such potential uses of AI in this part as well.

3.2. AI is the Object of the Contract

In this first part, the application of consumer protection rules to AI is analysed in the following hypothesis: a consumer³⁶⁹ concludes a contract with an undertaking³⁷⁰ which has AI as its object. This hypothesis potentially covers a wide number of situations and legal qualifications as such contracts could bear on goods,³⁷¹ services,³⁷² products³⁷³ or digital content.³⁷⁴

For instance, AI could be encompassed within a material good such as a robot and sold with its material container. An undertaking could also use AI to provide services in an automated manner. For example, an undertaking could provide AI integrated in a mobile phone application, as a personal assistant, to its consumers. In both cases, AI-systems would qualify as products, which notion encompasses goods and services, but also rights and obligations. In addition, the notion of digital content relates to “data which are produced and supplied in digital form”,³⁷⁵ which leaves no doubt on the fact that it includes AI.

As a preliminary remark, it should be noted that in addition to the rules studied in this part, sector-specific rules may also apply depending on the purposes/sectors for which AI-systems are designed and marketed (be it by their producers or by subsequent actors in the supply chain) or used by consumers. For instance, the rules contained in Book VII of the Code of Economic Law regarding payment services could apply if an undertaking uses AI to provide its payment services

³⁶⁷ The study analyses Belgian consumer protection laws, where such rules exist. In case no Belgian laws exist (yet), EU rules are analysed instead. As Belgian and European rules are considered alongside, throughout the study, and given the fact that legal definitions might vary depending on the legal order considered, and depending on the applicable set of rules, applicable legal definitions are provided within each part and subsection where relevant.

³⁶⁸ In the following paragraphs, the notion of AI should be understood as machine learning technology, as other types of AI (such as expert systems) do not raise specific questions regarding consumer protection.

³⁶⁹ According to Art. I.1, 2° CEL, this notion can be defined as any natural person who is acting for purposes other than trading, industrial, artisanal or liberal activities.

³⁷⁰ According to Art. I.8, 39° CEL, this notion can be defined as any legal or natural person that pursues a long-term economic aim, including its associations. Regarding this definition, see also European Court of Justice, judgement *Mannesmann AG v High Authority of the European Coal and Steel Community*, 13 July 1962, C-19/61, EU:C:1962:31.

³⁷¹ According to Art. I.1, 6° CEL, this notion can be defined as any tangible movable item.

³⁷² According to Art. I.1, 5° CEL, this notion can be defined as any performance of an undertaking, in relation to its professional activity, or to achieve its statutory objectives.

³⁷³ According to Art. I.1, 4°, CEL this notion can be defined as any good, service, immovable property, right, or obligation. See H. JACQUEMIN and J.-B. HUBIN, “Aspects contractuels et de responsabilité civile en matière d’intelligence artificielle”, in H. JACQUEMIN and A. DE STREEL, *Intelligence Artificielle et droit*, Bruxelles, Larcier, 2017, p. 91.

³⁷⁴ According to Art. I.8, 35° CEL, this notion can be defined as data which are produced and supplied in digital form.

³⁷⁵ *Ibid.* See also Art. 2, (1), Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, O.J., L 136.

to consumers. Similarly, rules arising from Book IX of the Code of Economic Law covering safety obligations for products and services could apply if an undertaking provides AI-systems to consumers such as robots marketed as toys. In addition, it should be kept in mind that companies might impose unfair contract terms upon consumers when AI-systems are the object of contracts concluded between such parties, despite the prohibition of such practices.³⁷⁶ However, as the legal rules regarding the prohibition of unfair terms in consumer contracts do not face specific issues when it comes to AI, these rules will not be studied as such within the following paragraphs.

In the following parts, the study considers the legal rules regarding warranty (part 3.2.1.), information obligations (part. 3.2.2.), unfair commercial and market practices (part 3.2.3.) and liability for defective products (part 3.2.4.).

3.2.1. Legal Rules on Warranty

Regarding warranty obligations for consumer goods, the currently applicable legal framework is composed of Articles 1649*bis* to 1649*octies* of the Code of Civil Law (CCL).³⁷⁷ However, this regime will soon be modified³⁷⁸ given the adoption of Directives 2019/770 and 2019/771³⁷⁹ at the EU level. Hence, the following paragraphs firstly describe the current legal framework in relation to AI (part A.). Secondly, the main changes brought by the European Directives will be studied (part B.).

As a preliminary remark, it should be noted here that this part of the study solely focuses on warranty obligations imposed under consumer protection law. Hence, the scope of the study is limited, *ratione personae*, to actors who legally bear such warranty obligations. Yet, other actors could potentially be liable for lacks of conformity on other grounds, for instance due to contractual obligations, or because they are upstream in the contract chains. For example, where a consumer purchases a computer, which includes AI applications, from a professional seller, the consumer might also conclude contracts with third parties who provide the AI applications, under the terms of operating licenses. In such cases, contractual obligations will apply alongside with the legal rules on warranty.

A. Currently Applicable Legal Framework

The principle contained in Article 1649*quater* of the Civil Code can be summarised as follows. Professional sellers,³⁸⁰ when selling consumer goods³⁸¹ to consumers,³⁸² are liable for any lack of conformity that already exists within the goods when they are delivered to consumers if such a lack of conformity appears within two years from the deliverance of the goods.

In order to verify whether this rule applies to AI, it is needed to assess if the notion of “consumer goods” encompasses AI. The notion of “lack of conformity” also requires an in depth analysis when it comes to AI.

³⁷⁶ Art. VI.82 to VI. 87 CEL.

³⁷⁷ Act of 1st September 2004 on the protection of consumers for the sale of consumer goods, M.B., 21 September 2004. This law transposes the Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, O.J.E.C., L 171, 7 July 1999.

³⁷⁸ I.e. as of 1st July 2021 at the latest, which is the deadline for the transposition of both Directives in national law. From 1st January 2022, Member States' national laws transposing the Directives have to apply.

³⁷⁹ Directive 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, O.J. L 136.

³⁸⁰ According to Art. 1649*bis*, § 2, 2^o CCL, this notion can be defined as any natural or legal person which sells consumer goods in the course of his professional or trading activities.

³⁸¹ According to Art. 1649*bis*, § 2, 3^o, CCL, this notion can be defined as any tangible movable item, excepted for goods sold by way of execution, water and gas where they are not put up for sale in a limited volume or set quantity, and electricity.

³⁸² According to Art. 1649*bis*, § 2, 1^o CCL, this notion can be defined as any natural person who is acting for purposes other than professional or trading activities.

The notion of consumer goods can be described as any tangible movable item besides a few exceptions.³⁸³ Based on this definition, it is unclear whether AI (which is a software) might qualify as consumer goods in all circumstances. Some authors consider software as a tangible good when it is included in a tangible item, such as a CD or a DVD. However, it cannot qualify as tangible good in the absence of a tangible medium (e.g. computer programs executed from a website).³⁸⁴ In this case, AI by itself would not be considered as consumer goods when it is not included in a tangible good, for example when it is proposed to consumers online. Other scholars consider that software should always qualify as tangible item as software is made of data and thereby takes some measurable physical space (e.g. in computers hard drives).³⁸⁵ Hence, AI could be considered as a consumer good in any case.

Following the first of these interpretations, AI-systems that are not encompassed within tangible items would not be subject to warranty obligations following Articles 1649*bis* to 1649*octies* of the CCL. This would cause a difference in treatment between consumers facing AI with a lack of conformity, depending upon the medium through which they are provided to consumers.

Regarding the notion of lack of conformity, it consists in a failure for the consumer good to fulfil one (or more) of the following conditions. Consumer goods should (i) match their descriptions, as they were made by their sellers; (ii) be fit for any specific use intended by the consumer if the consumer informed the seller about the specific use, and if the seller agreed to it; (iii) be fit for purposes goods of the same type are usually used for; and (iv) have the qualities and performances which are normal for goods of the same type, and that the consumer can reasonably expect, notably based on characteristics presented in advertising or on labelling of the good.³⁸⁶ Furthermore, the lack of conformity should already exist within the goods when they are delivered to consumers for the warranty obligations to apply.

In relation to AI, unforeseen behaviours may occur during the use of the software. This is notably due to the (self-)learning feature of such technology, which could lead AI consumer goods to differ widely from what is expected by the consumer. Such behaviours could constitute a lack of conformity from the moment one of the previously mentioned conditions failed, as long as the defaults pre-exist at the time of the delivery. On this point, literature states that when the programming of AI-systems did not prevent such changes in their behaviour, it might be considered as a pre-existing default. Hence, sellers should be the ones supporting the burden of changes of behaviour of AI-systems, rather than consumers, if the programming of the AI encompassed within a consumer good could not prevent it.³⁸⁷

In any case, when the lack of conformity takes place during the six months following delivery of the consumer goods, such lack of conformity is alleged to have pre-existed at the time of delivery.³⁸⁸ Sellers may, however, attempt to prove that it was not the case but they bear the burden of proof in this case. When consumers face a lack of conformity in consumer goods they purchased, they are entitled to require from the sellers that they repair or replace the consumer

³⁸³ See Article 1649*bis*, § 2, 3° CCL.

³⁸⁴ L. SERRANO, "Article 1er. Champ d'application et définitions", in M.C. BIANCA, S. GRUNDMANN and S. STIJNS (eds.), *La directive communautaire sur la vente - Commentaire*, Bruxelles, Bruylant, Paris, LGDJ, 2004, p. 130 ; Ch. BIQUET-MATHIEU, "La garantie des biens de consommation - présentation générale", in *La nouvelle garantie des biens de consommation et son environnement légal*, Bruxelles, la Charte, 2005, p. 64-65.

³⁸⁵ M. TENREIRO and S. GOMEZ, "La directive 1999/44/CE sur certains aspects de la vente et des garanties de biens de consommation", *R.E.D.C.* 2000, p. 12.

³⁸⁶ Art. 1649*ter*, § 1 CCL.

³⁸⁷ H. JACQUEMIN and J.-B. HUBIN, "Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle", *o.c.*, p. 99.

³⁸⁸ Art. 1649*quater*, § 4 CCL.

good, reduce the price in a proportionate manner or that contracts be rescinded for defective goods.³⁸⁹

B. Modifications Prescribed by Directives 2019/770 and 2019/771

The European rules that were adopted in May 2019 have a dualistic approach regarding warranty obligations based on the nature of the product supplied by professional traders and/or sellers to consumers. Hence, in the following paragraphs, the scopes of Directives 2019/770 and 2019/771 are respectively analysed. Their substantial rules and applicable sanctions are subsequently assessed.

B.1. Scope of Rules

- Directive 2019/770

On the one hand, Directive 2019/770 brings new warranty rules for the supply of digital content and of digital services. These are respectively defined as “data which are produced and supplied in digital form”³⁹⁰ and “service[s] that allow the consumer[s] to create, process, store or access data in digital form; or service[s] that allow the sharing of or any other interaction with data in digital form uploaded or created by the consumer[s] or other users of that service”³⁹¹. These definitions are very broad and undoubtedly encompass AI-systems as these are software, and hence are constituted of digital data, be they provided on a tangible medium or not³⁹².

The Directive applies to contracts where professional traders³⁹³ supply digital content or services to consumers³⁹⁴ in exchange of a price or in exchange of personal data.³⁹⁵ Partly overcoming the difference of treatment underlined above regarding the legal qualification of software (and more broadly of digital content) depending if they are supplied through a tangible medium or not (see part 3.2.1., section A), the Directive applies both to digital content supplied without tangible mediums and to digital content provided on tangible mediums if the mediums are exclusively used to carry the digital content.³⁹⁶ This legislative change should, hence, be welcomed.

However, not all AI-systems are covered by the rules laid down in Directive 2019/770. Among other, the legal text does not apply to digital content or digital services that “are incorporated in or interconnected with goods”³⁹⁷ with digital elements. Such goods with digital elements are defined as “any tangible movable items that incorporate, or are inter-connected with, digital content or a digital service in such a way that the absence of that digital content or digital service

³⁸⁹ Art. 1649*quinquies* CCL.

³⁹⁰ Art. 2, (1) Directive 2019/770.

³⁹¹ Art. 2, (2), (a) and (b) Directive 2019/770.

³⁹² For examples of digital content, see Recital 19 Directive 2019/770. This notably includes “computer programmes, applications, video files, audio files, music files, digital games, e-books or other e-publications, and also digital services which allow the creation of, processing of, accessing or storage of data in digital form, including software-as-a-service, such as video and audio sharing and other file hosting, word processing or games offered in the cloud computing environment and social media”.

³⁹³ According to Art. 2, (5) Directive 2019/770: “any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person’s name or on that person’s behalf, for purposes relating to that person’s trade, business, craft, or profession, in relation to contracts covered by this Directive”.

³⁹⁴ According to Art. 2, (6) Directive 2019/770: “any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person’s trade, business, craft, or profession”.

³⁹⁵ Article 3, § 1 Directive 2019/770. The notion of personal data in this Directive refers to the definition given to this notion within Article 4, (1) of the GDPR.

³⁹⁶ Art. 3, § 3 Directive 2019/770. See also R. STEENNOT and S. GEIREGAT, “Consumentenkoop & digitale inhoud: toepassingsgebied & afbakening”, in I. CLAEYS and E. TERRYIN (eds.), *Nieuw recht inzake koop & digitale inhoud en diensten*, Intersentia, 2020, p. 46-49.

³⁹⁷ Art. 3, § 4 Directive 2019/770.

would prevent the goods from performing their functions”.³⁹⁸ This definition could notably encompass robots powered by AI, meaning that such robots would not enter the scope of application of Directive 2019/770.

In addition, the Directive does not apply to “the provision of services other than digital services, regardless of whether digital forms or means are used by the trader to produce the output of the service or to deliver or transmit it to the consumer”.³⁹⁹ Thereby, the question could be raised whether a service consisting in providing legal advices or architectural plans when respectively provided by a lawyer or an architect through the use of an AI would fall within the scope of the Directive. The answer to such a question seems to be negative, as the provision of such types of services does not qualify as digital services.⁴⁰⁰ Thereby, this exclusion might constitute a gap in the scope of application of Directive 2019/770 regarding digital services provided by AI, which is used by a professional trader to automate its tasks. Furthermore, the Directive does not apply to several specific sectors, notably healthcare, electronic communications, gambling services or financial services.⁴⁰¹ This widely reduces its scope of application.

- Directive 2019/771

On the other hand, Directive 2019/771 brings new warranty rules for the sale of goods, which it defines as “any tangible movable items, [including] water, gas and electricity [...] where they are put up for sale in a limited volume or a set quantity; [and] any tangible movable items that incorporate or are inter-connected with digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions [i.e. goods with digital elements]”.⁴⁰² Hence, AI-systems that would be encompassed within material mediums, such mediums being used for anything more than carrying the AI, would qualify as goods with digital elements within the meaning of Directives 2019/770 and 2019/771. An example can be a robot as the AI it contains is needed for the robot to perform its functions, and as the body of the robot does more than merely carrying the AI.

Contracts concluded between a professional seller⁴⁰³ and a consumer⁴⁰⁴ in which the object of the contract is the sale of a good fall within the material scope of application of Directive 2019/771⁴⁰⁵, except when the contract is solely about the supply of digital content or services or where the contract bears on a tangible medium solely used to carry a digital content.⁴⁰⁶

³⁹⁸ Art. 2, (3) Directive 2019/770.

³⁹⁹ Art. 3, § 5, (a) Directive 2019/770.

⁴⁰⁰ In this regard, according to Recital 27, Directive 2019/770, are notably excluded from the scope of application of the Directive: “translation services, architectural services, legal services or other professional advice services, which are often performed personally by the trader, regardless of whether digital means are used by the trader in order to produce the output of the service or to deliver or transmit it to the consumer”.

⁴⁰¹ For a complete list of matters excluded from the scope of application of Directive 2019/770, see Art. 3, § 5.

⁴⁰² Art. 2, (5), (a) and (b), Directive 2019/771. For examples of goods with digital elements, see Recital 14, Directive 2019/771. This notably includes “Digital content that is incorporated in or inter-connected with a good can be any data which are produced and supplied in digital form, such as operating systems, applications and any other software. Digital content can be pre-installed at the moment of the conclusion of the sales contract or, where that contract so provides, can be installed subsequently. Digital services inter-connected with a good can include services which allow the creation, processing or storage of data in digital form, or access thereto, such as software-as-a-service offered in the cloud computing environment, the continuous supply of traffic data in a navigation system, or the continuous supply of individually adapted training plans in the case of a smart watch”.

⁴⁰³ According to Art. 2, (3), Directive 2019/771: “any natural person or any legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft or profession, in relation to contracts covered by this Directive”.

⁴⁰⁴ According to Art. 2, (2), Directive 2019/771: “any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft or profession”.

⁴⁰⁵ Art. 3, § 1, Directive 2019/771.

⁴⁰⁶ Art. 3, § 3 and § 4, (a), Directive 2019/771. For a complete list of matters excluded from the scope of application of Directive 2019/771, see Art. 3, § 4.

This dualistic approach may lead to a difference in treatment between consumers facing AI-systems with a lack of conformity depending upon the basis in which these systems are provided to consumers, whether as digital content or services or as goods with digital elements.

B.2. Substantial Rules and Applicable Sanctions

In both Directives, the European legislator decided that the level of discretionary power of Member States had to be strictly limited in the process of transposing them in national law. Indeed, both Directives are of maximum harmonisation. This means that Member States may not adopt more or less stringent provisions in their domestic laws regarding matters dealt with in the texts (and notably the provisions on warranty).⁴⁰⁷ Regarding warranty obligations stemming from both texts, in relation to AI, the rules contained in Directive 2019/770 and applying to digital content and services are first described in the following paragraphs. The applicable sanctions are also examined. Subsequently, the rules arising from Directive 2019/771 and applied to the sale of goods are examined, alongside with applicable sanctions.

- Directive 2019/770

Within Directive 2019/770, the principle is laid down in Article 11. It states that professional traders are liable for any lack of conformity of the digital content or services that they have provided to consumers if the lack of conformity already existed at the time of supply, and if such a lack of conformity appears within two years from the supply.⁴⁰⁸ In the case where the digital content or services require a continuous supply over a period of time, the traders are liable for any lack of conformity that occurs or becomes apparent during the period of time where the continuous supply takes place.⁴⁰⁹

Regarding the notion of lack of conformity, it consists in a failure for the digital content or services to fulfil one (or more) of the conditions set out in Articles 7 (subjective requirements for conformity) and 8 (objective requirements for conformity).⁴¹⁰ In addition, where the digital content or services require an integration into the consumers digital environments, a lack of conformity might also occur in specific cases.⁴¹¹

⁴⁰⁷ Art. 4 Directive 2019/770 and Art. 4, Directive 2019/771. However, specific Articles and Recitals within both Directives leave some margin of appreciation to Member States legislators, among other things regarding warranty. For instance, see Recitals 12 and 13, Directive 2019/770, respectively stating “[...] This Directive should also not affect national laws providing for non-contractual remedies for the consumer, in the event of lack of conformity of the digital content or digital service, against persons in previous links of the chain of transactions, or other persons that fulfil the obligations of such persons”, and “Member States also remain free, for example, to regulate liability claims of a consumer against a third party other than a trader that supplies or undertakes to supply the digital content or digital service, such as a developer which is not at the same time the trader under this Directive”. See also Recital 21, Directive 2019/771, “Member States should also remain free to extend the application of the rules of this Directive to contracts that are excluded from the scope of this Directive, or to otherwise regulate such contracts. For instance, Member States should remain free to extend the protection afforded to consumers by this Directive also to natural or legal persons that are not consumers within the meaning of this Directive, such as non-governmental organisations, start-ups or SMEs”. Another interesting point where Member States retain some margin of appreciation relates to the inclusion (or not) of platforms within the scope of application *ratione personae* of the obligations brought by both Directives within domestic laws (see Recital 18, Directive 2019/770, and Recital 23, Directive 2019/771).

⁴⁰⁸ Art. 11, § 2 Directive 2019/770.

⁴⁰⁹ Art. 11, § 3 Directive 2019/770.

⁴¹⁰ The addition of objective requirements for conformity, on top of subjective requirements, is meant to avoid that consumers are deprived of their rights in the case of contracts with very low standards, which consumers cannot always negotiate with traders (see Recital 45, Directive 2019/770). See also B. TILLEMANS and F. VAN DEN ABEEL, “Conformiteit in de Richtlijn Consumentenkoop 2019: heft de berg een muis gebaard?”, in I. CLAEYS and E. TERRY (eds.), *Nieuw recht inzake koop & digitale inhoud en diensten*, Intersentia, 2020, p. 96-98.

⁴¹¹ Art. 9 Directive 2019/770.

The subjective conditions set out in Article 7 are the following: digital content or services should (i) fit the description, quantity, quality, functionality,⁴¹² compatibility,⁴¹³ interoperability,⁴¹⁴ and other features set out in the contract; (ii) be fit for any specific use intended by the consumer, if the consumer informed the trader about the specific use, and if the trader agreed to it; (iii) be supplied with accessories, instructions (notably on installation), and customer assistance required by the contract; and (iv) be updated as agreed upon in the contract.

For the objective conditions set out in Article 8, they are as follows: digital content or services should (i) be fit for the purposes for which similar digital content or services would normally be used, taking into account existing EU or national law, technical standards, or sector-specific industry codes of conduct; (ii) be of quantity and possess the qualities and performance features (notably regarding functionality, compatibility, accessibility, continuity and security) that are normal for digital content or services of the same type and that the consumer may reasonably expect; (iii) be supplied with accessories and instructions which may reasonably be expected by consumers;⁴¹⁵ and (iv) comply with trial versions or previews of the digital content or services made available by the traders before the contract was concluded.⁴¹⁶ Within the same Article, the Directive states that traders have to supply consumers with information on updates and updates (notably security updates) that are needed to maintain the digital content or services in conformity.⁴¹⁷

It makes little doubt that AI-systems provided by traders to consumers, if entering the scope of application of the Directive, could fail to meet part or all of these conditions, and hence lack of conformity (see reasoning held above in part 3.2.1., section A). Notably, AI-systems as digital content could no longer fit the descriptions set out in the contracts and/or no longer be able to fulfil the purposes for which they would normally be used after an unforeseen change of behaviour caused by its (self-)learning capabilities.

For instance, a spam filter powered by AI could at first misclassify many emails when it is used by a consumer that receives a lot of advertising for which he subscribed. After its learning process, the spam filter might no longer block as spam any email classifying both desired and undesired advertising as authorised emails. In such a case, the spam filter might no longer fit its description as set out in the contract or be able to fulfil the purpose for which it should normally be used.

Yet, the Directive states that “[t]here shall be no lack of conformity [...] if, at the time of the conclusion of the contract, the consumer was specifically informed that a particular characteristic of the digital content or digital service was deviating from the objective requirements for conformity [...] and the consumer expressly and separately accepted that deviation when concluding the contract”.⁴¹⁸

Hence, traders could potentially try to avoid the legal qualification of lack of conformity for the potential flaws of their AI-systems by contractually providing information to consumers on the learning capabilities (and correlative potential for unforeseen changes of behaviour) of AI, and by

⁴¹² According to Art. 2, (11) Directive 2019/770: “the ability of the digital content or digital service to perform its functions having regard to its purpose”.

⁴¹³ According to Art. 2, (10) Directive 2019/770: “the ability of the digital content or digital service to function with hardware or software with which digital content or digital services of the same type are normally used, without the need to convert the digital content or digital service”.

⁴¹⁴ According to Art. 2, (12) Directive 2019/770: “the ability of the digital content or digital service to function with hardware or software different from those with which digital content or digital services of the same type are normally used”.

⁴¹⁵ This information obligation is detailed below, see part 3.2.2, part A.

⁴¹⁶ Art. 8, § 1 Directive 2019/770.

⁴¹⁷ Art. 8, § 2 Directive 2019/770. This information obligation is detailed below, see part 3.3.2 section A. If consumers do not install such updates, traders might not be held liable for resulting lacks of conformity in certain circumstances (see Recital 47 and Art. 8, § 3).

⁴¹⁸ Art. 8, § 5 Directive 2019/770.

obtaining consumers' acceptance for that deviation. In the case of a spam filter powered by AI, for instance, a trader might inform its consumers in contracts that its AI has a particular characteristic, namely the ability to learn, that could be deviating from the objective requirements for conformity such as the ability to fulfil the purpose for which the spam filter should normally be used. In such cases, consumers might not have many other choices than to accept the deviance when concluding the contracts.

In any case, at this stage, it is unclear whether such information from traders and the acceptance of the deviance from consumers would be sufficient to avoid the legal qualification of lack of conformity. That is because such a solution might allow traders to seriously limit the cases in which they would be held liable for the lack of conformity regarding AI-systems. Regarding this issue, case-law will then be needed to determine to what extent traders could avoid liability through this mean.

In addition, the Directive provides that traders may substantially modify their digital content or services, without causing a lack of conformity, where the digital content or services are continuously provided to consumers over a period of time. Traders may do so if several conditions are met, notably when the contract allows for such a modification and provides reasons for it.⁴¹⁹ In relation to AI-systems, and given the fact that such software can learn and evolve, traders might at some point need to make substantial modifications to their digital content or services. In such cases, Article 19 states that consumers may, however, terminate their contracts with traders if the modification negatively and substantially affects the consumers access or use of the digital content or service.⁴²⁰

The Directive also imposes rules on the burden of proof.⁴²¹ If a lack of conformity becomes apparent within one year from the supply of the digital content or services, traders bear the burden to prove that there was none at the time of the supply, and that digital content or services were conform.

However, this period of one year from the supply might prove too short, as AI-systems are able to continuously learn and evolve. AI-systems supplied to consumers as digital content or services could be conform during one year, but still lack conformity before the end of the warranty period. In such a case, it could prove difficult for consumers to prove that the lack of conformity already existed in the AI-systems at the time of supply of the digital content or services. Yet, consumers could hire experts to help them find out about the origin of such lacks of conformity.

In addition, this period of one year foreseen by the Directive might cause a difference of treatment between digital content or services, and goods with digital elements, for which Member States can extend the period during which the burden of proof is on the sellers up to two years (cf. *infra*).⁴²²

In the case where the digital content or services are continuously supplied over a period of time, and the lack of conformity becomes apparent in that period of time, traders bear the burden of proof in any case.⁴²³

⁴¹⁹ Art. 19, § 1 Directive 2019/770. The conditions set out by the Directive are the following : "(a) the contract allows, and provides a valid reason for, such a modification; (b) such a modification is made without additional cost to the consumer; (c) the consumer is informed in a clear and comprehensible manner of the modification; and (d) [...] the consumer is informed reasonably in advance on a durable medium of the features and time of the modification [...] or of the possibility to maintain the digital content or digital service without such a modification [...]"

⁴²⁰ Art. 19, § 2 Directive 2019/770.

⁴²¹ Art. 12, § 2, and § 3 Directive 2019/770.

⁴²² See Art. 11, § 2, Directive 2019/771.

⁴²³ See G. STRAETMANS and B. VANLERBERGHE, "De nieuwe Richtlijnen Consumentenkoop en Levering van digitale inhoud: bewijsaspecten", in I. CLAEYS and E. TERRY (eds.), *Nieuw recht inzake koop & digitale inhoud en diensten*, Intersentia, 2020, p. 416-418.

Yet, traders can reverse the burden of proof and shift it upon the consumers if they manage to demonstrate that the digital environment of the consumers are not compatible with the digital content or services supplied. This is only possible if traders can demonstrate that they have clearly informed consumers about technical requirements of the digital content or services before the conclusion of any contract. In this regard, consumers have the obligation to cooperate with traders to ascertain the cause of the lack of conformity.⁴²⁴

When a lack of conformity is faced by a consumer, various remedies can apply. Consumers are entitled to require from traders to bring the digital content or service into conformity, reduce the price in a proportionate manner or terminate the contract for defective contents or services.⁴²⁵ It is interesting to note that the termination of the contracts is limited to cases where the lack of conformity is not only minor, which the traders have to prove.⁴²⁶ Regarding AI-systems, it might be difficult to ascertain when a lack of conformity will be only minor and when it will be more than only minor. In addition, when contracts are terminated, consumers may request from traders to receive any non-personal data which was provided or created by them when using the digital content or services.⁴²⁷

Before turning to warranty rules created by Directive 2019/771, a few considerations may prove relevant. Firstly, Directive 2019/770 states that the rules it contains are mandatory. Contractual terms contrary to these rules and detrimental to consumers are not allowed.⁴²⁸ Secondly, Directive 2019/770 applies to the supply of digital content or services by traders when provided in exchange of personal data by consumers. In this regard, the Directive states that it applies alongside the GDPR, and that in the event of a conflict between both legal texts, the dispositions of the GDPR have to prevail.⁴²⁹ This point seems important as most AI-systems use personal data to perform their tasks. Hence, consumer protection rules described above might be completed and reinforced by those arising from the GDPR. Furthermore, a breach of the GDPR by a digital content or service (being an AI-systems) and provided in exchange of personal data could potentially lead to a lack of conformity of this content or service if it enters the scope of application of the Directive 2019/770.⁴³⁰

- Directive 2019/771

Within Directive 2019/771, Article 10 states that sellers are liable for any lack of conformity of the goods, including goods with digital elements which they have sold to consumers, if the lack of conformity already existed at the time of delivery, and if such a lack of conformity appears within two years from the delivery.⁴³¹ In the case of goods with digital elements, where the digital content or services are continuously supplied over a period of time, the sellers are liable for any lack of

⁴²⁴ Art. 12, § 4, and § 5 Directive 2019/770.

⁴²⁵ Art. 14 Directive 2019/770. See also M. E. STORME, "Remedies bij digitale inhoud en diensten", in I. CLAEYS and E. TERRYN (eds.), *Nieuw recht inzake koop & digitale inhoud en diensten*, Intersentia, 2020, p. 246-252.

⁴²⁶ Art. 14, § 6 Directive 2019/770.

⁴²⁷ Art.16, § 4 Directive 2019/770. The objective is to avoid that consumers be discouraged to exercise their right to termination of the contracts, when digital content or services lack conformity, as they could be afraid to be deprived of access to their non-personal data afterwards (see Recital 70).

⁴²⁸ Art. 22 Directive 2019/770.

⁴²⁹ Art. 3, § 8 Directive 2019/770.

⁴³⁰ This could be based on Art. 8, § 1, (a) Directive 2019/770, which states that digital content or services shall "be fit for the purposes for which digital content or digital services of the same type would normally be used, taking into account, where applicable, any existing Union [...] law [...]" (own emphasis). It could also be based on Art. 8, § 1, (b), which states that digital content or services shall "be of the quantity and possess the qualities and performance features, including in relation to functionality, compatibility, accessibility, continuity and security, normal for digital content or digital services of the same type and which the consumer may reasonably expect [...]" (own emphasis). In both cases, traders might be expected to respect binding rules of law such as those arising from the GDPR when supplying their AIs, whether by considering the respect of data protection when assessing if a digital content or service is fit for purpose, or by considering the respect of data protection when assessing the digital content or service qualities and performance features.

⁴³¹ Art. 10, § 1 Directive 2019/771.

conformity that occurs or becomes apparent during the period of time where the continuous supply takes place.⁴³²

The notion of lack of conformity, under this Directive, is very similar to the one under Directive 2019/770. It consists in a failure for the goods to fulfil one (or more) of the conditions set out in Article 6 (subjective requirements for conformity) and Article 7 (objective requirements for conformity). Again, where the goods (notably goods with digital elements) require an installation, a lack of conformity might also occur in specific cases.⁴³³

The subjective conditions set out in Article 6 are similar to those arising from Directive 2019/770. Goods should (i) fit the description, type, quantity, quality, functionality,⁴³⁴ compatibility,⁴³⁵ interoperability,⁴³⁶ and other features set out in the sales contract; (ii) be fit for any particular purpose intended by the consumer, if the consumer informed the seller about the particular use, and if the seller agreed to it; (iii) be delivered with accessories, instructions (notably on installation), agreed upon in the contract; and (iv) be updated as agreed upon in the contract.

For the objective conditions set out in Article 7, they slightly differ from those arising included in Directive 2019/770 due to the different nature of the products at stake. They are as follows. Goods should (i) be fit for the purposes for which goods of the same type would normally be used, taking into account existing EU or national law, technical standards, or sector-specific industry codes of conduct; (ii) where applicable, be of the quality and correspond to the description of samples or models made available to consumers before contracting; (iii) where applicable, be delivered with accessories and instructions which may reasonably be expected by consumers;⁴³⁷ and (iv) be of quantity and possess the qualities and other features (including durability, functionality, compatibility, and security) that are normal for goods of the same type and that the consumer may reasonably expect.⁴³⁸ Within the same Article, the Directive states that sellers have to supply consumers of goods with digital elements with information on updates and updates (notably security updates) that are needed to maintain them in conformity.⁴³⁹

Here again, it seems that AI-systems encompassed within tangible items (i.e. goods with digital elements), such as robots, might fail to comply with one or more of the conditions set out in Articles 6 and 7 of the Directive, and hence lack conformity (see in this regard the reasoning held in part 3.2.1., section A). For example, a robot toy powered by AI and developed for children could at first be fully functional but might start to adopt inappropriate behaviours (e.g. saying things that are inappropriate or offensive to children) after learning such behaviour from other persons to which it is passively exposed. After its learning process, the robot might hence no longer fit its description as set out in the contract (i.e. being a toy destined to children) or be able to fulfil the purpose for which it should normally be used (i.e. interacting with children).

Yet, the Directive 2019/771 states, likewise Directive 2019/770, that “[t]here shall be no lack of conformity [...] if, at the time of the conclusion of the sales contract, the consumer was specifically informed that a particular characteristic of the goods was deviating from the objective

⁴³² Art. 10, § 2 Directive 2019/771.

⁴³³ Art. 8 Directive 2019/771.

⁴³⁴ According to Art. 2, (9) Directive 2019/771: “the ability of the goods to perform their functions having regard to their purpose”.

⁴³⁵ According to Art. 2, (8) Directive 2019/771: “the ability of the goods to function with hardware or software with which goods of the same type are normally used, without the need to convert the goods, hardware or software”.

⁴³⁶ According to Art. 2, (10) Directive 2019/771: “the ability of the goods to function with hardware or software different from those with which goods of the same type are normally used”.

⁴³⁷ This information obligation is detailed below, see part 3.2.2. section A.

⁴³⁸ Art. 7, § 1 Directive 2019/771.

⁴³⁹ Art. 7, § 3 Directive 2019/771. This information obligation is detailed below, see part 3.2.2. section A. If consumers do not install such updates, sellers might not be held liable for resulting lacks of conformity in certain circumstances (see Recital 30 and Art. 7, § 4).

requirements for conformity [...] and the consumer expressly and separately accepted that deviation when concluding the sales contract". Hence, here again, sellers might try to avoid the qualification of lack of conformity for the potential flaws of their AI-systems. This can be done by providing information to consumers on the learning capabilities of their goods with digital elements and by obtaining consumers' acceptance for that deviation. In the case of a robot toy powered by an AI, a seller might inform its consumers that its AI-system has a particular characteristic, that is to say the ability to learn, which could be deviating from the objective requirements for conformity set out in the Directive. In such cases, consumers may have no other choice than to accept the deviance when concluding the contracts. As it is the case for Directive 2019/770, case law will be needed to determine to what extent traders could avoid liability through this mean.

Regarding the burden of proof, a lack of conformity that becomes apparent within one year from the delivery of goods (notably goods with digital elements) is alleged to have existed at the time of delivery.⁴⁴⁰ However, the Directive states that Member States may decide of a longer period (up to two years from delivery) for this presumption.⁴⁴¹ In such a case, the sellers bear the burden to prove that there was no lack of conformity at the time of the delivery and that goods were conform. When goods with digital elements are continuously supplied over a period of time, and a lack of conformity arises in that period of time, the sellers also bear the burden of proof.⁴⁴²

In terms of remedies to a lack of conformity, consumers are entitled to have their goods brought into conformity or replaced, to have a proportionate reduction of the price of the goods or to terminate the contracts.⁴⁴³ Here again, it should be noted that termination of the contracts is limited to cases in which the lack of conformity is not only minor that the sellers have to prove.⁴⁴⁴ Regarding AI-systems, it might be difficult to ascertain when a lack of conformity will be only minor and when it will be more than minor. In addition, consumers may withhold the payment of the price of the goods purchased until the sellers fulfil their obligations in case of a lack of conformity.⁴⁴⁵

3.2.2. Information obligations

Regarding information obligations arising from consumer protection law, the legal framework is mainly constituted by the book VI of the Code of Economic Law.⁴⁴⁶ In addition, some legal instruments recently adopted at the EU level have not yet been transposed in Belgian law but also contain a few information obligations. These are notably the Directives 2019/770 and 2019/771. All such information obligations arising from consumer protection law will first be examined in relation to AI (part A.). Consumer protection law is not the only relevant tool to consider when it comes to information obligations. Indeed, consumers often qualify as data subjects⁴⁴⁷ within the meaning of the GDPR. As such, they benefit from several additional information obligations. This

⁴⁴⁰ Art. 11, § 1 Directive 2019/771. See also S. STIJNS and S. JANSEN, "Remedies bij consumentenkoop", in I. CLAEYS and E. TERRYNS (eds.), *Nieuw recht inzake koop & digitale inhoud en diensten*, Intersentia, 2020, p. 192-193.

⁴⁴¹ Art. 11, § 2 Directive 2019/771.

⁴⁴² See G. STRAETMANS and B. VANLERBERGHE, "De nieuwe Richtlijnen Consumentenkoop en Levering van digitale inhoud: bewijsaspecten", *o.c.*, p. 405.

⁴⁴³ Art. 13, § 1 Directive 2019/771. See also S. STIJNS and S. JANSEN, "Remedies bij consumentenkoop", *o.c.*, p. 204-213.

⁴⁴⁴ Art. 13, § 5 Directive 2019/771.

⁴⁴⁵ Art. 13, § 6 Directive 2019/771.

⁴⁴⁶ Which is notably the Belgian transposition of Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, O.J., L 304.

⁴⁴⁷ According to Art. 4, (1) GDPR: "an identifiable natural person [, i.e. a natural person] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

is even more the case when dealing with AI-systems as automated processing of personal data might trigger specific additional information obligations (e.g. in the case of some fully automated decisions). Hence, information obligations arising from the field of data protection will also be analysed in relation to AI (part B.).

A. Consumer Protection Law

Allegedly, consumers suffer from a certain weakness in their relations with undertakings.⁴⁴⁸ Therefore, European and Belgian legislators have attempted to restore some kind of balance in contractual relations between undertakings and consumers.⁴⁴⁹ This can notably be seen in relation to information obligations. As undertakings supposedly benefit from more information regarding the elements and objects of the contracts they conclude with consumers, they are required to provide the latter with various types information, which are listed within different legal provisions studied below.

In relation to AI, it should be noted that the weakness and correlative lack of information of consumers mainly finds its origins within the object of the contracts. Indeed, average consumers do not necessarily have knowledge regarding technical functioning of AI-systems, either as software or incorporated in robots. For instance, they are not aware, *ab initio*, of the AI-system's functionalities, interoperability with other components or software, etc.⁴⁵⁰

The various information obligations that are imposed by the legal framework are analysed below. Firstly, relevant rules contained in Book VI of the Code of Economic Law are examined. Secondly, obligations arising from Directives 2019/770 and 2019/771 are analysed as well. Book VI of the Code of Economic Law contains information obligations in Articles VI.2 focusing on all contracts other than distance or off-premises contracts, Article VI.45 dealing with distance contracts⁴⁵¹ and Article VI.64 focusing on off-premises contracts.⁴⁵² In each case, these articles only apply when consumers⁴⁵³ interact with undertakings.⁴⁵⁴ It should be highlighted that Article VI.2 applies when consumers purchase 'products',⁴⁵⁵ which also includes AI, whatever its form, given its broad

⁴⁴⁸ See notably M. FONTAINE, "La protection de la partie faible dans les rapports contractuels (Rapport de synthèse)", in J. GHESTIN and M. FONTAINE, *La protection de la partie faible dans les rapports contractuels. Comparaisons franco-belges*, Paris, LGDJ, 1996, p. 616-617; Ch. BOURBIER, *La faiblesse d'une partie au contrat*, Bruxelles, Bruylant, 2003, p. 22 and following.

⁴⁴⁹ H. JACQUEMIN and J.-B. HUBIN, "Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle", *o.c.*, p. 89.

⁴⁵⁰ *Ibid.*, p. 90.

⁴⁵¹ According to Art. I.8, 15° CEL, this notion can be defined as any contract concluded between an undertaking and a consumer, relating to sales or services provided at distance, where the consumer and the undertaking are not physically simultaneously present, through the use of distance communication techniques.

⁴⁵² According to Art. I.8, 31° CEL, this notion can be defined as any contract between a consumer and an undertaking, (i) concluded in the simultaneous physical presence of the undertaking and of the consumer, in a place which is not the commercial establishment of the undertaking; (ii) where the consumer made an offer to the undertaking in the simultaneous physical presence of the undertaking and of the consumer, in a place which is not the commercial establishment of the undertaking; (iii) concluded in the commercial establishment of the undertaking, through the use of distance communication techniques, immediately after the consumer was personally and individually solicited by the undertaking, both parties being simultaneously physically present, in a place which is not the commercial establishment of the undertaking before the conclusion of the contract; (iv) concluded during an outing, the objective or effect of which is to promote and sell goods or services to consumers.

⁴⁵³ According to Art. I.1, 2° CEL, this notion can be defined as any natural person who is acting for purposes other than trading, industrial, artisanal or liberal activities.

⁴⁵⁴ According to Art. I.8, 39° CEL, this notion can be defined as any legal or natural person that pursues a long-term economic aim, including its associations. Regarding this definition, see also European Court of Justice, judgement *Mannesmann AG v High Authority of the European Coal and Steel Community*, 13 July 1962, C-19/61, EU:C:1962:31.

⁴⁵⁵ According to Art. I.1, 4° CEL, this notion can be defined as any good, service, immovable property, right, or obligation.

definition.⁴⁵⁶ The Articles VI.45 and 64 apply to goods⁴⁵⁷, services⁴⁵⁸ and to some extent to digital content,⁴⁵⁹ hence partially encompassing AI whatever medium it is provided with (i.e. tangible or not).

The information required by the Articles VI.2, 45 and 64, which can prove relevant when AI-systems are at stake, is relatively similar. This information notably consists in the provision to consumers, before any contract is concluded, of (i) the main characteristics of the product,⁴⁶⁰ or of the good or service;⁴⁶¹ (ii) where applicable, the functionality of the digital content, including information on applicable technical protection measures;⁴⁶² and (iii) where applicable, any interoperability of the digital content with other hardware, software, or services, which the undertaking is (or should reasonably be) aware of.⁴⁶³

These information obligations need to be analysed in-depth. Regarding the information that should be given to consumers about the main characteristics of products, goods or services, guidance is provided by the European Commission. The EC explains that “[t]his information requirement is identical to the one in Article 7(4)(a) of the UCPD. The existing 2009 Guidance on the UCPD (p. 49-52) explains that the detail of the information to be provided depends on the complexity of the product and highlights the importance of explaining any restrictive conditions concerning the offer, such as very limited period during which a service is provided”.⁴⁶⁴ The Guidance issued by the EC in 2009, referred to in the previous sentence, adds that “complex products may require the provision of more information than simple ones”.⁴⁶⁵

As AI-systems are very likely to be considered complex products due to their technological complexity, undertakings will have to provide more information than they usually do for simple or more traditional products.⁴⁶⁶ Notably, undertakings should make sure to clearly inform consumers about the limits that AI-systems face, about their accuracy and about the risks of harms for consumers and third parties that might reasonably be foreseen through the use of such products.

Turning to the notion of functionality of digital content, this is understood as “the ability of the digital content or digital service to perform its functions having regard to its purpose”.⁴⁶⁷ According to the EC, this information obligation notably requires undertakings to provide consumers with explanations on (i) the language of the content; (ii) the method for providing the content (e.g.

⁴⁵⁶ H. JACQUEMIN and J.-B. HUBIN, “Aspects contractuels et de responsabilité civile en matière d’intelligence artificielle”, o.c., p. 91.

⁴⁵⁷ According to Art. I.1, 6° CEL, this notion can be defined as any tangible movable item.

⁴⁵⁸ According to Art. I.1, 5° CEL, this notion can be defined as any performance of an undertaking, in relation to its professional activity or to achieve its statutory objectives.

⁴⁵⁹ According to Art. I.8, 35° CEL, this notion can be defined as data which are produced and supplied in digital form.

⁴⁶⁰ Art. VI.2, 1° CEL.

⁴⁶¹ Articles VI. 45, 1°, and VI. 64, 1° CEL. None of these two Articles mentions digital content at this stage, which might cause an issue. In the case of goods, it is not sure whether all AI-systems are encompassed within this legal qualification (see reasoning in part 3.2.1, section A). Similarly, for the notion of services, it is unsure whether all AI-systems would be encompassed. For instance, an AI-system that would be purchased online by a consumer might fail to qualify as a service, due to the absence of any performance of a service, as much as it might fail to qualify as a good, due to the absence of tangible medium. Thereby, the current legal framework might cause a difference of treatment between consumers facing AI-systems that they purchased through intangible mediums, on the basis of the type of contract concluded by the consumers (i.e. distance and off-premises contracts vs. other contracts).

⁴⁶² Art. VI.2, 8°, VI.45, 18°, and VI.64, 17° CEL.

⁴⁶³ Art. VI.2, 9°, VI.45, 19°, and VI.64, 18° CEL.

⁴⁶⁴ European Commission, “DG Justice Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council”, June 2014, p. 22.

⁴⁶⁵ European Commission, “Commission Staff Working Document – Guidance on the implementation/application of Directive 2005/29/EC on unfair commercial practices”, 4th December 2009, SEC(2009) 1666 final, p. 48.

⁴⁶⁶ H. JACQUEMIN and J.-B. HUBIN, “Aspects contractuels et de responsabilité civile en matière d’intelligence artificielle”, o.c., p. 91-92.

⁴⁶⁷ Art. 2, (11) Directive 2019/770.

streaming, online, one-off downloading, etc.); (iii) the playing duration of the content, for video or audio files; (iv) the size and file type for downloadable files; and (v) limitations on the use of the content, such as a limited number of replays for a video or audio file, or limits regarding the possibility to make a private copy.⁴⁶⁸ As AI-systems are software, the information on the limitations on its use might prove particularly relevant for consumers.

Furthermore, the notion of interoperability of digital content is defined as “the ability of the digital content or digital service to function with hardware or software different from those with which digital content or digital services of the same type are normally used”.⁴⁶⁹ Under this information obligation, the undertaking should inform the consumer “on devices that the content can be used with; where applicable this should include information about the necessary operating system and additional software, including the version number, and hardware, such as processor speed and graphics card features”.⁴⁷⁰ Once more, AI-systems being qualified as software, information on interoperability will be necessary to ensure that consumers can use their AI-products.

There are, *prima facie*, no specific sanctions that might apply when these information obligations are not respected. However, if the lack of information leads consumers to adopt an economic behaviour that they would otherwise not have adopted, the sanctions applicable to unfair commercial practices might apply (see below part 3.2.3, section A).⁴⁷¹

In addition to these information obligations, Articles VI.9 and 10 provide that the King might impose complementary measures to ensure a high level of commercial fairness and consumer protection for the sale of goods and the supply of services. Such complementary measures may consist in information obligations, as the King could decide how packages should be presented and what labels they should bear, to be placed on the market.⁴⁷²

Under the Directives 2019/770 and 2019/771, several information obligations have also been established.⁴⁷³ Both Directives state that professional traders⁴⁷⁴ and/or sellers⁴⁷⁵ have to provide their consumers⁴⁷⁶ with information such as “installation instructions or other instructions, as the consumer may reasonably expect to receive”.⁴⁷⁷ If such information is not provided to consumers, the object of the contracts between professionals and consumers will not comply with the objective conformity requirements. Installation instructions and instructions regarding the use of AI-systems might thereby be provided by professionals to their consumers. Professionals also have to inform their consumers about the existence of updates to satisfy conformity requirements, which will undoubtedly prove useful for AI-systems.⁴⁷⁸

⁴⁶⁸ European Commission, “DG Justice Guidance ... Council”, *o.c.*, p. 67-68.

⁴⁶⁹ Art. 2, (12) Directive 2019/770.

⁴⁷⁰ European Commission, “DG Justice Guidance ... Council”, *o.c.*, p. 68.

⁴⁷¹ See Art. VI.38 CEL. See also N. GILLARD, “Protection des consommateurs”, *Guide juridique de l'entreprise*, Titre XI, Livre 110.1, 2019, p. 24.

⁴⁷² Art. VI.9, § 1, 1° CEL. At best of our knowledge, no such text was already adopted in relation to AI.

⁴⁷³ C. DELFORGE, “Bientôt de nouvelles règles de protection des consommateurs”, *Les pages – Obligations, Contrats et Responsabilités*, 2020, n° 71, p. 1-2.

⁴⁷⁴ According to Art. 2, (5) Directive 2019/770: “any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft, or profession, in relation to contracts covered by this Directive”.

⁴⁷⁵ According to Art. 2, (3) Directive 2019/771: “any natural person or any legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft or profession, in relation to contracts covered by this Directive”.

⁴⁷⁶ According to Art. 2, (6) Directive 2019/770 and Art. 2, (2), Directive 2019/771: “any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft, or profession”.

⁴⁷⁷ Art. 8, § 1, c) Directive 2019/770 and Art. 7, § 1, c), Directive 2019/771.

⁴⁷⁸ Art. 8, § 2 Directive 2019/770 and Art. 7, § 3, Directive 2019/771.

B. Data Protection Law

In addition to consumer protection law, the field of data protection law also contains some information obligations that might prove relevant to this study. Although the beneficiaries of such obligations are qualified as data subjects,⁴⁷⁹ rather than consumers, there can be a strong link between both legal qualifications when AI is considered.

As a matter of fact, when European consumers use AI, there is a process⁴⁸⁰ of the consumers' personal data⁴⁸¹ by these systems in nearly all cases. In such cases, the GDPR will apply.⁴⁸² For instance, if an undertaking supplies AI embedded in a robot, the robot (and hence the AI) will at some point process personal data such as the voice of the consumer, his/her picture or his/her location. Similarly, if an undertaking supplies an AI-based personal assistant as a service, for instance on a smartphone, AI will in addition to his/her voice have access to many types of personal data on the consumer's phone (i.e. agenda, pictures, etc.).

For information obligations contained in the GDPR to apply to undertakings and benefit to consumers (i.e. data subjects), undertakings have to qualify as data controllers. The notion of data controller is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".⁴⁸³

Most of the time, if not always, undertakings will determine the purposes and the means of the processes rather than consumers. That is because consumers will not have any access to the inner workings of AI-systems, nor be able to decide what purposes are pursued by the products they use when it processes their personal data. In the example of the AI-based personal assistant, the provider of the service is able to decide the purposes for which the system collects data, and how it does so, while the consumer of such service is only be able to use the AI supplied to him/her.

Thereby, the information obligations set out in Articles 13 and/or 14 have to be respected by undertakings that also qualify as data controllers. Both Articles have similar requirements, the difference between them being that Article 13 applies when personal data are directly collected directly from data subjects, while Article 14 applies when personal data are indirectly collected (i.e. from another source than the data subject).

The information to be communicated to data subjects notably encompasses (i) the purposes of the processing and the legal basis for the processing; (ii) the recipients of personal data; (iii) the existence of transfers of personal data outside the EU and the guarantees set out to protect personal data in such cases; (iv) the period for which personal data will be retained; (v) the existence of data subjects' rights, such as the right to rectification of incorrect data, or the right to data portability; and (vi) the existence of automated decision-making in the meaning of Article 22, and if so, meaningful information about the logic involved, the significance, and the envisaged consequences of such processing.⁴⁸⁴

⁴⁷⁹ According to Art. 4, (1) GDPR: "an identifiable natural person [, i.e. a natural person] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

⁴⁸⁰ According to Art. 4, (2) GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

⁴⁸¹ According to Art. 4, (1) GDPR: "any information relating to an identified or identifiable natural person".

⁴⁸² In relation to the scope of application of the GDPR, see Art. 2 and 3.

⁴⁸³ Art. 4, (7) GDPR. See also C. DE TERWANGNE, "Définitions clefs et champ d'application du RGPD", *Le règlement général sur la protection des données*, Bruxelles, Larcier, 2018, p. 67-68.

⁴⁸⁴ Art. 13, § 1 and § 2, and 14, § 1 and § 2 GDPR.

Regarding the information obligations related to automated decision-making, these apply when data controllers (intend to) make fully automated decisions that will produce legal effects concerning data subjects, or will similarly significantly affect them.⁴⁸⁵ This could be the case, for instance, when AI is used by an undertaking to provide legal advices to a consumer. In such cases, part of the literature considers that data subjects also have the right to receive an explanation of such automated-decisions, in addition to meaningful information on the logic involved,⁴⁸⁶ albeit not all authors agree upon the existence of this right.⁴⁸⁷ However, it is extremely challenging, from a technical perspective, to provide satisfactory and legible explanations about the decisions made by some AI-systems (such as decisions made by neural network technology, which is a form of machine learning).⁴⁸⁸

Such information obligations, based on the Articles 13-14, and potentially on Article 22, provide data subjects with a better understanding of the processes carried out on their personal data. These provisions seek to restore some balance between data subjects and data controllers – in the same vein as consumer protection rules aim between consumers and undertakings.⁴⁸⁹ In a context in which AI is involved, technological complexity of data processing makes it difficult for data subjects to know if there is a processing, whom makes it, and for what purposes personal data is collected.⁴⁹⁰ Hence, data protection law attempts to counter-balance the asymmetry of information that exists between data subjects and data processors.

In the case where the information obligations described above are not respected by data controllers, data subjects are entitled to lodge complaints with the competent data protection authorities.⁴⁹¹ Following such complaints, data protection authorities may investigate the cases submitted and impose legally binding sanctions to data controllers. These include (i) issuing warnings to data controllers; (ii) issue reprimands to data controllers; (iii) order the controllers to comply with data subjects' requests to exercise their rights; (iv) order the controllers to bring its operations into compliance with the provisions of GDPR; and/or (v) impose administrative fines as provided for in Article 83.⁴⁹² Data subjects are also entitled to file suits in front of Member States' national jurisdictions, and to sue data controllers that fail to comply with their information obligations.⁴⁹³

3.2.3. Unfair Commercial Practices

When AI is the object of contracts concluded between undertakings and consumers, one could imagine that undertakings do not give sufficient (or give incorrect) information to consumers about the capabilities and limits of the AI-systems to be provided. This could mislead their consumers and affect their economic behaviours. In other cases, companies could potentially adopt aggressive behaviours towards their consumers, through AI-products supplied to them as services, goods or

⁴⁸⁵ Art. 22 GDPR.

⁴⁸⁶ See notably L. EDWARDS and M. VEALE, "Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For", *Duke Law & Technology Review* 2017, vol. 16, p. 18-84, G. MALGIERI and G. COMMANDÉ, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law* 2017, vol. 7, p. 243-265, B. GOODMAN and S. FLAXMAN, "European Union regulations on algorithmic decision-making and a "right to explanation"", *AI Magazine* 2017, vol. 38, p. 50-57.

⁴⁸⁷ See notably S. WACHTER, B. MITTELSTADT, and L. FLORIDI, "Why a right to explanation of automated decision-making does not exist in the general data protection regulation", *International Data Privacy Law* 2017, vol. 7, p. 76-99.

⁴⁸⁸ European Commission, "White Paper on Artificial Intelligence – A European Approach to excellence and trust", 19th February 2020, COM(2020) 65 final, p. 12.

⁴⁸⁹ Recitals 39 and 60 and Art. 5 GDPR.

⁴⁹⁰ Recital 58 GDPR.

⁴⁹¹ Art. 77 GDPR.

⁴⁹² Art. 83, § 2 GDPR.

⁴⁹³ Art. 79 GDPR.

digital content. For example, AI supplied as a service to a consumer might unduly influence the latter and lead him/her to buy other related products.

Hence, turning back to consumer protection law, the following paragraphs focus on the prohibition of unfair commercial practices towards consumers (part A).⁴⁹⁴ Similarly, Belgian law prohibits unfair market practices between undertakings. Hence, the same misleading and/or aggressive practices should also be considered in the relations between undertakings (part B).⁴⁹⁵

A. Unfair Commercial Practices Towards Consumers

Under the terms of Article VI.95, undertakings⁴⁹⁶ are forbidden to adopt unfair commercial practices⁴⁹⁷ towards consumers.⁴⁹⁸ Given the broad definition given by the Belgian legislator to the notion of commercial practices, and the fact that it applies to the promotion, sale, or supply of products,⁴⁹⁹ there is little doubt that contracts between undertakings and consumers, the object of which is AI, might fall within the scope of application of this Article.

In order to verify whether a commercial practice adopted by an undertaking towards a consumer is unfair, and hence prohibited, a three-step test has to be conducted. Firstly, Articles VI.100 and VI.103 provide lists of practices that are deemed to be, respectively, misleading⁵⁰⁰ or aggressive⁵⁰¹ in any case. Secondly, if the commercial practice is not included in the list, the practice is assessed through the lens of Articles VI.97 to 99, which prohibit several types of misleading practices, and of Articles VI.101 to 102, which prohibit several types of aggressive practices. At this stage, it is also required that the practices materially distort (or will likely materially distort) the economic behaviour⁵⁰² of the average consumers whom it reaches or to whom it is addressed, or of the average member of the group when the commercial practices are directed to a group of consumers, regarding the products at stake. Thirdly, if the commercial practice under assessment is not found to be misleading or aggressive under the previous two steps, the practice has to be analysed in the light of Article VI.93. Under this Article, commercial practices are unfair if they (i) are contrary to the requirements of professional diligence;⁵⁰³ and (ii) substantially distort (or will likely distort substantially) the economic behaviour of the average consumers (or group of consumers) that it reaches or is addressed to, regarding the products at stake.

Although the notion of average consumers is not defined within the Code of Economic Law, nor in legally binding dispositions of Directive 2005/29, Recital 18 of the same Directive provides a definition. This Recital states that “this Directive takes as a benchmark the average consumer, who is reasonably well informed and reasonably observant and circumspect, taking into account social,

⁴⁹⁴ Art. VI.92 to 103 CEL. This set of rules is the Belgian transposition of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council, O.J., L 149.

⁴⁹⁵ Art. VI. 103/1 to 109/3 CEL.

⁴⁹⁶ According to Art. I.8, 39° CEL, this notion can be defined as any legal or natural person that pursues a long-term economic aim, including its associations. Regarding this definition, see also European Court of Justice, judgement *Mannesmann AG v High Authority of the European Coal and Steel Community*, 13 July 1962, C-19/61, EU:C:1962:31.

⁴⁹⁷ According to Art. I.8, 23° CEL, this notion can be defined as any action, omission, behaviour, commercial communication (including advertisement and marketing) from an undertaking, in relation to the promotion, sale, or supply of a product.

⁴⁹⁸ According to Art. I.1, 2° CEL, this notion can be defined as any natural person who is acting for purposes other than trading, industrial, artisanal or liberal activities.

⁴⁹⁹ According to Art. I.1, 4° CEL, this notion can be defined as any good, service, immovable property, right, or obligation.

⁵⁰⁰ According to Art. VI.94, 1° CEL, misleading practices are considered unfair.

⁵⁰¹ According to Art. VI.94, 2° CEL, aggressive practices are considered unfair.

⁵⁰² According to Art. I.8, 25° CEL, this notion can be defined as the use of a commercial practice that appreciably compromises the ability of a consumer to make informed decisions, and hence leads the consumer to make a transactional decision that he would not have taken otherwise.

⁵⁰³ According to Art. I.8, 24° CEL, this notion can be defined the level of skill and care that a trader may reasonably be expected to have towards his consumers, in accordance with honest commercial practices.

cultural and linguistic factors, as interpreted by the Court of Justice”.⁵⁰⁴ If this notion is to be applied to consumers when they conclude contracts with undertakings, having as object AI-products, the average consumers will likely be considered to be in a particularly weak position. That is because AI-systems are complex products for which consumers lack information and knowledge.⁵⁰⁵

Examples of unfair commercial practices, in which AI is the object of contracts concluded between undertakings and consumers, could be the following. An undertaking which supplies personal assistants to its consumers might fail to inform them on the risks for privacy of such a product, especially regarding the use that will be made of consumers’ personal data or the risks for data breaches. Similarly, an undertaking that supplies domestic robots to consumers might fail to inform them on the risks of physical injuries potentially incurred. In both cases, the commercial practices of such undertakings may potentially qualify as misleading, and hence be forbidden.⁵⁰⁶

In addition, a few types of commercial practices relating to AI, which could potentially qualify as unfair, are highlighted by scholars and appear to be relevant for this study. These examples relate to contracts in which undertakings pretend that they will provide AI-powered services to their consumers but instead provide them with human labour. This could, for instance, be the case when a person chats online with a consumer, whereas the consumer concluded a contract with the undertaking providing the service, having for object the supply of a chatbot.⁵⁰⁷ Another type of problematic practice could consist in the supply, by an undertaking, of a translation software allegedly operated by AI but in which the translations are actually made by humans.⁵⁰⁸ Such practices could likely qualify as misleading, under the wording of Article VI.97.⁵⁰⁹

Regarding the sanctions that apply in the case of unfair commercial practices, Article VI.38 provides for two main principles. For most unfair commercial practices, judges have the power to order the reimbursement of consumers, while consumers may keep the products supplied to them.⁵¹⁰ However, in some cases, when the unfair commercial practices are particularly significant, consumers have the right to require the reimbursement of all sums paid and may keep the products supplied to them, without any judge being involved in the process.⁵¹¹ Furthermore, criminal penalties can be imposed as well, which notably includes fines from 26 to 10.000 euros.⁵¹²

B. Unfair Market practices Towards Undertakings

In relations between undertakings,⁵¹³ unfair market practices are prohibited.⁵¹⁴ More specifically, Article VI.104 states that undertakings are forbidden to adopt behaviours contrary to fair market practices, which cause (or could potentially cause) harms to the professional interests of other

⁵⁰⁴ Regarding the Court of Justice case law, see notably European Court of Justice, Judgement *Nemzeti Fogyasztóvédelmi Hatóság*, 16 April 2015, C-388/13, EU:C:2015:225. This wording is also used within Belgian case law, regarding the definition of average consumers. In this regard, see notably Comm. Bruxelles (Prés.), 17 July 2009, *Ann. Prat. Comm.* 2009, p. 144, note H. DE BAUW, and Anvers, 21 November 2012, *Ann. Prat. Comm.* 2012, p. 458.

⁵⁰⁵ H. JACQUEMIN and J.-B. HUBIN, “Aspects contractuels et de responsabilité civile en matière d’intelligence artificielle”, o.c., p. 95.

⁵⁰⁶ Art. VI.97, 2° CEL.

⁵⁰⁷ H. JACQUEMIN and J.-B. HUBIN, “Aspects contractuels et de responsabilité civile en matière d’intelligence artificielle”, o.c., p. 96.

⁵⁰⁸ Ch. HOLDER, V. KHURANA, F. HARISSON and L. JACOBS, “Robotics and law: Key legal and regulatory implications of the robotics age (Part I of II)”, *Computer Law and Security Review* 2016, vol. 32, no. 3, p. 396.

⁵⁰⁹ Art. VI.97, 1° CEL.

⁵¹⁰ Art. VI.38, al. 2 CEL.

⁵¹¹ Art. VI.38, al. 1 CEL.

⁵¹² Art. XV.83, 13°, and XV.70, al. 3 CEL.

⁵¹³ According to Art. I.8, 39° CEL, this notion can be defined as any legal or natural person that pursues a long-term economic aim, including its associations. Regarding this definition, see also European Court of Justice, judgement *Mannesmann AG v High Authority of the European Coal and Steel Community*, 13 July 1962, C-19/61, EU:C:1962:31.

⁵¹⁴ Art. VI.104 CEL.

undertakings. Moreover, Article VI.104/1 states that market practices adopted by undertakings towards other undertakings are unfair whenever such practices are misleading⁵¹⁵ or aggressive.⁵¹⁶ It makes little doubt that practices similar to those described above (see part 3.2.3. section A) taking place between undertakings rather than involving consumers, would also qualify as unfair market practices. For instance, if an undertaking provides incorrect or voluntarily false information to its customers (i.e. other undertakings) about the existence, capabilities, and limits of the AI-systems that are the object of a contract between them, such practice could potentially qualify as misleading, and hence be forbidden.⁵¹⁷

Regarding applicable sanctions, criminal penalties can be decided, which notably includes fines from 26 to 10.000 euros.⁵¹⁸ Moreover, interested parties such as undertakings subject to unfair market practices,⁵¹⁹ and the Minister that has competence for Economy and Middle Classes,⁵²⁰ may require judges to issue orders of cessation towards unfair market practices.

3.2.4. Liability for Defective Products

In terms of liability for defective products, the legal framework is composed of the Act of 25 February 1991 (Product Liability Act),⁵²¹ which transposes the Directive 85/374/EEC (Product Liability Directive)⁵²² Article 2 defines products as any movable goods, including goods that are incorporated to other movable goods, or to goods incorporated in immovable goods, and goods that became immovable by means of incorporation. Although this definition does not clearly state it, software should normally be encompassed in the notion.⁵²³ This means that AI-systems (be they included in a tangible medium or not) are, most likely, included in the scope of application of the law.⁵²⁴

The main principle of this framework is stated within Article 1, which attributes liability for damages caused by defective products to their producers.⁵²⁵ Where producers cannot be identified, suppliers of defective products are considered as producers, and hence can be held liable.⁵²⁶

Regarding the notion of default in a product, Article 5 states that a product is defective when it does not provide the safety that could legitimately be expected from it (cf. legitimate expectations), taking into account (i) the packaging/presentation of the product; (ii) the use made of the product, which should be normal or at least reasonable; and (iii) the moment when the product was placed on the market. The criterion of legitimate expectations remains very vague. It gives judges a wide margin of appreciation. As a consequence, it is difficult to predict how this

⁵¹⁵ Within the meaning of Art. VI.105 to 109 CEL.

⁵¹⁶ Within the meaning of Art. VI.109/1 to 109/3 CEL.

⁵¹⁷ Art. VI.105, 1° and 2° CEL.

⁵¹⁸ Art. XV.83, 13/1° and XV.70, al. 3 CEL.

⁵¹⁹ Art. XVII.7, 1° CEL.

⁵²⁰ Art. XVII.7, 2/2° CEL.

⁵²¹ Act of 25th February 1991 on the liability for defective products, *M.B.*, 22 March 1991.

⁵²² Directive 85/374/EEC of the Council of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, *O.J.*, L 210.

⁵²³ See *Projet de loi relatif à la responsabilité des produits défectueux*, *Doc. Parl.*, Ch. repr., sess. ord. 1989-1990, n°1262/5, p. 4-6.

⁵²⁴ H. JACQUEMIN and J.-B. HUBIN, "Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle", *o.c.*, p. 129-130.

⁵²⁵ According to Art. 3 Product Liability Act, this notion can be defined as the manufacturer of a finished product, the manufacturer of a component part of a finished product, or the producer of any raw material, as well as any persons that present themselves as manufacturer or producer, by marking the product with their names, their trademarks, or any other distinctive feature. In addition, Art. 4 provides that any persons who, as part of their economic activities, imports products within the EU in order to sell it or distribute it in any other way, is to be considered as a producer, and will also be liable.

⁵²⁶ Art. 4, § 2 Product Liability Act.

criterion will be applied in the context of AI-systems. The safety expectations will be very high for AI-systems used in high-risk contexts such as healthcare or mobility. At the same time, however, the concrete application of this test remains difficult for AI-systems because of their novelty, the complexity to compare these systems with human or technological alternatives and the characteristics of autonomy and opacity.⁵²⁷ Additional clarification on the notion of defect may thus be required.

In the case where a defective product causes damages, it is up to the injured person⁵²⁸ to carry the burden of proof and demonstrate the existence of a default within the product, alongside with the damage suffered and the causal relationship between both.⁵²⁹ If the injured person successfully proves these three elements, the producer of the defective product has the obligation to reimburse damages caused to persons⁵³⁰ as well as damages caused to any item of property.⁵³¹ Injured persons have to act within three years from the moment when they find out about the existence of the damage, the default and the identity of the producer, or within three years from the moment they should reasonably have found out. In any case, injured persons have ten years from the moment when the product is placed on the market for their action to be admissible.⁵³² However, producers can avoid liability if they manage to prove, among other things, that (i) the default which caused damages did not exist at the moment when the product was placed on the market or at least that the default appeared later; or (ii) the state of scientific and technical knowledge, at the moment when the product was placed on the market, was not sufficient to enable the discovery of the default.⁵³³

Scholars have highlighted several potential issues with this framework in relation to product liability and AI.⁵³⁴ Such concerns notably relate to the definition of the producer, the burden of proof, the possibilities left to producers to avoid liability and the period left for injured persons to act. These elements are briefly discussed in the following paragraphs. It should be noted that the need to ensure adequacy of the rules on liability for defective products to AI and other technological developments is currently taken care of at the EU level. This notably stems from the evaluation of Directive 85/374 conducted in 2018,⁵³⁵ from the report of the Expert Group on Liability and New Technologies in 2019,⁵³⁶ from the EC's white paper on Artificial Intelligence in 2020,⁵³⁷ and from the EC's report on the safety and liability implications of AI, the Internet of Things, and robotics in 2020 as well.⁵³⁸

⁵²⁷ J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems", *o.c.*, p. 381.

⁵²⁸ This notion is not defined within the legal text.

⁵²⁹ Art. 7 Product Liability Act.

⁵³⁰ Art. 11, § 1 Product Liability Act., which encompasses both material and moral damages.

⁵³¹ Art. 11, § 1 Product Liability Act. The reimbursement of this type of damages is however limited, as it does not include damages caused to the defective product itself. In addition, the producer of the defective product deduces 500 euros from the total amount due to the injured person. See Art. 11, § 2 Product Liability Act.

⁵³² Art. 12 Product Liability Act.

⁵³³ Art. 8, b) and e) Product Liability Act.

⁵³⁴ H. JACQUEMIN and J.-B. HUBIN, "Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle", *o.c.*, p. 130-138. The following developments are mainly inspired by this research. See also B. BENICHOU, T. GILS, J. DE BRUYNE, and E. WAUTERS, "Regulating AI in the European Union: Seven Key Takeaways", 2020, available at <https://ai-laws.org/en/2020/05/an-eu-perspective-on-liability-and-artificial-intelligence/>; J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems", *o.c.*, p. 359-402.

⁵³⁵ European Commission, "Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products", 2018.

⁵³⁶ Expert Group on Liability and New Technologies, "Liability for Artificial Intelligence and Other Emerging Technologies", 2019, available at

<https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>.

⁵³⁷ European Commission, "White Paper on Artificial Intelligence – A European Approach to excellence and trust", *op cit*.

⁵³⁸ European Commission, "Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee – Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics", 19th February 2020, COM(2020) 64 final.

The notion of producers is extremely broad but does not necessarily encompass all actors that intervene in the process of training and developing AI-systems. Although all the actors that have a role to play until AI-systems are placed on the market are likely to qualify as producers, some actors might still intervene after the systems are marketed. This could be the case because AI-systems might need to be trained more than once or might need a continuous training after they are placed on the market. Actors that would play this role would have significant impact on the risk of accidents, while not being liable as producers within the meaning of the law if accidents happen. As such, there is some uncertainty regarding the allocation of responsibilities between different economic operators in the supply chain of AI-systems. Several parties can be involved such as the developers of the software/ algorithm, the producer of the hardware, owners/keepers of the AI product, suppliers of data, public authorities and the users of the product. Persons who have suffered harm may not have effective access to the evidence that is necessary to build a case in court and may have less effective redress possibilities compared to situations where the damage is caused by 'traditional' products.⁵³⁹

Regarding the burden of proof, it may be challenging for injured persons. They may not necessarily have the required knowledge on AI-technology to prove that an accident was caused by a default of their AI-products. Although it is in Belgium accepted that a default can be deduced from an abnormal behaviour of the product at stake without having to prove the existence of the default itself from a technical perspective,⁵⁴⁰ injured persons may not be aware when an AI-system behaves abnormally. This might cause injured persons to incur high expenses, to obtain expert reports or deter victims to claim the application of their rights.⁵⁴¹

Moreover, pursuant to Article 8(b) producers may avoid liability if they succeed to prove that defaults did not exist within their products when they were first put into circulation or that this defect came into being afterwards. The notion of 'putting into circulation' can be challenging for products incorporating software or AI-systems that may change over time. The self-learning and autonomous nature of AI-systems has a continuous 'production process', even without external interaction.⁵⁴² As AI-systems are characterised by their learning capabilities, producers could invoke this defence to attempt to escape liability when accidents are caused by AI-systems due to their learning processes. The question that arises, hence, is to what extent defaults already existed at the time of marketing, or solely came to existence after that the products were marketed. In this regard, the Expert Report by the European Commission stipulates that the producer should remain liable where the defect has its origin (a) in a defective digital component or digital ancillary part or in other digital content or services provided for the product with the producer's assent after the product has been put into circulation; or (b) in the absence of an update of digital content, or of the provision of a digital service which would have been required to maintain the expected level of safety within the time period for which the producer is obliged to provide such updates. The producer should thus be strictly liable for defects in emerging digital technologies even if these defects appear after the product was put into circulation, as long as the producer was still in control of updates to or upgrades of the technology.⁵⁴³ Additional clarification may thus be required.

Similarly, producers may avoid liability if they prove that the state of scientific and technical knowledge was not sufficient to discover the defaults. at the moment when the product was

⁵³⁹ European Commission, "On Artificial Intelligence – A European approach to excellence and trust", o.c., p. 13

⁵⁴⁰ Civ. Namur, 21 November 1996, *J.L.M.B.* 1997, p. 104.

⁵⁴¹ This element was already raised within the European Commission's report from 2011 on the application of Directive 85/374/EEC, although this point was made in general, and not in relation to AI. See European Commission, "Fourth report on the application of Directive 85/374/EEC of the Council of 25 July 1985 on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products, modified by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999", COM(2011) 547, p. 7.

⁵⁴² J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems", o.c., p. 386.

⁵⁴³ Expert Group on Liability and New Technologies, New Technologies Formation, "Liability for Artificial Intelligence and Other Emerging Digital Technologies", o.c., p. 42-44.

placed on the market. This defence may become more important considering that producers of sophisticated AI-systems will probably frequently invoke it to refute liability. The question, however, is how this defence should be applied with regard to AI-systems. Due to the autonomous nature of AI-systems, their behaviour is not entirely foreseeable. Nevertheless, the fact that damage will occur is foreseeable.⁵⁴⁴ The Expert Report eventually concludes that the development risk defence should not be available in cases where it was predictable that unforeseen developments might occur.⁵⁴⁵ In this regard, the (self-)learning capabilities of AI-systems or even the lack of technical knowledge on the effects of such technology might be used by producers to avoid liability, thereby hampering the protection of injured persons

Finally, regarding the time left for injured persons to act, the duration provided by the Product Liability Act might be problematic when it comes to AI-systems (i.e. ten years from the moment when the product is first placed on the market). Given the fact that AI-systems have a learning feature, their capabilities should in principle increase over time. Hence, they may be used much longer than other types of products, which face physical constraints and deterioration because of their use. AI-systems might potentially also cause damages for longer periods of time than ten years.

3.3. AI is Used to Conclude the Contract

In this part, the application of consumer protection rules to AI is analysed when it is used to conclude a contract with a consumer.⁵⁴⁶ More specifically, AI is relied upon by an undertaking⁵⁴⁷ to automate the conclusion of contracts with its consumers or even to conclude such contracts in an autonomous manner. This hypothesis potentially covers a wide number of situations as consumer contracts concluded by AI could have countless objects in virtually any field of human activity, and cover goods,⁵⁴⁸ services,⁵⁴⁹ products,⁵⁵⁰ or digital content.⁵⁵¹ This part of the study also considers, where applicable, the hypothesis in which AI-systems autonomously conclude contracts with undertakings, on the behalf of consumers. This could be the case if a consumer buys a smart fridge from an undertaking A, where the smart fridges autonomously orders fresh food items from undertakings A, B and/or C when it is empty, without any active intervention from the consumers.

As a preliminary remark, it should be noted that in addition to the legal qualifications referred to above, and in addition to the general legal rules studied in this chapter, sector-specific rules can apply as well depending on the purposes/sectors for which AI is used to conclude contracts with consumers. For instance, the rules on the protection of investors might apply if an undertaking uses AI to autonomously conclude investment contracts with investors.⁵⁵² In addition, it should be noted that AI-systems relied upon by undertakings to conclude contracts may impose unfair terms

⁵⁴⁴ J. DE BRUYNE, E. VAN GOOL and T. GILS, "Tort Law and Damage Caused by AI Systems", o.c., p. 359-402.

⁵⁴⁵ Expert Group on Liability and New Technologies, *New Technologies Formation*, "Liability for Artificial Intelligence and Other Emerging Digital Technologies", o.c., p. 42-43; H. JACQUEMIN and J.B. HUBIN, "Aspects contractuels et de responsabilité civile en matière d'intelligence artificielle", o.c., p. 137;

⁵⁴⁶ According to Art. I.1, 2° CEL, this notion can be defined as any natural person who is acting for purposes other than trading, industrial, artisanal or liberal activities.

⁵⁴⁷ According to Art. I.8, 39° CEL, this notion can be defined as any legal or natural person that pursues a long-term economic aim, including its associations. Regarding this definition, see also European Court of Justice, judgement *Mannesmann AG v High Authority of the European Coal and Steel Community*, 13 July 1962, C-19/61, EU:C:1962:31.

⁵⁴⁸ According to Art. I.1, 6° CEL, this notion can be defined as any tangible movable item.

⁵⁴⁹ According to Art. I.1, 5° CEL, this notion can be defined as any performance of an undertaking, in relation to its professional activity, or to achieve its statutory objectives.

⁵⁵⁰ According to Art. I.1, 4° CEL, this notion can be defined as any good, service, immovable property, right, or obligation.

⁵⁵¹ According to Art. I.8, 35° CEL, this notion can be defined as data which are produced and supplied in digital form.

⁵⁵² See notably Act of 2 August 2002 on the monitoring of the financial sector and financial services, *M.B.*, 4 September 2002.

to consumers, despite the legal prohibition of such practices.⁵⁵³ Yet, the legal rules regarding the prohibition of unfair terms in consumer contracts do not face specific issues when it comes to AI. Hence, these rules will not be studied in details within the following paragraphs. Instead, the study will focus on the use of automated means for prospection (part 3.3.1.), information obligations (part 3.3.2.), unfair commercial practices (part 3.3.3.) and requirements for consent (part 3.3.4.).

3.3.1. Use of Automated Means for Prospection

In most cases, contracts involving AI and consumers⁵⁵⁴ will likely be concluded online on the website of the undertaking.⁵⁵⁵ Such contracts might also be concluded in physical places (e.g. shops) in which consumers would interact with robots powered by AI. In these two hypothesis, consumers would initiate the process and enter in communication with an undertaking's AI-systems, either by going on the undertakings' websites or visit the latter's shops.

Another hypothesis occurs when AI is used for prospection, to conclude contracts with consumers. For instance, AI might profile⁵⁵⁶ consumers on the basis of all previously collected data by the undertaking (e.g. consumers' buying behaviours) and subsequently target consumers to propose specific products and conclude a contract. Undertakings can use AI to conclude contracts with consumers by using various channels such as phone calls, emails, targeted advertising, etc. Applicable rules on this practice are notably contained within Article VI.110 of the Code of Economic Law. They apply without a doubt to AI as Article VI.10 focuses on faxes and any type of automated system used to make calls. According to this Article, the use of faxes and automated systems to make calls with a purpose of direct prospection is forbidden, unless the recipient of the fax or call consented to such communications. The same principle applies for emails following Article XII.13. It is forbidden for undertakings (and hence for the AI-systems they use) to send emails with a purpose of direct prospection, unless the recipient of the email consented to such communications.

However, exceptions to this principle exist. When three cumulative conditions are met, undertakings (or the AI-systems they rely upon) may send emails to consumers for prospection purposes without having received recipients' consent. These conditions are: (i) the undertaking has legally obtained the consumers' email address, through the supply of a product or service to him; (ii) the advertising is limited to products or services provided by the undertaking itself, which are similar to the products or services already purchased by the consumer; and (iii) consumers that receive advertising emails must be able oppose to further prospection.⁵⁵⁷ In such cases, AI may be used by undertakings to prospect potential customers among consumers, and eventually conclude contracts with them.

Although there is no specific civil sanction when the rules described in this section are not respected, the sanctions applicable to unfair commercial practices might apply (see above part 3.2.3, section A).

⁵⁵³ Art. VI.82 to VI. 87, CEL.

⁵⁵⁴ According to Art. I.1, 2° CEL, this notion can be defined as any natural person who is acting for purposes other than trading, industrial, artisanal or liberal activities.

⁵⁵⁵ According to Art. I.8, 39° CEL, this notion can be defined as any legal or natural person that pursues a long-term economic aim, including its associations. Regarding this definition, see also European Court of Justice, judgement *Mannesmann AG v High Authority of the European Coal and Steel Community*, 13 July 1962, C-19/61, EU:C:1962:31.

⁵⁵⁶ According to Art. 4, (4) GDPR: "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

⁵⁵⁷ Art. 1, Arrêté Royal of 4 April 2003 on the use of emails for advertising purposes, M.B., 28 May 2003.

3.3.2. Information Obligations

In terms of information obligations, when AI is used to conclude contracts with consumers or on their behalf, the relevant legal rules are relatively similar to those analysed above (see part 3.2.2). The legal framework in consumer protection law is, once again, mainly constituted by provisions of Book VI of the Code of Economic Law, which transposes Directive 2011/83 in Belgium. In addition, Directive 2019/2161⁵⁵⁸ creates some new information obligations within Directive 2011/83 which will most likely apply to AI when used to conclude contracts with consumers. The legal framework also includes a few provisions in Directives 2019/770 and 2019/771, which are not yet transposed within Belgian law. Further information obligations might in the near future also be imposed due to the European Commission's Proposal for a Digital Services Act (DSA).⁵⁵⁹

All these information obligations regarding AI arising from consumer protection law will be examined (part A.). Additionally, consumers that qualify as data subjects⁵⁶⁰ in the meaning of the GDPR may need to be given additional information by the AI-systems in order to conclude contracts. Here again, the automated processing of personal data might trigger specific additional information obligations (e.g. in the case of fully automated decisions that produce legal effects for data subjects), which might be the case when a consumer concludes a contract with an AI-system. Hence, information obligations arising from the field of data protection will be examined as well in relation to AI (part B.).

A. Consumer Protection Law

- Code of Economic Law

In the case in which contracts are concluded with consumers⁵⁶¹ by autonomous AI-systems to the benefit of the undertakings⁵⁶² using such systems, information obligations imposed by Book VI of

⁵⁵⁸ Directive 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, *O.J.*, L 328.

⁵⁵⁹ European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31, COM(2020) 825 final, 15 December 2020.

⁵⁶⁰ According to Art. 4, (1) GDPR: "an identifiable natural person [, i.e. a natural person] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

⁵⁶¹ According to Art. I.1, 2° CEL, this notion can be defined as any natural person who is acting for purposes other than trading, industrial, artisanal or liberal activities.

⁵⁶² According to Art. I.8, 39° CEL, this notion can be defined as any legal or natural person that pursues a long-term economic aim, including its associations. Regarding this definition, see also European Court of Justice, judgement *Mannesmann AG v High Authority of the European Coal and Steel Community*, 13 July 1962, C-19/61, EU:C:1962:31.

the Code of Economic Law may apply. Depending on the type of contract at stake, the applicable provisions will be included in Article VI.2,⁵⁶³ Article 45⁵⁶⁴ and Article 64.⁵⁶⁵

Indeed, as undertakings *prima facie* seek to conclude contracts with consumers by relying on AI, they have to make sure that these systems will comply with the information obligations throughout the process of concluding contracts in an autonomous manner. In this regard, the lists of information to be given to consumers does not raise specific concerns.

In the case in which contracts are concluded with undertakings, by autonomous AI-systems, and on the behalf of consumers, information obligations imposed by Book VI of the Code of Economic Law may also apply, so that undertakings have to provide consumers' AI-systems with several information. As such contracts will most likely be distance contracts,⁵⁶⁶ the applicable provisions will be included in Article VI. 45. In this regard, the list of information to be given to consumers does not raise specific concerns either.⁵⁶⁷

Furthermore, in this hypothesis, it should be noted that undertakings who supply consumers with AI-systems able to autonomously conclude contracts with third parties, have to respect the information obligations detailed in part 3.2.2, Section A of the study, in the first place.⁵⁶⁸ Such undertakings also have to respect legal rules on warranty, if the autonomous AI-systems supplied to consumers to conclude contracts on their behalf lack conformity (for a detailed analysis of legal rules on warranty regarding AI, see part 3.2.1 of the study). For instance, if a smart fridge autonomously orders more food than the consumer wishes, warranty obligations might apply.⁵⁶⁹

Once again, there are no specific civil sanctions that apply when most of these information obligations are not respected by companies or by AI-systems deployed by undertakings to conclude consumer contracts. Yet, regarding the right of withdrawal,⁵⁷⁰ if no information is provided to consumers, Articles VI.48 and 68 state that the right of withdrawal is extended for a duration up to twelve months. This period starts fourteen days after the delivery or supply. In

⁵⁶³ This Article applies to all contracts other than distance or off-premises contracts. It could be applicable regarding AI, notably in situations where consumers conclude contracts with AIs such as robots in physical stores (e.g. in a supermarket where cashiers would be replaced by robots).

⁵⁶⁴ This Article applies to distance contracts. According to Art. I.8, 15° CEL, this notion can be defined as any contract concluded between an undertaking and a consumer, relating to sales or services provided at distance, where the consumer and the undertaking are not physically simultaneously present, through the use of distance communication techniques. It could be applicable regarding AI, notably in situations where consumers conclude contracts with AIs online (e.g. on the website of a seller).

⁵⁶⁵ This Article applies to off-premises contracts. According to Art. I.8, 31° CEL, this notion can be defined as any contract between a consumer and an undertaking, (i) concluded in the simultaneous physical presence of the undertaking and of the consumer, in a place which is not the commercial establishment of the undertaking; (ii) where the consumer made an offer to the undertaking in the simultaneous physical presence of the undertaking and of the consumer, in a place which is not the commercial establishment of the undertaking; (iii) concluded in the commercial establishment of the undertaking, through the use of distance communication techniques, immediately after the consumer was personally and individually solicited by the undertaking, both parties being simultaneously physically present, in a place which is not the commercial establishment of the undertaking before the conclusion of the contract; (iv) concluded during an outing, the objective or effect of which is to promote and sell goods or services to consumers. It could be applicable regarding AI, notably in situations where consumers conclude contracts with AIs such as robots during an outing (e.g. in a fair where sellers would be replaced by robots).

⁵⁶⁶ E.g. where a smart fridge autonomously orders food items for a consumer, it does so online. Hence, this operation qualifies as a distance contract.

⁵⁶⁷ At this stage, there seems to be no binding rule, within consumer protection law, that forbids AI-systems to autonomously conclude contracts with undertakings on the behalf of consumers. If something goes wrong in the use of such AI-systems (for instance, if a smart fridge orders too much food), the legal rules on warranty may apply where a lack of conformity exists, and the supplier of the AI-system could be held liable. In addition, contract law and correlative consumer protection rules could apply as well (e.g. the prohibition of abusive clauses in contracts towards consumers).

⁵⁶⁸ Notably by providing extensive and detailed information on the main characteristics of the good or service (Art. VI. 45, 1°, CEL).

⁵⁶⁹ In this regard, it should be noted that risks for consumers will likely be limited, where a smart fridge lacks conformity and orders too much food. Yet, in domains such as the financial sector, higher risks might occur for consumers (e.g. important losses due to faulty investments made by an AI on the behalf of a consumer).

⁵⁷⁰ This right is only applicable in the case of distance and off-premises contracts, as provided for in Art. VI.45, § 1, 8°, and VI.64, § 1, 7°, CEL.

addition, if the lack of information can be considered as a misleading commercial practice, the sanctions applicable to unfair commercial practices might apply (see above part 3.2.3. section A).⁵⁷¹ Moreover, it should be noted that the King might impose complementary measures, in accordance to Articles VI.9 and 10, to ensure a high level of commercial fairness and consumer protection for the sale of goods and the supply of services. Such complementary measures may consist of information obligations, which AI-systems concluding contracts with consumers would have to respect as well. For instance, the King could decide how packages should be presented and what mentions they should bear to be lawfully placed on the market.⁵⁷²

- Directive 2019/2161

Regarding the information obligations created by Directive 2019/2161,⁵⁷³ two requirements are added within the list of information under Directive 2011/83 to be supplied by traders⁵⁷⁴ to consumers⁵⁷⁵ in the case of distance⁵⁷⁶ and off-premises contracts.⁵⁷⁷

Firstly, Directive 2019/2161 adds the requirement for undertakings to inform their consumers, where applicable, “that the price was personalised on the basis of automated decision-making”.⁵⁷⁸ Thereby, when AI modifies the price of goods,⁵⁷⁹ services⁵⁸⁰, or digital content⁵⁸¹ proposed to a consumer, such information needs to be supplied to the consumer in addition to other information required in the case of distance and off premises contracts.⁵⁸²

It should be highlighted that this information obligation does not apply in relation to contracts other than distance or off-premises contracts. Although there are currently not many cases in which AI-systems conclude such types of contracts with consumers and personalise prices to be paid, this might constitute a gap within European rules. It creates a difference of treatment on the basis of the type of contract concluded (i.e. distance and off-premises contracts vs. other

⁵⁷¹ See Art. VI.38 CEL. See also N. GILLARD, “Protection des consommateurs”, o.c., p. 24.

⁵⁷² Art. VI.9, § 1, 1° CEL.

⁵⁷³ Directive 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, O.J., L 328. This Directive should be transposed within Member States’ law by 28 November 2021 at the latest. From 28 May 2022, Member States’ national laws transposing the Directives have to apply.

⁵⁷⁴ According to Art. 2, (2) Directive 2011/83: “any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive”.

⁵⁷⁵ According to Art. 2, (1) Directive 2011/83: “any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession”.

⁵⁷⁶ According to Art. 2, (7) Directive 2011/83: “any contract concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded”.

⁵⁷⁷ According to Art. 2, (8) Directive 2011/83: “any contract between the trader and the consumer: (a) concluded in the simultaneous physical presence of the trader and the consumer, in a place which is not the business premises of the trader; (b) for which an offer was made by the consumer in the same circumstances as referred to in point (a); (c) concluded on the business premises of the trader or through any means of distance communication immediately after the consumer was personally and individually addressed in a place which is not the business premises of the trader in the simultaneous physical presence of the trader and the consumer; or (d) concluded during an excursion organised by the trader with the aim or effect of promoting and selling goods or services to the consumer”.

⁵⁷⁸ New Art. 6, § 1, (ea) Directive 2011/83.

⁵⁷⁹ According to Art. 2, (3) Directive 2011/83, as modified by Directive 2019/2161: “(a) any tangible movable items; water, gas and electricity are to be considered as goods within the meaning of this Directive where they are put up for sale in a limited volume or a set quantity; (b) any tangible movable items that incorporate or are inter-connected with digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions (‘goods with digital elements’).”

⁵⁸⁰ According to Art. 2, (6) Directive 2011/83, the notion of service contract is defined as “any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof”.

⁵⁸¹ According to Art. 2, (1), Directive 2019/770 : “data which are produced and supplied in digital form”.

⁵⁸² For a complete overview on the practice of price personalisation, see F. JACQUES, “Personnalisation des prix – Regard européen sur la pratique”, *R.D.T.I.* 2020, n°78-79, p. 53-90.

contracts). Yet, the risks for consumers facing personalised prices are likely the same regardless of whether the contract is a distance or off-premises contract or not.

Secondly, Directive 2019/2161 adds a new Article 6a within Directive 2011/83. It imposes to online marketplaces⁵⁸³ the obligation to provide several information to consumers before they are bound by any distance contract. The new Article 6a of Directive 2011/83 will apply when online marketplaces use AI to automate the conclusion of contracts between third party traders and consumers having as their object goods, services or digital content. Among other information, this provision requires online marketplaces to provide consumers with “general information on the main parameters determining ranking [...] of offers presented to the consumer[s] as a result of the[ir] search quer[ies] and the relative importance of those parameters as opposed to other parameters”.⁵⁸⁴ Given the fact that ranking⁵⁸⁵ parameters are in most cases decided and adapted by automated (or autonomous) AI-systems, it is very likely that online marketplaces will have to provide information on the main ranking parameters⁵⁸⁶ of their AI-systems to their consumers, when this provision applies.

For both information obligations imposed by Directive 2019/2161, there is at this stage no applicable sanction, given the fact that they have not been transposed within Belgian law yet.

- Directives 2019/770 and 2019/771

Regarding the information requirements arising from Directives 2019/770 and 2019/771 (see part 3.2.2 section A), it seems clear that AI-systems concluding contracts with consumers⁵⁸⁷ should provide the required information. The same reasoning as the one previously discussed with regard to the provision of information should be followed. If AI-systems used for the conclusion of contracts fail to comply with these information obligations, the object of the contracts between professional traders⁵⁸⁸ and/or sellers⁵⁸⁹ and consumers will not satisfy to objective conformity requirements.⁵⁹⁰ As a result, consumers will be allowed to require the application of remedies described in part 3.2.1 section B.

- European Commission’s Digital Services Act Proposal

⁵⁸³ According to the new Art. 2, (17) Directive 2011/83: “a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers”.

⁵⁸⁴ New Art. 6a, § 1, (a) Directive 2011/83.

⁵⁸⁵ According to the new Art. 2, (1), (m) Directive 2005/29, to which the new Art. 6a, § 1, (a), Directive 2011/83 refers: “the relative prominence given to products, as presented, organised or communicated by the trader, irrespective of the technological means used for such presentation, organisation or communication”.

⁵⁸⁶ According to Recital 22 Directive 2019/2161: “any general criteria, processes, specific signals incorporated into algorithms or other adjustment or demotion mechanisms used in connection with the ranking”.

⁵⁸⁷ According to Art. 2, (6), Directive 2019/770 and Art. 2, (2) Directive 2019/771: “any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person's trade, business, craft, or profession”.

⁵⁸⁸ According to Art. 2, (5) Directive 2019/770: “any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft, or profession, in relation to contracts covered by this Directive”.

⁵⁸⁹ According to Art. 2, (3) Directive 2019/771: “any natural person or any legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft or profession, in relation to contracts covered by this Directive”.

⁵⁹⁰ Art. 8, Directive 2019/770, and Art. 7, Directive 2019/771.

Finally, the European Commission's DSA Proposal seeks to impose several information obligations to online platforms⁵⁹¹ and very large online platforms.⁵⁹² As this legislative proposal is still at its preliminary stage, and will likely be modified through the legislative process, the following paragraphs only provide a short overview of the relevant proposed substantive rules rather than a detailed analysis.

According to Article 22, online platforms would have to collect and verify information regarding traders whenever they allow consumers⁵⁹³ to conclude distance contracts (within the meaning of Directive 2011/83) with traders.⁵⁹⁴ Such information includes among others the traders' names, addresses, phone numbers and trade register numbers.⁵⁹⁵ In addition, online platforms would have to communicate part of the information collected and verified to consumers.⁵⁹⁶ Where online platforms use AI to automate the conclusion of contracts between consumers and traders through the platforms, the AI-systems would have to respect this information obligation towards consumers.

Furthermore, very large platforms using recommender systems⁵⁹⁷ would have to set out in their terms and conditions the main parameters used in their recommender systems, alongside with information on "any options for the recipients of the service[s] to modify or influence those main parameters that they may have made available, including at least one option which is not based on profiling".⁵⁹⁸ Given the fact that recommender systems' parameters are in the vast majority of cases decided and adapted by AI-systems, it is likely that very large online platforms would have to provide information on the main parameters of their AI-systems to users (which can be consumers), where this provision would apply.

Another information obligation that lies in the European Commission's DSA Proposal relates to online advertising. According to Article 30, very large online platforms would have to make publicly available for one year after display, a repository containing (i) the content of the advertising displayed; (ii) the person on whose behalf the advertising was displayed; (iii) the period during which the advertising was displayed; (iv) if applicable, the particular group(s) of recipients that were targeted, and the parameters used for that purpose; and (v) the total number of recipients of the advertising. As online advertising is mostly made through the use of AI, it is once again likely that very large online platforms would have to provide information on their advertising strategies to users (which will often be consumers).

Before turning to information obligations arising under data protection law, one remark should be made. Although there is, so far, a large set of information obligations that might be applicable when AI-systems conclude contracts with consumers, it should be noted that no general obligation exists within consumer protection law requiring undertakings to inform consumers of the fact that they

⁵⁹¹ According to Art. 2, (h) DSA Proposal: "a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation".

⁵⁹² According to Art. 25 DSA Proposal: "online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph 3".

⁵⁹³ According to Art. 2, (c) DSA Proposal: "any natural person who is acting for purposes which are outside his or her trade, business or profession".

⁵⁹⁴ According to Art. 2, (e) DSA Proposal: "any natural person, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession".

⁵⁹⁵ For a detailed list, see Art. 22, § 1, (a) to (f) DSA Proposal.

⁵⁹⁶ Art. 22, § 6 DSA Proposal.

⁵⁹⁷ According to Art. 2, (o) DSA Proposal: "a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed".

⁵⁹⁸ Art. 29 DSA Proposal.

are concluding a contract with an AI rather than with a human. Currently, it is only indirectly, and solely in specific cases, that consumers legally benefit from information on the fact that they are in contact with AI-systems rather than humans (that is to say, when personalised prices are used or when ranking is made by an online marketplace).⁵⁹⁹ Furthermore, consumers do not benefit either from a right to an explanation of the actions taken by an AI-system towards them in the process of concluding a contract, at least from consumer protection law.⁶⁰⁰ Hence, this may constitute a gap in the existing substantial rules of consumer protection that needs to be addressed.

B. Data Protection Law

As a matter of fact, when European consumers (i.e. data subjects)⁶⁰¹ deal with AI-systems in the conclusion of contracts, there is necessarily a processing⁶⁰² of the consumers' personal data⁶⁰³ by these systems. Hence, the GDPR will apply to such processing.⁶⁰⁴ For instance, for AI to conclude a contract with a consumer, the system will at some point need to have access to the name, the address, the email address and the banking information of the consumer.

For information obligations contained in the GDPR to apply to undertakings deploying AI and benefit to consumers, undertakings have to qualify as data controllers. A data controller is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".⁶⁰⁵ It makes no doubt that undertaking will in almost any cases qualify as such in their relations with consumers.⁶⁰⁶

Thereby, the information obligations set out in Articles 13 and/or 14 have to be respected by undertakings that qualify as data controllers.⁶⁰⁷ Among the information that has to be provided to data subjects, Articles 13 and 14 of the GDPR mention "the existence of automated decision-making, including profiling, referred to in Article 22 [...] and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".⁶⁰⁸ Automated decision-making, within the meaning of Article 22, encompasses fully automated decisions that will produce legal effects concerning data subjects or will similarly significantly affect them. Where undertakings use AI to conclude contracts with consumers, this legal qualification could be met very often, given the fact that contracts produce legal effects, and may in any case have significant effects on consumers that conclude these contracts with AI-systems.⁶⁰⁹ For instance, where an AI is used by an undertaking

⁵⁹⁹ Such a right exists within data protection law, but only where a fully automated decision, which has legal or otherwise significant effects on the data subject, is made (see below, part 3.3.2. section B). Hence, this information is also limited to specific cases rather than a general obligation.

⁶⁰⁰ However, there might be such a right that arises from data protection law, see below, part 3.3.2. section B.

⁶⁰¹ According to Art. 4, (1) GDPR: "an identifiable natural person [, i.e. a natural person] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

⁶⁰² According to Art. 4, (2) GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

⁶⁰³ According to Art. 4, (1) GDPR: "any information relating to an identified or identifiable natural person".

⁶⁰⁴ In relation to the scope of application of the GDPR, see Art. 2 and 3.

⁶⁰⁵ Art. 4, (7) GDPR.

⁶⁰⁶ C. DE TERWANGNE, "Définitions clefs et champ d'application du RGPD", *o.c.*, p. 67-68.

⁶⁰⁷ Both Articles have similar requirements, the difference between them being that Art. 13 applies when personal data are collected directly from data subjects, while Article 14 applies when personal data are collected indirectly (i.e. from another source than the data subject).

⁶⁰⁸ Art. 13, § 2, f), and 14, § 2, g) GDPR.

⁶⁰⁹ See Article 29 Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", *WP 251rev.01*, 3 October 2017, revised on 6 February 2018, p. 21-22.

to decide whether a bank will allow a consumer to receive a credit or not, the legal qualification of automated decision-making will very likely be held.

In such cases, part of the literature considers that data subjects also have the right to receive an explanation of such automated-decisions, in addition to meaningful information on the logic involved.⁶¹⁰ Yet, not all authors agree upon the existence of this right.⁶¹¹ In any case, it is extremely challenging, from a technical perspective, to provide satisfactory and legible explanations about the decisions made by some AIs (such as decisions made by neural network technology, which is a form of machine learning).⁶¹²

In the case where the information obligations described above are not respected by data controllers, applicable sanctions are the same as described above (see part 3.2.2., section B). Notably, data subjects are entitled to lodge complaints with the competent data protection authorities.⁶¹³ Following such complaints, data protection authorities may investigate cases submitted and impose legally binding sanctions to data controllers, such as (i) issuing warnings to data controllers; (ii) issue reprimands to data controllers; (iii) order the controllers to comply with data subjects' requests to exercise their rights; (iv) order the controllers to bring its operations into compliance with the provisions of GDPR; and/or (v) impose administrative fines as provided for in Article 83.⁶¹⁴ Data subjects are also entitled to file suits in front of Member States' national jurisdictions and to sue data controllers that fail to comply with their information obligations.⁶¹⁵

3.3.3. Unfair Commercial Practices

When AI is used by undertakings⁶¹⁶ to conclude contracts with consumers,⁶¹⁷ or when AI is used by consumers to autonomously conclude contracts with undertakings, one could imagine that AIs do not give sufficient (or give incorrect) information to consumers about the object of the contract, or any other element that is the object of information obligations, thereby misleading consumers and substantially affecting their economic behaviours.⁶¹⁸ In other cases, AI-systems could potentially adopt aggressive behaviours towards their consumers, notably by manipulating them. Such unfair commercial practices⁶¹⁹ are forbidden under the terms of Article VI.95 of the Code of Economic Law. As the reasoning that should be relied upon to assess whether a commercial practice is unfair or not was already analysed above (see part 3.2.3 section A), the following paragraphs only focus on several types of commercial practices that AI could adopt when concluding contracts with consumers, or with undertakings, on the behalf of consumers.

⁶¹⁰ See notably L. EDWARDS and M. VEALE, "Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For", *o.c.*; G. MALGIERI and G. COMMANDÉ, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *o.c.*; B. GOODMAN and S. FLAXMAN, "European Union regulations on algorithmic decision-making and a "right to explanation"", *o.c.*

⁶¹¹ See notably S. WACHTER, B. MITTELSTADT, and L. FLORIDI, "Why a right to explanation of automated decision-making does not exist in the general data protection regulation", *o.c.*

⁶¹² European Commission, "White Paper on Artificial Intelligence – A European Approach to excellence and trust", *o.c.*, p. 12.

⁶¹³ Art. 77 GDPR.

⁶¹⁴ Art. 58, § 2 GDPR.

⁶¹⁵ Art. 79 GDPR.

⁶¹⁶ According to Art. I.8, 39°, CEL, this notion can be defined as any legal or natural person that pursues a long-term economic aim, including its associations. Regarding this definition, see also European Court of Justice, judgement *Mannesmann AG v High Authority of the European Coal and Steel Community*, 13 July 1962, C-19/61, EU:C:1962:31.

⁶¹⁷ According to Art. I.1, 2°, CEL, this notion can be defined as any natural person who is acting for purposes other than trading, industrial, artisanal or liberal activities.

⁶¹⁸ According to Art. I.8, 25° CEL, this notion can be defined as the use of a commercial practice that appreciably compromises the ability of a consumer to make informed decisions, and hence leads the consumer to make a transactional decision that he would not have taken otherwise.

⁶¹⁹ According to Art. I.8, 23° CEL, this notion can be defined as any action, omission, behaviour, commercial communication (including advertisement and marketing) from an undertaking, in relation to the promotion, sale, or supply of a product.

Indeed, there are a few types of commercial practices relating to AI that could potentially qualify as unfair.⁶²⁰ Regarding misleading practices, for instance, AI-systems might fail to provide sufficient information to consumers in the process of concluding a contract. This could notably be the case because AI-systems do not understand the context, and hence might not successfully adapt to the situations in which companies use those systems, or might fail to transmit relevant information to consumers on behalf of who they conclude contracts. AI could also provide false information to consumers due to a malfunction or a faulty programming. If such practices have a substantial impact on the economic behaviour of average consumers, the qualification of unfair trading practices could indeed be retained.

As to aggressive practices, AI-systems could unduly manipulate consumers in order to facilitate the conclusion of contracts as consumers might not even be aware that they are interacting with AI. For instance, AI-systems could repeatedly make phone calls or send emails to consumers to push them to conclude contracts (see above part 3.3.1). If, thereby, the economic behaviour of average consumers is substantially affected, the qualification of unfair trading practices might be retained. Similarly, if an AI concluding contracts with undertakings on the behalf of consumers repeatedly orders one product which the consumer made clear he/she not want to purchase, and if the economic behaviour of average consumers is substantially affected, the qualification of unfair trading practices might be retained.

Finally, it should be noted that Directive 2019/2161 forbids a new misleading practice at the European level as it inserts an additional paragraph in Article 7 of Directive 2005/29. This provision considers as a misleading omission, the fact for online marketplaces to fail to provide to consumers “the main parameters determining the ranking of products presented to the consumer as a result of the search query and the relative importance of those parameters, as opposed to other parameters”.⁶²¹ However, no sanction exists within the Belgian legal order, as such a practice is not yet prohibited by Belgian law.

3.3.4. Requirements for Consent

In order to conclude a contract, a few conditions are required under Belgian civil law.⁶²² Among other things, the parties willing to enter in a contract have to consent, that is to say, they have to express their will to contract, and thereby produce legal effects.⁶²³

When an undertaking uses AI to conclude contracts with consumers in an automated or autonomous manner, part of the literature points out that the requirement for consent might not be met, or at least, that the existence of a valid consent might be difficult to prove.⁶²⁴ For instance, the undertaking that deploys AI could potentially assert that it did not formally consent to the contract concluded between the consumer and the AI-system when it autonomously concludes a contract that does not suit the undertaking (e.g. because the consumer is insolvent which the AI did not succeed to verify). On this ground, the undertaking could try to obtain the nullity of contracts concluded by the AI-system. Yet, one might argue that the undertaking consented to conclude such contracts implicitly and beforehand when it chose to rely on AI to autonomously conclude contracts.

⁶²⁰ For an in-depth analysis of such practices, see H. JACQUEMIN, “Comment lever l’insécurité juridique engendrée par le recours à l’intelligence artificielle lors du processus de formation des contrats?”, *Law, norms and freedom in the cyberspace – Droit, normes et libertés dans le cybermonde: liber amicorum Yves Poulet*, Bruxelles, Larcier, 2018, p. 170.

⁶²¹ Art. 7, § 4a Directive 2005/29.

⁶²² Art. 1108 CCL.

⁶²³ P. WERY, *Droit des obligations*, vol. 1, *Théorie générale du contrat*, 2^{ème} éd., Bruxelles, Larcier, 2011, p. 223-224.

⁶²⁴ H. JACQUEMIN, “Comment lever l’insécurité juridique engendrée par le recours à l’intelligence artificielle lors du processus de formation des contrats?”, o.c., p. 146. The following developments are mainly based on this research.

The undertaking that uses AI to autonomously conclude contracts with its consumers could also require the annulment of (part of) the concluded contracts on the basis of vitiated consent, and more precisely based on the theory of error. If an error occurs, such as the AI-system concluding a contract with a consumer for the sale of a good A, while the undertaking does no longer have such good, and only wishes to sell good B, the undertaking may try to achieve the annulment of any contracts having as object good A. Therefore, the undertaking could be arguing that it did consent to contract with consumers through its AI-system, but assert that the error that took place should be sufficient for the contract to be annulled.

In such a case, the undertaking would have to prove that the conditions set out to invoke the theory of error are met. These conditions are: (i) the error is on substantial qualities of the object of the contract; (ii) the error is common to all parties to the contract; and (iii) the error is excusable.⁶²⁵ Although the first two conditions could be fulfilled by the example given, the third one seems more debatable: the error might not be excusable for the undertaking, as it voluntarily decided to use an autonomous system and knew that contracts would be concluded by it, potentially with mistakes as no technology is fully accurate in all circumstances.

In any case, consumers facing such issues regarding consent of undertakings could potentially call upon the theory of appearance in order to enforce the contracts they concluded with autonomous AI-systems and to achieve legal certainty, despite contestations from the undertakings regarding their consent. In order to apply, the theory of appearance requires three conditions to be fulfilled, (i) there must be an apparent situation; (ii) the victim makes a legitimate mistake; and (iii) the apparent situation can be imputed to a subject of law.⁶²⁶

Regarding the first condition, there is an apparent situation, which seems conform to reality, and where the contract seems to be concluded, as the consumer goes through the entire process of concluding its contract with the AI-system. For the second condition, the mistake made by the consumer seems to be legitimate as consumers would not suspect that undertakings might contest the validity of contracts concluded by their own AI-systems. Finally, the apparent situation can most likely be imputed to a subject of law as there will necessarily be a natural person that deploys the AI-system – whether for him/herself, whether as an organ of a legal person.⁶²⁷

It should be noted that the entire reasoning held in this part of the study can be transposed, *mutatis mutandis*, to the hypothesis in which the consumer uses AI-systems to autonomously conclude contracts with undertakings. Consumers, to avoid being bound by such contracts, could invoke the same grounds as detailed above. Likewise, undertakings could invoke the same grounds as explained above to prove that contracts were effectively concluded with the consumers, through the use of their AIs.

3.4. Overview of the Identified Gaps

In this part of the study, many legal rules were considered as consumer protection is a field of law that encompasses numerous different legal texts. The main questions that arise are to know (i) if existing (and to some extent future) rules are applicable regarding AI and when they are, (ii) to know if they provide an adequate level of consumer protection (i.e. a level of protection similar to cases in which AI is not at stake). On the basis of the analysis conducted, the following main gaps, that have (or might have) an impact regarding consumer protection when AI is at stake, should be highlighted:

⁶²⁵ P. WERY, *Droit des obligations*, vol. 2, *Les sources des obligations extracontractuelles. Le régime général des obligations*, Bruxelles, Larquier, 2016, p. 231 et seq.

⁶²⁶ *Ibid.*, p. 255 et seq.

⁶²⁷ H. JACQUEMIN, "Comment lever l'insécurité juridique engendrée par le recours à l'intelligence artificielle lors du processus de formation des contrats?", o.c., p. 151.

- Art. 1649bis to 1649octies of the CCL (Belgian legal rules on warranty, transposing Directive 1999/44/EC on the sale of consumer goods and associated guarantees) apply to consumer goods. At this stage, it is unclear whether AI (which is a software) might qualify as consumer goods in all circumstances. In the near future, Directive 2019/770, which applies to the supply of digital content and services, will tackle this gap (i.e. when it will be transposed in Belgian law).
- Directive 2019/770 does not apply to digital content or digital services that are incorporated in or interconnected with goods with digital elements, as these enter the scope of application of Directive 2019/771 (on contracts for the sale of goods). This dualistic approach might lead to a difference of treatment between consumers depending on the manner in which AI is provided to them, whether as digital content or services or as goods with digital elements. For instance, the period during which lacks of conformity that survene are deemed to have existed at the time of supply of can be up to two years for goods with digital elements, according to Directive 2019/771, while it is limited to one year for digital content or services, according to Directive 2019/770.
- Directive 2019/770 does not apply to several specific sectors, notably regarding healthcare, electronic communications, gambling services, or financial services, which widely reduces its scope of application when consumers are facing AI powered digital content/services.
- Directive 2019/770 provides for a duration of one year, during which lacks of conformity that survene are deemed to have existed at the time of supply of the digital content or services. This period of time might be too short, due to the continuous learning feature of AI-systems.
- Under both Directives 2019/770 (on digital content) and 2019/771 (on contracts for the sale of goods), traders and/or sellers could potentially try to avoid the legal qualification of lack of conformity, for the potential flaws of their AI-systems, by contractually providing information to consumers on the learning capabilities (and correlative potential for unforeseen changes of behaviour) of their systems, and by obtaining consumers' acceptance for that deviation. Case law will be required on this matter to determine if this constitutes a gap or not.
- The Act of 25 February 1991 on the liability for defective products (Belgian transposition of the Product Liability Directive) raises criticism regarding several of its elements which might be considered as gaps in relation to AI. These notably relate to the definition of the producer, the burden of proof, the notion of product and defect, the possibilities left to producers to avoid liability and the period left for injured persons to act.
- Directive 2019/2161 (Omnibus Directive) requires undertakings to inform their consumers when prices are personalised on the basis of automated decision-making. Yet, this obligation only applies to distance and off-premises contracts. This creates a difference of treatment on the basis of the type of contract concluded (i.e. distance and off-premises contracts vs. other contracts), while the risks for consumers facing personalised prices are likely the same whether the contract is a distance or off-premises contract or not.
- More generally, at this stage, no general obligation exists within consumer protection law requiring undertakings to inform consumers of the fact that they are concluding a contract with an AI-system rather than with a human.
- Directive 2019/2161 considers as a misleading omission, the fact for online marketplaces to fail to provide to consumers the main parameters determining the ranking of products presented as a result of the search query and the relative importance of those parameters. Yet, no sanction exists, at this stage, within the Belgian legal order as such a practice is not yet prohibited by Belgian law.

CHAPTER 4 - TELECOMMUNICATION AND INFORMATION SOCIETY (WP 4)

1. Introduction

In this chapter, several aspects related to AI and telecommunication and information society are examined. The study will first focus on cybersecurity (part 2). We will also assess the relationship between AI and the data-economy (part 3) as well as electronic identification (part 4). The final part of this chapter relates to e-commerce (part 5).

2. AI Safety and Cybersecurity (WP 4.1.)

2.1. Introduction

In order for AI-systems to be considered trustworthy and their effectiveness maximised, it is essential that AI-systems are safe and secure. This is easier said than done. First of all, being a dual-use technology, AI-systems can be used for beneficial purposes, but also for malicious purposes. As with any automated process, this increases the scale, use and efficiency of such attacks, thereby increasing risks.⁶²⁸ AI-systems also cause new threats, such as deepfakes.⁶²⁹ Second, AI-systems have their own vulnerabilities, which can either be exploited by attackers, or arise as a function of their design; after all, all systems are bound to fail and cause harm.⁶³⁰ The latter is exacerbated by some AI-systems' inherently unpredictable design.⁶³¹ However, AI-systems also can be used to support cybersecurity: real advances are being made when it comes to automated intrusion detection systems, allowing AI-systems to guard against attacks and other forms of illegal behaviour.⁶³²

Through the increased digitisation of society – and with it the increased interconnectivity of all systems (IoT) and the increased use of (and dependence on) AI, the importance of safe and secure AI cannot be understated. It is, therefore, no surprise that the EU Commission published a report regarding an evaluation of the Product Liability Directive and that the Expert Group on New Technologies and the European Parliament published their report on liability (and safety legislation) for Artificial Intelligence.⁶³³ Similarly, it is no surprise that in December 2020, the Commission unveiled its New Cybersecurity Strategy, including a reform of the Directive on security of network and information systems (NIS Directive), the Critical Infrastructures Directive

⁶²⁸ See M. BRUNDAGE, S. AVIN, J. CLARK, H. TONER, P. ECKERSLEY, B. GARFINKEL, A. DAFOE, P. SCHARRE, T. ZEITZOFF, B. FILAR, H. ANDERSON, H. ROFF, G. ALLEN, J. STEINHARDT, C. FLYNN, S. Ó HÉIGEARTAIGH, S. BEARD, H. BELFIELD, S. FARQUHAR, C. LYLE, R. CROOTOFF, O. EVANS, M. PAGE, J. BRYSON, R. YAMPOLSKIY and D. AMODEI, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation*, Oxford, OUP, 2017, p. 16 *et seq.*; ENISA, "AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence", December 2020, p. 7 available at https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges/at_download/fullReport.

⁶²⁹ *Ibid.*

⁶³⁰ *Ibid.*; also see S. HERPIG, "No Safety without Cybersecure AI", 9 April 2020, available at <https://directionsblog.eu/no-safety-without-cybersecure-ai/>.

⁶³¹ M. BRUNDAGE *et al.*, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation*, *o.c.*, p. 21-22.

⁶³² ENISA, "AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence", *o.c.* Also see e.g. I. AL-MANDHARI, L. GUAN and E. EDIRISINGHE, "Investigating the Effective Use of Machine Learning Algorithms in Network Intruder Detection Systems" in K. ARAI, S. KAPOOR and R. BATIA, *Advances in Information and Communication Networks – Proceedings of the 2018 Future of Information and Communication Conference (FICC)*, Vol. 2, New York, Springer, 2019, p. 154-162. An example would be the Antwerp-based Textgain, which has developed a system that automatically detects online jihadist hate speech with over 80% accuracy (see <https://www.textgain.com/portfolio/automatic-detection-of-online-jihadist-hate-speech/>).

⁶³³ European Commission, Expert Group on Liability and New Technologies – New Technologies Formation, "Liability for Artificial Intelligence and Other Emerging Technologies", 2019, available at

<https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>;

A. BERTOLINI, "Artificial Intelligence and Civil Liability", July 2020, available at

[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf).

and the announcement of the development of the EU Cyber Defence Shield.⁶³⁴ A review of the General Product Safety Directive is also planned.⁶³⁵ As was stressed in the White Paper, the security of AI-systems is the EC's clear priority.⁶³⁶

Many rules under Belgian law (many of which transpose EU Directives or consist of European Regulations) already ensure that the risks of products and services are mitigated. These rules include general contract and tort law, data protection law, as well as specific laws on product safety and cybersecurity. Some of these regulations are general, others are sector-specific. In order to structure the analysis, we will follow the regulatory framework along three steps in the AI-system lifecycle. First, we will briefly describe the relevant risk factors of AI-systems regarding safety and security (part 2.2.). Second, we will discuss the requirements to implement security and safety in the design of AI-systems (part 2.3.). Third, we will discuss the general monitoring obligations and corrective obligations that producers and users face once the AI-system has been released (part 2.4.). We will not only discuss the rules which mitigate the risks of AI, but also those rules related to the use of AI-systems to prevent and/or mitigate risk (part 2.5.). We will conclude with an overview of the gaps (part 2.6.).

2.2. Security and Safety Related to AI

In the following paragraphs, it will first be established what cybersecurity and safety mean with regard to AI-systems (part 2.2.1.). It will then be examined what characteristics of AI-systems have an impact on safety and security (part 2.2.2.).

2.2.1. What are Cybersecurity and Safety Regarding AI?

Before analysing the rules regarding security and safety, it is essential to provide a clear definition of each term. As will be seen throughout the analysis, the term is often used ambivalently. For example, security is defined as “protection against something bad that might happen in the future”, correlating with the notion of safety.⁶³⁷ Indeed, the term is often used interchangeably.⁶³⁸

Legally speaking, both relate to the minimalization of risk and harm. The difference between the two lies in the harm that is minimised. Safety regulation minimises the harm that products, services or systems can cause to human beings. Security relates to the minimisation of harm to the system

⁶³⁴ European Commission, “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient”, 16 December 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391; European Commission, “Proposal for a Directive on Measures for a high common level of cybersecurity across the Union”, COM(2020)823; European Commission, “Proposal for a Directive on the resilience of critical entities”, COM(2020)829; also see European Commission, “Joint Communication to the European Parliament and the Council – the EU’s Cybersecurity Strategy for the Digital Decade”, JOIN(2020)18.

⁶³⁵ See European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme: a Union that Strives for More”, COM(2020)37 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1581957029354&uri=CELEX:52020DC0037>.

⁶³⁶ See European Commission, “White Paper on Artificial Intelligence – a European Approach to Excellence and Trust”, 19 February 2020, COM(2020)65 final, p. 14-15.

⁶³⁷

<https://www.oxfordlearnersdictionaries.com/definition/english/security#:~:text=%5Buncountable%5D%20the%20activities%20involved%20in,against%20attack%2C%20danger%2C%20etc.&text=security%20against%20something%20The%20bars,provide%20security%20against%20break%2Dins..>

⁶³⁸ For example, BRUNDAGE et al. uses the term “security” to define various scenario’s which are not strictly cybersecurity: M. BRUNDAGE et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation*, o.c., p. 23 et seq.

itself. Cybersecurity is the security of IT-systems.⁶³⁹ The main objectives of cybersecurity is to preserve the confidentiality, integrity and availability of the IT system or the data stored on it.⁶⁴⁰

The legal rules applicable in Belgium (and within the EU) follow this duality between the two fully. The rules on product safety are implemented in Book IX of the Code on Economic Law and in sectoral legislation defining essential requirements for specific products. Under Article I.10, 2°, a product is considered “safe” if, under reasonable or normally foreseeable conditions of use, does not present any risk or only minimum risks, ... consistent with a high level of protection for the safety and health of persons.⁶⁴¹ The types of risk are not strictly defined, but the main focus appears to be the mitigation of physical harm. It must be noted, though, that the types of risk must be widely construed so that other types of harm are also included.⁶⁴² This can become relevant as not all harm caused by AI-systems is physical. Emotional AI, for example, can cause mental harm as well (although, given the nature of said harm, it may be harder to detect).⁶⁴³ AI can also be used to cause mental harm or even political harm. For instance, the current polarisation of the political sphere is in part attributed to the use of AI-algorithms which create “filter bubbles”.⁶⁴⁴ AI-systems can also be used to purposefully manipulate such systems.⁶⁴⁵ Granted, these can be guarded through other rules or means. These will be partially discussed in part 2.5.

Meanwhile, the definitions of security under the General Data Protection Regulation (GDPR), the definition under the NIS Directive and its implementation in Belgium, the Act of 7 April 2019, as well as the Law on Critical Infrastructures refer to measures which preserve the so-called “CIA” triad (confidentiality, integrity, availability).⁶⁴⁶ This is in accordance with most standards on cybersecurity.⁶⁴⁷

It must be noted that the notions of safety and security are bound to overlap. For example, cybersecurity is one of the essential measures to ensure that AI-systems are always safe and resilient during normal use. At the same time, the definition of safety determines, in part, the scope of these regimes, which result in fragmentation and gaps in their coverage. For example, the product safety regime covers only physical products and does not occupy itself with software which is not embedded into hardware. At the same time, (cyber)security is mainly preoccupied with preventing and avoiding external attacks to itself, not taking into account the safety risks it inherently may pose to humans. This lack of convergence between the two regimes is, therefore, a first main gap that shows itself through the analysis of these regimes. This gap is already being addressed in some way. For example, in the field of certification, the EU Cybersecurity Act defines “cybersecurity” as the activities necessary to protect both IT systems and their users from cyber

⁶³⁹ W. WAHLSTER and C. WINTERHALTER, *German Standardization Roadmap on Artificial Intelligence*, November 2020, p. 92.

⁶⁴⁰ *Ibid*; see also Art. 5.1(f) GDPR, art. 32.1(b) GDPR. Also, see the definition of “cybersecurity” in the standard ISO/IEC JTC1/SC27 IT-Security Techniques; ENISA, “Definition of Cybersecurity – Gaps and overlaps in standardisation”, December 2015, p. 13 *et seq.*

⁶⁴¹ Art. I.10, 2° CEL; also see Art. 2, (b) Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, *OJ.L.* 11, 15 January 2002, p. 4-17.

⁶⁴² For a general overview of the concept of safety, see D. VERHOEVEN, *Productaansprakelijkheid en productveiligheid*, Antwerp, Intersentia, 2018, p. 93 *et seq.*

⁶⁴³ This risk can be especially prevalent in the use of artificially intelligent chatbots for psychotherapy, or AI-systems that may induce alterations in emotional state. See, for example, A. MINER, A. MILSTEIN, J. HANCOCK, “Talking to Machines About Personal Mental Health Problems”, *JAMA* 2017, p. 1217-1218.

⁶⁴⁴ I. LAMBRECHT, “The Filter Bubble: to burst or to blow over?”, *KU Leuven CiTIP Blog*, 29 November 2016, <https://www.law.kuleuven.be/citip/blog/the-filter-bubble-to-burst-or-to-blow-over/>.

⁶⁴⁵ See, e.g., M. BRUNDAGE *et al.*, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation*, o.c., p. 28-29 for an overview of potential scenarios in which AI is maliciously used.

⁶⁴⁶ Art. 3, 13° Law on Critical Infrastructures; Art. 6, °9 Law establishing a Framework for the security of network and information systems of general interest to public security; see Articles 5 and 32 of the GDPR.

⁶⁴⁷ See, for example, ISO/IEC 27032:2012: ENISA, “A Definition of Cybersecurity – Gaps and overlaps in standardisation”, o.c., p. 15 *et seq.*

threats.⁶⁴⁸ Similarly, the EU Commission has planned a review of the General Product Safety Directive, which serves to adapt its rules to include non-embedded software.⁶⁴⁹ Moreover, it must be noted that the security of AI-systems is a core component of its safety.

2.2.2. What Characteristics of AI-systems Influence Security and Safety?

As explained in the EU Commission's Communication on AI for Europe and the AI HLEG, AI refers to systems that display intelligent behaviour by analysing their surroundings and taking actions – with some degree of autonomy – to achieve specific goals.⁶⁵⁰ For the purposes of the safety of AI, the Expert Group on Liability and New Technologies already issued its report on the safety and liability implications of Artificial Intelligence, the IoT and robotics. In it, the following traits which are relevant for liability law (and also for safety law) include:⁶⁵¹

- Complexity: the increasing complexity of the technology makes it difficult to figure out who caused harm;
- Opacity: the more complex digital technologies become, the less those using their functions can understand how they function (and thus how they cause harm). Black-box algorithms are a prime example of this. Therefore, it is much harder to define when the expectations have been broken or even to understand the reason a product has become unsafe;
- Openness: once placed on the market, AI-systems and other IT-systems are often updated. Thus, they are not the same throughout their lifecycle. Nonetheless, their lifecycle must be protected all the same.
- Autonomy: AI-systems are adaptive and autonomous. They make decisions without human oversight. Machine learning-based AI-systems adapt to their surroundings and thus alter their initial algorithms. The choice of the data and the resulting outcome are therefore always changing. Nonetheless, the safety must be ensured in all those instances.
- Predictability: many systems have been designed to not only result to predetermined inputs, but also to identify new inputs and link them to self-chosen criteria. Therefore, they become unpredictable. This is exacerbated by the fact that, even in the event that risks materialize, it may be very difficult to trace back the exact cause of the harm, as well as to “unlearn” faulty self-programming.⁶⁵²
- Data-drivenness: AI-systems often process data from sensors, which is not pre-installed. Essential data may be absent through these flaws. More generally, the data used to train or adjust algorithms determine the outcomes. Flaws or biases in the data reflect in the outcome.
- Vulnerability: similar to all digital technologies, AI-systems have inherent vulnerabilities and are constantly in contact with other systems. This interconnectedness increases the risk of being attacked by other systems.

⁶⁴⁸ Article 2, (1) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), *OJ.L.* 151, p. 15-69.

⁶⁴⁹ European Commission, “Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions – Artificial Intelligence for Europe”, COM(2018)237, 2; also see AI HLEG, “A Definition of AI: Main Capabilities and Disciplines”, 8 April 2019, p. 9, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651.

⁶⁵⁰ European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe”, Brussels, 25 April 2018, COM(2018)237 final.

⁶⁵¹ European Commission, Expert Group on Liability and New Technologies – New Technologies Formation, “Liability for Artificial Intelligence and Other Emerging Technologies”, *o.c.*, p. 32 *et seq.*

⁶⁵² *Ibid.*, p. 32 *et seq.*

In short, AI-systems are unpredictable, hard to control and create new risks for their continued safety.⁶⁵³ Therefore, the White Paper on AI already proposed to ensure that there is a strict liability regime for high-risk AI-systems and the Product Safety Directive is currently under review.⁶⁵⁴ Similar risks arise for AI-systems in relation to cybersecurity. First, AI-systems cannot be seen apart from the other technological developments taking place in the Fourth Industrial Revolution. Digitisation is increasingly important to more and more aspects of our daily lives. Devices are becoming more and more interconnected (IoT). The use of AI also means that we outsource many types of decisions – previously made solely by humans – to digital systems interconnected as part of the IoT. These systems are more efficient and scalable and lend themselves to rapid diffusion.⁶⁵⁵ This alone makes that the attack surface for AI-systems is extended.

AI adds specific risks to cybersecurity. In a study published in December 2020, the European Union Agency for Cybersecurity (ENISA) outlined the AI Cybersecurity Threat Landscape. In it, ENISA named three dimensions in which AI has become relevant:⁶⁵⁶

- Cybersecurity for AI: AI-models are vulnerable to specific outside attacks and exploits of their vulnerabilities. These attacks can take place at several stages in the AI-lifecycle, for instance through manipulation of the training data (e.g. data poisoning), through exploitation of the model (e.g. model evasion, morphing attacks), ... The Threat Landscape goes on to provide an overview of said risks.
- AI to support cybersecurity: AI can be used as a tool to improve cybersecurity by developing more effective (and adaptive) cybercontrols (e.g. automated intrusion detection) and can make the work of law enforcement and supervisors easier through allowing algorithms to increase the efficiency and scale of their investigations. Examples of the latter include automated financial fraud detection.⁶⁵⁷
- Malicious use of AI: &s was underlined by, inter alia, BRUNDAGE, AI can be used to create more powerful attacks. Examples include AI-powered malware, using AI to create more advanced forms of social engineering,⁶⁵⁸ AI-augmented DDOS attacks. As AI-tools can be disseminated digitally in the form of tools, these increasingly powerful hacker tools are democratised, only increasing their use.

M. BRUNDAGE summarises the risks created by the proliferation of AI as follows:⁶⁵⁹

- Expanding existing threats: AI-systems will expand existing threats by lowering the cost of attacks, thus increasing the set of actors who can carry out such attacks, the rate by which those attacks can be executed and their potential targets;
- Introducing new threats: AI-systems will introduce new threats, which relate to the use of AI's new possibilities and the exploitation of AI's vulnerabilities;

⁶⁵³ See also European Commission, "Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions – Artificial Intelligence for Europe", COM(2018)237, 2; also see AI HLEG, "A Definition of AI: Main Capabilities and Disciplines", 8 April 2019, p. 12-13 available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651.

⁶⁵⁴ An Impact Assessment was published on 23 June 2020: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12466-Review-of-the-general-product-safety-directive>.

⁶⁵⁵ M. BRUNDAGE *et al.*, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation*, o.c., p.3-4.

⁶⁵⁶ ENISA, "AI Cybersecurity Challenges – Threat Landscape for Artificial Intelligence", December 2020, p. 7.

⁶⁵⁷ See e.g. J. PEROLS, "Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms", *Auditing: a Journal of Practice & Theory* 2011, vol. 30, p. 19-50.

⁶⁵⁸ An example include the use of deepfakes, which challenge the notion "seeing is believing" for anything one sees on the Internet. See M. BRUNDAGE *et al.*, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation*, o.c., p. 49.

⁶⁵⁹ *Ibid.*, p. 5.

- Altering the typical character of threats: In light of the above, AI will alter the typical character of threats.

The above factors thus lead us to presume that the proliferation of AI-systems will increase the risk, where the solution is sought in the use of AI-based defence tools. It is in light of these tendencies that the pending reforms to the EU's cybersecurity rules must be understood. These will be discussed further below.

2.3. Legal Rules Governing the Security of the Design (or Security by Default) of AI-systems

2.3.1. Introduction

In this part, we will discuss the general rules that prescribe the developers, deployers and users of AI-systems to ensure that their systems are safe and secure as they apply under Belgian law. We will group these obligations according to their place in the AI-lifecycle. We will discuss the rules that impose "security/safety by design". We will first discuss contract and tort law provisions (part 2.3.2.). This is followed by an analysis of product safety legislation (part 2.3.3.), the applicable data protection legislation (part 2.3.4.) and the general cybersecurity framework (part 2.3.5.). Sectoral cybersecurity regulations are also included in the analysis (part 2.3.6.) as well the certification under the Cybersecurity Act (part 2.3.7.).

2.3.2. General Contract and Tort Law

Before discussing more specific rules discussing product safety, cybersecurity, etc., it must be noted that the compliance with standards of safety can also be enforced through general contract laws. However, these rules fail to cover all necessary risks brought about by AI-systems and, therefore, necessitate the further regulation mentioned below (part A.). We will also focus on tort law provisions that may be relevant for AI-systems (part B.).

A. Contract Law

AI-systems can be sold to the market. However, the law for the sale of goods only applies whenever a physical good is sold. In other words, when AI-systems are sold as products embedded in hardware, they fall under the sale of goods.⁶⁶⁰ In the event mere possession is given, the rules for rent apply. This creates a first gap/lack of convergence, as due to digitisation, AI-systems are sold less and less in physical form and more and more as a service (servitisation). In the event software is supplied in an immaterial form, then the rules for the contract of enterprise (Article 1787 *et seq.* Code Civil Law – CCL) apply. We will discuss the remedies below.

Articles 1604 and 1614 BCC stipulate that the seller must deliver to the buyer a good which is in conformity with the agreement (conform delivery). This conformity relates not only to the time of delivery and the quantity of the goods, but also to the quality.⁶⁶¹ Thus, parties are free to agree to certain security standards – as is often the case, e.g. by agreeing that a good must comply with all compatible ISO standards applicable to it. Once the buyer has accepted the good, however, no use of conformity can be invoked, unless if the seller had warranted compliance. After acceptance of

⁶⁶⁰ See Art. 1582 CCL. An example would be the sale of a self-driving car, or an AI-powered toothbrush: J. PETERS, "Oral-B's New \$220 toothbrush has AI to tell you when you're brushing poorly", *The Verge*, 25 October 2019, available at <https://www.theverge.com/circuitbreaker/2019/10/25/20932250/oral-b-genius-x-connected-toothbrush-ai-artificial-intelligence>.

⁶⁶¹ See B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht*, Antwerpen, Intersentia, 2012, p. 221 *et seq.*

the delivery, the buyer may still sue in liability based on the theory of hidden defects.⁶⁶² A good is considered defective when a product shows traits that were present at the time of the sale, which would have caused that the purchase would not have gone through, had the buyer known them, and which the buyer could not have discovered through a normally thorough analysis.⁶⁶³ This defective trait is defined functionally: a good is defective if it does is incapable of fulfilling its general purpose.⁶⁶⁴ Compliance with a technical standard may form an indication of showing hidden defects or not, but it does not guarantee this. There may still be a defect when there is compliance.⁶⁶⁵

The notion of “defect” also covers instances in which a good cannot be used safely and, therefore, covers defects in AI-systems. However, the use of such systems becomes extremely difficult when dealing with adaptive and autonomous systems, especially “black box algorithms”. For example, when an AI-system “learns” dangerous or dysfunctional behaviour, it is unclear whether or not this is a design flaw or if it is a later cause than any design flaw. For the latter, there is no remedy unless explicitly warranted by contract or by mandatory law (such as consumer protection).⁶⁶⁶

More generally, the notion of “defectiveness” imposes a huge burden of proof on the claimant (in this case the buyer) when dealing with a self-learning system. After all, it is then upon the buyer to prove that the good, through a fault in its design (which is often imperfectly logged or random through the nature of AI), became defective in a way that it breached the buyer’s reasonable expectations. This burden may prove excessively hard to any claimant at all.⁶⁶⁷ This is one of the reasons that, in their report, the Expert Group on Liability and New Technologies claimed that strict liability must be granted to the buyers of high-risk AI-systems (without defining such risk) against both operators and producers of AI-systems.⁶⁶⁸ However, even in the event such a claim would succeed on the basis of sales law, the sanction towards the buyer would be liability, either to take back the defective good and to repay the price or to claim for a reduction of the price.⁶⁶⁹ This does not prevent the appearance of risk *ipso facto* and only serves to repay an aggrieved customer after the fact. Whether this is sufficient to ensure safety of an AI-system will require further research.

Similarly, whenever software – and thus also AI-systems – are supplied virtually, the rules of enterprise require the service supplier to observe a certain quality on the basis of general contract law, as applied to the service contract.⁶⁷⁰ This entails that the service supplier must deliver the service in accordance with “the rules of the art”, which includes any applicable standards.⁶⁷¹ In IT, this could form a basis for an obligation to comply with safety standards to provide the average safety that an AI-system must reasonably provide.⁶⁷² However, such standard is all but clear. In practice, this is achieved through Service Level Agreements (SLAs), which completely regulate safety requirements. This subjects the safety of an AI-based service to the bargaining power

⁶⁶² B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht*, o.c., p. 28 et seq.; Cass. 19 December 2007, *TBH* 2008, p. 152 et seq.; H. DE WULF, “Samenloop of exclusiviteit tussen de sanctionering van niet-conforme levering en verborgen gebreken: heeft cassatie de controverse beslecht?”, note under Cass. 19 december 2007, *TBH* 2008, p. 154 et seq.

⁶⁶³ B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht*, o.c., p. 311-312.

⁶⁶⁴ *Ibid.*

⁶⁶⁵ B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht*, o.c., p. 336-337.

⁶⁶⁶ B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht*, o.c., p. 336.

⁶⁶⁷ See e.g. EUROPEAN COMMISSION, EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES – NEW TECHNOLOGIES FORMATION, “Liability for Artificial Intelligence and Other Emerging Technologies”, o.c., p. 20-21 in relation to tort law. The same burden of proof applies to any claims of causation under contractual liability.

⁶⁶⁸ *Idem*, p. 39 finding no. 9. See, however, A. BERTOLINI, “Artificial Intelligence and Civil Liability”, o.c., p. 77 et seq.

⁶⁶⁹ Art. 1641 et seq. CCL.

⁶⁷⁰ F. BURSSSENS, *Handboek Aannemingsrecht*, Morsel, Intersentia, 2019, p. 107-109.

⁶⁷¹ *Ibid.*

⁶⁷² *Ibid.*

between the parties. If no explicit standard was provided, the service provider must provide his/her services in accordance with the “rules of the art”. Such “rules of the art” arise as a result of professional usage.⁶⁷³ These usages are very opaque when it comes to AI and may not be known to judges. They may also be subject to rapid change as a result of technological progress and therefore unfit to be developed through the legal process. Standards provide guidance in this regards. However, standards are always voluntary and may be unfit to the case at hand; therefore, standardisation only creates a presumption of compliance, as they are the minimum.⁶⁷⁴ Standards therefore only do so much to ensure conformity of the service.

Consumer protection law does provide some protection to consumers regarding safety. For example, the functionalities must clearly be notified and for the sale of consumer goods, the conformity is warranted and more clearly defined.⁶⁷⁵ However, these regimes are still based too much on either the sale of consumer goods (and thus physical goods, covering only AI-systems embedded in hardware) and do not entirely prevent security regulations altogether. For software services supplied virtually, the applicable framework is assumed to be all rules related to cybersecurity. Then again, as will be explained below, the standardisation – and especially the certification – framework for AI-systems is still undergoing development.

In order to mitigate the problem of bargaining power, there are mandatory contract law rules that impose suppliers to provide certain quality standards to consumers. Examples include the Law on the Sale of Consumer Goods (Articles 1649*bis et seq.* CCL). These provide a warranty for all conformity and stipulate that a good is considered in conformity in the event the good is suited for purpose that the consumer may reasonably expect, given the nature of the good and the disclosures given. These rules cannot be negotiated away via contract.⁶⁷⁶ However, this does not mitigate the other risks identified above. Moreover, the abovementioned rules only apply to the sale of physical goods, implying that the sale of software through digital distribution is not covered (own underlining). In light of the increasing “servitisation” of business models corresponding to digitisation, this is a clear regulatory gap.⁶⁷⁷

Recent European legislation attempts to transcend the limitations of the abovementioned regimes, at least when it comes to contracts between commercial enterprises and consumers. EU Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services and EU Directive 2019/771 on certain aspects concerning contracts for the sale of goods provide updated requirements for conform delivery and safety of the supply of any and all digital content, embedded in physical goods (in the case of the latter) or not (in the case of the former). “Digital content” is defined as “data which are produced and supplied in digital form” and may, therefore, define any sort of computer program, including an AI-system.⁶⁷⁸ Security is made a component of the objective conformity of any delivered digital content, digital service (or good delivered alongside them), insofar as the consumer was reasonably entitled to expect them, given the nature of the digital content and digital service and taking into account any public statement made by or on behalf of the trader.⁶⁷⁹ The latter – again – begs the question what security

⁶⁷³ F. BURSENS, *Handboek aannemingsrecht*, Mortsel, Intersentia, 2019, p. 107 *et seq.*

⁶⁷⁴ *Ibid.*

⁶⁷⁵ See e.g. Art. VI.45 §1, 18° CEL for distance sales; see Article 1649*bis et seq.* CCL.

⁶⁷⁶ See Art. 1649*bis et seq.* CCL.

⁶⁷⁷ See for example, B. KEIRSBILCK, E. TERRY, E. VAN GOOL, “Consumentenbescherming bij servitisation en product-dienst-systemen (PDS)”, *TPR* 2019, p. 817-899. An overview of the rules can be found in I. CLAEYS AND E. TERRY (eds), *Nieuw recht inzake koop & digitale inhoud en diensten*, Antwerp, Intersentia, 2020, 426 p.

⁶⁷⁸ Art. 2(1) Directive 2019/770; Art. 2(6) Directive 2019/771.

⁶⁷⁹ See e.g. Art. 8.1(b) Directive 2019/770: “In addition to complying with any subjective requirement for conformity, the digital content or digital service shall: (b) be of the quantity and possess the qualities and performance features, including in relation to functionality, compatibility, accessibility, continuity and security, normal for digital content or digital services of the same type and which the consumer may reasonably expect [...]”; Article 7.1(d) Directive 2019/771.

consumers are entitled to expect from adaptive systems. This is more likely to clarify itself with regard to each AI-system, as their use proliferates throughout the market. Also note that there is no lack of conformity if the consumer was specifically informed that a particular characteristic of the digital content or digital service deviated from the objective requirements for conformity and if the consumer expressly and separately accepted that deviation.⁶⁸⁰ This can provide an easy way out for suppliers who wish to evade liability for deviations caused by AI-systems, which due to their adaptive and autonomous nature become unpredictable. Both Directives are to be transposed into Belgian law ultimately on 1 July 2021. Moreover, the abovementioned rules depend on casuistry regarding AI-systems in litigation. This can take years, which is simply time one does not have. Therefore, preventive regulation is required.

For the abovementioned reasons, general contract law appears insufficient to provide for the security of AI-systems. At the same time, contract law – mainly due to its *inter partes* nature – does not appear to be the right vehicle to ensure the safety of AI-systems. More specific regulation is required. This will be further discussed below.

B. Tort Law and Product Liability

Similarly, towards third parties, general tort law imposes a duty on the suppliers and deployers of AI-systems to take any necessary measures to avoid that the design of their AI-system and/or the use of their AI-system causes harm to other individuals, to whom they are not bound by contract. In light of the problems regarding the burden of proof, the Product Liability Directive may also apply. Nonetheless, given the specific problems, product safety rules must complement them.

In accordance with Article 1382 CCL, the general principle is that whoever causes damage through a wrongful act, must compensate said damage. A wrongful act must be imputable to the tortfeasor. The tortfeasor must be culpable for the harm. A wrongful act can either be committed through infringing a clear duty imposed by a legal prescription or by negligent behaviour (i.e. behaviour which falls short of the general duty of care). The duty of care is the amount of care that is taken by the “normally prudent person”.⁶⁸¹ Any professional is presumed to know the standards of his/her trade and therefore can be considered to breach the duty of care if he/she does not follow these standards.⁶⁸²

The abovementioned duty of care also applies to the developers of IT-systems (and by extension AI-systems). One can, therefore, conduct an entire analysis regarding the duty of care when it comes to cybersecurity. Such a study has been conducted by TJONG TJIN TAI and others with regard to the general duty of care under Dutch tort law.⁶⁸³ Nonetheless, again the weaknesses of a tort-based regime come to the fore here. Tort law depends on development through case law, which depends on the decisions of less than perfectly informed judges. Pre-emptive regulation is, therefore, a better solution to proactively define what behaviour is correct under duress.⁶⁸⁴

It must be noted, however, that the Expert Group on New Technologies has proposed some measures which constitute a duty of care for AI-systems. For example, it is recommended that

⁶⁸⁰ See e.g. Art. 8.5 Directive 2019/770; Art. 7.5 Directive 2019/771.

⁶⁸¹ M. KRUIHOF, *Tort Law in Belgium in International Encyclopaedia of Tort Law*, Alphen aan den Rijn, Kluwer Law International, 2018, p. 45-53. Also see J. DE BRUYNE, E. VAN GOOL and T. GILS, “Tort Law and Damage Caused by AI Systems”, *o.c.*, p. 362-363.

⁶⁸² See, e.g., H. BOCKEN, I. BOONE with cooperation by M. KRUIHOF, *Inleiding tot het schadevergoedingsrecht: Buitencontractueel aansprakelijkheidsrecht en andere schadevergoedingsstelsels*, Bruges, Die Keure, 2015, p. 90-91.

⁶⁸³ TJONG TJIN TAI, E. KOOPS, D. OP HEIJ, K. E SILVA AND I. SKORVANEK, “Duties of Care and diligence against cybercrime”, Tilburg University, 2015 available at https://pure.uvt.nl/ws/portalfiles/portal/5733322/Tjong_Tjin_Tai_cs_Duties_of_Care_and_Cybercrime_2015.pdf.

⁶⁸⁴ For a comprehensive overview of the arguments pro and contra *ex post* liability and *ex ante* regulation for AI-systems, see M. SCHERER, “Regulating Artificial Intelligence Systems: Risks, Challenges, Competences, and Strategies”, *Harv. J. L. & Tech.* 2016, p. 354 *et seq.*

there should be a duty on producers to equip technology with the means of information about the operation of the technology (logging by design) whenever such information is necessary for establishing whether a risk materialised. This provision was drafted especially for autonomous systems, requiring that changes to the algorithm (and the reasons why are logged). This is a step in the good direction, but is nonetheless not sufficient.

Making the duty of care clearer is achieved under Belgian law in two ways. First, as will be mentioned below, compliance with product safety laws and cybersecurity laws is usually subject to criminal sanctions and is, therefore, a strict legal prescription which also results in civil liability.⁶⁸⁵ Liability is, therefore, but one enforcement mechanism for the regulatory standards referred to in these laws. Another way is through the use of product liability, which is covered by the Act of 25 February 1991 on the Liability for Defective Products. According to this law, the producer is liable for any and all damage caused by defective products. Again, the scope is limited to physical products, i.e. AI-systems that are embedded in hardware.⁶⁸⁶ The notion of defectiveness is determined at the time of marketing, however, which creates problems for autonomous and adaptive systems. Algorithmic changes may not be covered as “defects” or may be considered alternative causes by the environment. Moreover, adaptive/autonomous systems cause issues when discussing the development defence: how can one exonerate himself/herself for risks which were unknown at the time of development, when the purpose of the system is to further develop itself?⁶⁸⁷

Aside from the abovementioned concerns regarding the duty of care, it must be noted that the opaqueness of the algorithms and the complexity of the technology make faults in the defect, design and/or use of an AI system often very difficult to most claimants.⁶⁸⁸ The Expert Group on Liability and Technologies therefore recommended that the possibility is given to judges to reverse the burden of proof. It must be noted that Article 8.6 of the New Belgian Civil Code allow proof of probability and Article 8.4 allows a judge to reverse the burden of proof if, in light of exceptional circumstances, to maintain the previous rules would be manifestly unreasonable.⁶⁸⁹

To address the abovementioned concerns, the Expert Group on Liability and New Technologies, as well as the European Parliament, have issued reports proposing changes to the Product Liability Directive as well as the general liability framework. One such change proposed by the Expert Group is to impose a strict liability (i.e., entirely faultless) for the producers of high-risk AI-systems, as well as their operators.⁶⁹⁰ This creates thorny questions, which arise in part from gaps. First, it is essential to provide a reform of the Product Liability Directive in order to accommodate for harm caused by non-embedded software. Second, the definition regarding high-risk and low-risk requires clarification. When discussing logging by design, it must be noted that mere access is insufficient; there must be an opportunity for meaningful use of said information, not information overload of the harmed person or of the liable person. Moreover, the distinction between low-risk AI-systems and high-risk AI-systems requires the need to provide a definition of the factors that increase risk and the calculation of risk. This is often not possible due to, *inter alia*, a lack of available statistical data or a lack of the possibility to standardize such factors in a general rule.⁶⁹¹

⁶⁸⁵ See e.g. Art. XI.102 CEL; Art. 51 Act of 7 April 2019 establishing a framework for the security of network and information systems of general interest to public security.

⁶⁸⁶ Art. 2 Product Liability Act.

⁶⁸⁷ European Commission, Expert Group on Liability and New Technologies – New Technologies Formation, “Liability for Artificial Intelligence and Other Emerging Technologies”, o.c., p. 14 therefore argues that a development risk defence should not apply. Also see *infra* part 2.4.2. section B.

⁶⁸⁸ J. DE BRUYNE *et al.*, o.c., 364-366.

⁶⁸⁹ Articles 8.4 and 8.6 Civil Code; also see J. DE BRUYNE, *idem*, 366.

⁶⁹⁰ See for example European Commission, Expert Group on Liability and New Technologies – New Technologies Formation, “Liability for Artificial Intelligence and Other Emerging Technologies”, o.c., p. 39 *et seq.* (operator’s liability) and 42 *et seq.* (producer’s liability).

⁶⁹¹ A. BERTOLINI, “Artificial Intelligence and Civil Liability”, o.c., p. 87 *et seq.*

On 20 October 2020, the European Parliament also adopted a resolution on recommendations for civil liability for the use of AI systems. In this Resolution, the EP provides its own proposal for a civil liability regime for the operation of AI-systems.⁶⁹² It subjects operators of high-risk AI-systems to a strict liability regime. High-risk AI systems are to be listed in an annex to the final Regulation, but no such proposal has been circulated yet, so nothing can be said about what AI-systems will be covered. For other AI-systems, fault liability is retained.

More discussions must, therefore, ensue on this issue. Given the proposal for a Regulation on AI-systems that is to be expected in the first quarter of 2021, any proposed response cannot be formulated without knowledge of this proposal's contents.⁶⁹³

2.3.3. General and Sectoral Product Safety law

Transposing EU Directive 2001/95/EC on General Product Safety, Book IX of the Code on Economic Law provides in general rules governing the safety of all products marketed in Belgium. To specific categories of products, including machines, electrical equipment, medical devices, ... more specific legislations apply to define essential safety requirements for these products.⁶⁹⁴ A comprehensive analysis of all sector- and/or product-specific regulations would exceed the scope of this study. However, a short overview of their essential requirements will be discussed below.

The first gap that immediately becomes apparent is the *lacking substantive scope*. Pursuant to Article I.10, 2° CEL, the scope of "product" is limited to physical products.⁶⁹⁵ Whereas the safety obligation also extends to services, "services" are, for the purposes of Book IX of the Code on Economic Law, defined as "any placement of a product at the disposal of a user and every use by a service provider of a product that entails risks for a consumer, insofar as the service is directly related to that product".⁶⁹⁶ The obligation therefore does not only apply to service providers regarding AI software; it only applies to those who rent hardware-based AI-systems.⁶⁹⁷

This lack of convergence has already been touched upon in the reports on liability for AI-systems and requires reform. For now, the general security obligations for software are enshrined in the cybersecurity regimes (see below), which focus mainly on protection against outside attacks to the systems, but therefore only incidentally on the harm caused by AI-systems to people.

According to Article IX.2 CEL, producers are required to only place on the market products and/or services that are safe and therefore do not cause any harm to individuals that they may not expect. What may be expected, depends in part on the presentation of the good and may therefore be

⁶⁹² European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, 2020/2014(INL), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.pdf.

⁶⁹³ European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme: a Union that Strives for More", COM(2020)37 final, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1581957029354&uri=CELEX:52020DC0037>.

⁶⁹⁴ For a comprehensive overview, the European Commission provides an overview of the product categories on https://ec.europa.eu/growth/single-market/ce-marking/manufacturers_en. Similarly, also see K. VRANCKAERT, J. DE BRUYNE, T. GILS, E. WAUTERS, B. BENICHO and P. VALCKE, "Ethische principes en (niet)-bestaande juridische regels voor AI. Een praktische gids", December 2020, p. 21, https://data-en-maatschappij.ai/uploads/20201112_Rapport-Ethische-richtsnoeren_v1_2020-12-07-151030.pdf. For a general analysis of the specific sectoral obligations under Belgian law see I. CLAEYS and K. KINNAER, "Sectoregerelateerde veiligheidsregelgeving: een bos doorheen de bomen?" in I. CLAEYS and R. STEENNOT (eds.), *Aansprakelijkheid, veiligheid en kwaliteit*, Mechelen, Kluwer, 2015, p. 81-142.

⁶⁹⁵ Note that this was not clear, and not strictly prohibited, under the European framework, it being understood that the framers had only physical products in mind: see e.g. D. FAIRGRIEVE, G. HOWELLS, P.P. MØGELVANG-HANSEN, G. STRAETMANS, D. VERHOEVEN, P. MACHNIKOWSKI, A. JANSSEN and R. SCHULZE, "Product Liability Directive" in P. MACHNIKOWSKI (ed.), *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Cambridge, Cambridge University Press, 2016, p. 46-47.

⁶⁹⁶ See Art. I.10, 5°-7° CEL; also see S. VAN CAMP, "Productveiligheid en Product Recall", *TBH* 2010, p. 455, no. 7.

⁶⁹⁷ *Ibid.*

mitigated by information, or by the function of the AI-system. For example, a knife is not unsafe if it can harm or kill by cutting, but it is unsafe when it can shoot out of the user's hands uncontrollably.⁶⁹⁸ It remains to be seen whether general inferences can be made about these risks for AI-systems.

What constitutes a "safe" product is only defined in general terms to products that, under normal circumstances, produce no risks or risks that are only justified or that may be accepted. This provides no clarification by design; it is nigh impossible to define safety for any product category, which is usually done on a case-by-case basis.⁶⁹⁹

Therefore, Article IX.3 CEL provides a *presumption of safety*: a product is presumed to be safe when it is in conformity with any harmonised standards, concerning the risk categories and the risks covered under those standards.⁷⁰⁰ EU harmonised standards are considered to take precedence over merely national standards. Harmonised standards flow from the EU's New Approach and Legislative Framework, introduced in 1985. The essence is that the Commission determines safety requirements and mandates a European standardisation organisation to draw up standards, which are later published.⁷⁰¹ The safety presumption is then met if the product has been tested in accordance with said standard, in accordance with the required conformity assessment procedure.⁷⁰² These assessment procedures depend on the product that is being tested. These tests may vary from self-certification to prior marketing approval by a specific government body.⁷⁰³

In practice, very often standards are first adopted internationally and then accepted by the standardisation bodies. For the EU, there are three relevant standardisation organisations: CEN (Comité Européen de Normalisation), CENELEC (Comité Européen de Normalisation Électrotechnique) and ETSI (European Telecommunication Standards Institute). Nonetheless, standards comprise of a very wide gamut of standards created by a wealth of bodies: in the field of AI alone, relevant standards are developed by the IEE (Institute of Electrical and Electronics Engineers), International Organization for Standardization (ISO), etc.⁷⁰⁴

In the absence of such harmonised standards, the presumption of safety is evaluated by: non-binding standards that implement other than harmonised standards; national Belgian standards, recommendations of the Commission, any codes of conduct that may be applicable, the state of the art, the safety that users are entitled to expect and any international standards.⁷⁰⁵

It must be noted that the presumption of safety is *rebuttable*. Even if a good were to comply with a standard – or even if its characteristics were to be altered as a result of changes – this presumption of safety can be rebutted.⁷⁰⁶ This becomes relevant in light of AI-systems' inherent adaptive characteristics or as a result of external attacks.

Nonetheless, self-defeating adaptiveness can (and, if possible, should) be avoided. This requires that safety mechanisms are to be built in. We previously mentioned that logging by design should

⁶⁹⁸ Art. I.10, 2° CEL.

⁶⁹⁹ See e.g. D. VERHOEVEN, *Productaansprakelijkheid en productveiligheid*, Antwerp, Intersentia, 2018, p. 97-99.

⁷⁰⁰ *Ibid*, p. 194-195.

⁷⁰¹ For EU harmonised standards, the process is described in Regulation 765/2008/EC setting out the requirements for market accreditation and market surveillance relating to the marketing of products, OJ.L. 218, p. 13-47. For Belgian standards, this process is described under Book VIII of the Code on Economic Law.

⁷⁰² K. VRANCKAERT et al., *Ethische principes en (Niet)-bestaande juridische regels voor AI: een praktische gids*, o.c., p. 20-21.

⁷⁰³ An example can be found in Annex II to Decision 768/2008/EC on a common framework for the marketing of products, OJ. L. 218,, p. 82-128.

⁷⁰⁴ K. VRANCKAERT et al., *Ethische principes en (Niet)-bestaande juridische regels voor AI: een praktische gids*, o.c., p. 20. Another overview of standards related to AI can be found in W. WAHLSTER and C. WINTERHALTER, *German Standardization Roadmap on Artificial Intelligence*, November 2020, p. 144 et seq.

⁷⁰⁵ Art. IX.3§2 CEL.

⁷⁰⁶ D. VERHOEVEN, *Productaansprakelijkheid en productveiligheid*, o.c., p. 195-196.

be implemented.⁷⁰⁷ Other such rules could be clear operational limiters or clear caps on the weights to ensure that the design cannot become unsafe. These essential requirements are clearly applicable. For example, the Royal Decree on the Marketing of Machines defines as an essential requirement that “the operating system must be designed and built in such a way that no dangerous situations arise... that mistakes in the operating logic must not lead to a dangerous situation”, or that a machine may never uncontrollably activate itself.⁷⁰⁸ This also ties in to cybersecurity being an essential part of the design. This is, amongst other things, one of the purposes of the certification framework being developed by ENISA in implementation of the EU Cybersecurity Act (see 2.3.7).

When looking at the standardisation landscape regarding AI-systems, it must be noted that several bodies have taken up the duty of developing standards for AI-systems, such as the ISO, ETSI and the IEEE. Several more are currently under development.⁷⁰⁹ Due to these standards often being private and copyrighted, these are made available at cost. This should pose little problems for large companies, but for SMEs, this lack of transparency could be a hindrance to effective AI development.⁷¹⁰ Therefore, there is a clear need to ensure that standards are made available in a more transparent and affordable way.

Given the lack of access to these standards, it becomes difficult to gauge whether the current certification frameworks will be sufficient to ensure safety of AI-systems. Given the adaptive nature of AI-systems, a continuous certification should be required, although most conformity assessment procedures focus on testing a product before its marketing. This can be avoided by adding clear safeguards in the design, but these could still hinder the functionality of the AI-systems concerned. If that arises, the only way to ensure safety is through good monitoring obligations. This will be discussed in part 4.

2.3.4. General Data Protection Regulation

Several principles of the General Data Protection Regulation also ensure that the design of any ICT product, process or service complies with its laws. As cybersecurity is a part of the principles ensured by the GDPR to protect digital privacy, cybersecurity by design is also supported by the GDPR.

As one of the principles, Article 5 GDPR states that data must be processed “manner and ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures”.⁷¹¹ This supports that security is a part of data protection – as in, the protection of data against external attacks. Similarly, data processing must be kept accurate and up to date, which impacts data quality in some degree. The latter does not, necessarily, ensure sufficient data quality to protect against e.g. algorithmic bias.⁷¹² A similar effect can be observed with the principle of data minimisation, which ensures that only the data is collected and used to train the model which is necessary for the functioning of the AI-system.⁷¹³

⁷⁰⁷ Expert Group on Liability and New Technologies, “Liability for Artificial Intelligence and Other Emerging Technologies”, o.c., recommendation 14.

⁷⁰⁸ Annex I to the Royal Decree of 12 August 2008 on the marketing of machines.

⁷⁰⁹ For a complete overview, W. WAHLSTER and C. WINTERHALTER, *German Standardization Roadmap on Artificial Intelligence*, o.c., p. 14 *et seq.*

⁷¹⁰ See e.g. K. VRANCKAERT et al., *Ethische principes en (Niet)-bestaande juridische regels voor AI: een praktische gids*, o.c., p. 41.

⁷¹¹ Art. 5.1(f) GDPR.

⁷¹² This will be discussed further in part 2.5.3.

⁷¹³ See e.g. T.GILS, E. WAUTERS, B. BENICHO, J. DE BRUYNE and P. VALCKE, *Artificiële intelligentie en gegevensbescherming: een verkennende gids*, Kenniscentrum Data en Maatschappij, Brussels, 2020, p. 37-48.

Based on Article 32 GDPR, the controller and processor of a data processing operation are also required to take all “appropriate” technical and organisational measures to ensure a level of security appropriate to the risk. The type of security refers to the CIA triad mentioned above under 2. This general obligation is general and applies throughout the AI-system lifecycle. It, therefore, also applies in the design phase.⁷¹⁴ What is appropriate depends on the state of the art, the costs of implementation, the context and the risks for data subjects.⁷¹⁵ Security is therefore dynamic and based on risk and context. Some measures are suggested, e.g. the encryption and pseudonymisation of data, the ability to ensure ongoing CIA, the ability to restore the availability and access to personal data in the event of an accident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for security.⁷¹⁶ Compliance with a certified standard (through a certification scheme as provided under the EU Cybersecurity Act (see below part 2.3.7.) or with an approved code of conduct may act as proof of compliance.⁷¹⁷ An often used standard in cybersecurity is and remains ISO 27001. As mentioned previously however, the standardisation and certification framework for AI is still undergoing development.

Article 25 GDPR requires the controller to implement data protection by design and data protection by default. In other words, compliance with data-protection principles must be inserted into the technical design of any system processing personal data, and compliance with data protection principles must be the default setting. The same therefore goes with regard to AI-systems, which must by their technical design limit themselves to the data required and be secure. Again, compliance is proven by adherence to a standard. As previously developed, this standardisation framework is still undergoing development. Practical guidance is therefore limited.⁷¹⁸

In order to comply with any of the abovementioned requirements, a risk assessment prior to the design of an AI-system is required. For some AI-systems, a *data protection impact assessment* will also be required before any processing of personal data, be it for the training of a model or even before the collection of relevant data.⁷¹⁹ More specifically, a Data Protection Impact Assessment (DPIA) is required whenever a processing is likely to lead to high risk to the rights and freedoms of natural persons.⁷²⁰ A DPIA is especially required in three cases: a) systematic profiling, b) profiling on a large scale of sensitive data or c) a systematic monitoring of a publicly accessible area.⁷²¹ In practice, DPIAs serve to document measures that are taken to ensure mitigation of risk, such as a description of the processing operations, the necessity and proportionality, a risk assessment and a suggestion of measures. This carries within it the risk of a “tick-the-box” attitude to risk assessment, which must be avoided at all cost.⁷²² Again, compliance can be proven by

⁷¹⁴ See e.g. ENISA, “AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence”, December 2020, p. 10-11.

⁷¹⁵ Art. 32.1 and 32.2. GDPR; see Recital 83 GDPR.

⁷¹⁶ Art. 32.1. GDPR. For an overview, see T.GILS, E. WAUTERS, B. BENICHO, J. DE BRUYNE and P. VALCKE, *Artificiële intelligentie en gegevensbescherming: een verkennende gids*, o.c., p. 49-57.

⁷¹⁷ Art. 32.3. GDPR.

⁷¹⁸ Nonetheless, a practical overview can be found in T.GILS, E. WAUTERS, B. BENICHO, J. DE BRUYNE and P. VALCKE, *Artificiële intelligentie en gegevensbescherming: een verkennende gids*, o.c., p. 29-37.

⁷¹⁹ Art. 35 GDPR.

⁷²⁰ Art. 35.1 GDPR. Note that the rights and freedoms do not only concern the right to privacy, but may require the controller to take into account other rights as well: ARTICLE 29 WORKING PARTY, “Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”, 4 April 2017, p. 6.

⁷²¹ Art. 35.3 GDPR. Other examples are given in ARTICLE 29 WORKING PARTY, *idem.*, 9-10. Notable examples include evaluation or scoring systems and any use of innovative new technologies. In other words, whenever AI is used in a field where the application is novel, a DPIA could very well be required by the local data protection authority. Similarly, the Data Protection Authority adopted its own list of processing operations for which a DPIA is required: Beslissing van het Algemeen Secretariaat no. 01/2019 van 16 januari 2019, available at <https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf>.

⁷²² See, among others, T. GILS et al., *Artificiële intelligentie en gegevensbescherming: een verkennende gids*, o.c., p. 50-65.

adherence with an approved code of conduct.⁷²³ Data protection impact assessments are also dynamic: where necessary, they must be repeated in the event of a change of risk.⁷²⁴ For adaptive systems, there must therefore be systems in place to ensure that such changes are detected (logging by design). In the event there remains a high risk, the local data protection authority must be consulted before proceeding. Local laws may require controllers to obtain prior authorisation.

The GDPR, therefore, requires AI developers and designers to conduct risk assessments and to ensure that any personal data is sufficiently protected. How they are to do so, is left unclear by the legal rules and depends on either the technical inventiveness of the AI designer and/or the implementation of developing standards. Moreover, it must be noted that the risk assessment enables, but does not require the protection of any interests other than privacy. Since AI-systems' use can also impact freedom of speech and physical integrity (to name but a few), other risk assessments are required. However, the GDPR, given its scope, fits its purpose as well as the other frameworks do theirs: flexibly, albeit vaguely, and dependent on concrete standardisation.⁷²⁵

It must be noted that the European Data Protection Board is beginning to publish guidance on how to comply with its regulation for certain tools that often make use of AI. Examples include virtual voice assistants (such as Apple's Siri, Google's Google Home, Microsoft's Cortana and Samsung's Bixby) and connected vehicles.⁷²⁶

2.3.5. General Non-Sectoral Cybersecurity Regulation: The NIS Act and the CIC Act

Information security is directly protected under Belgian law by the Act of 7 April 2019 establishing a framework for the security of information systems of general interest to public security (NIS Act).⁷²⁷ This law implements the NIS Directive into Belgian law and provides general obligations to take any necessary cybersecurity measures towards some (but not all) operators of ICT services.⁷²⁸ For some entities providing critical importance to security (not just information security), the Act of 1 July 2011 on the security and protection of critical infrastructures (CIC Act) provides for additional obligations.⁷²⁹ This law implements the Directive on Critical Infrastructures into Belgian law.⁷³⁰ As a part of its New Cybersecurity Strategy, the Commission has published proposals to reform both Directives.⁷³¹ Both regimes (both current and future) will be discussed.

⁷²³ Art. 35.8. GDPR.

⁷²⁴ Art. 35.11 GDPR.

⁷²⁵ See also M. FIERENS, S. ROYER and P. VALCKE, "Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels", RW 2020, p. 322-335.

⁷²⁶ European Data Protection Board, Guidelines 02/2021 on Virtual Voice Assistants, 9 March 2021, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_022021_virtual_voice_assistants_adopted-public-consultation_en.pdf; European Data Protection Board, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, 9 March 2021, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf.

⁷²⁷ Act of 7 April 2019 establishing a framework for the security of network and information systems of general interest to public security, MB. 3 May 2019.

⁷²⁸ Directive 2016/1148/EU concerning measures for a high common level of security of network and information systems across the Union, OJ.L. 194, p. 1-30.

⁷²⁹ Act of 1 July 2011 concerning the security and protection of critical infrastructures, MB 15 July 2011.

⁷³⁰ Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ.L. 345, p. 75-82.

⁷³¹ European Commission, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient", 16 December 2020 available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391; Proposal for a Directive on measures for high common level of cybersecurity across the Union, COM(2020)823, available at <https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union>; Proposal for a Directive on the resilience of critical entities, COM(2020)829, available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf.

First, we will discuss the scope. Then, we will discuss the general security obligations as provided for under these regimes.

- Definition of Cybersecurity

As previously mentioned, cybersecurity is defined under the NIS Act and the CIC Act as the preservation of the CIA triad, nothing more.⁷³² Therefore, the protective measures are mainly directed towards protecting AI-systems from external attacks by attackers using whatever means that are available, including other AI-systems. Harm caused to humans is left entirely to product safety legislation or to sector-specific legislation protecting certain types of legislation (e.g. financial stability is protected by financial security regulation). These are discussed in other points in this report. The lack of convergence was already identified as a regulatory gap.

The measures proposed by the NIS Act are best summarised as “incident handling”. Incidents are defined as any event with a negative impact on information security. Incident handling relates to any procedure to detect, analyse and respond to incidents.⁷³³

Under the CIC Act, the definition of information security refers to the abovementioned definition under the NIS Act.⁷³⁴

- Responsible Entities

Under the NIS Act, there are two possible entities responsible for compliance. The first are Operators of Essential Services (OES). The latter are digital service providers.⁷³⁵

OES are public or private entities that are active in one of the sectors referred to under Annex I of the NIS Act and have been identified as such by the competent sectoral authority.⁷³⁶ For said designation, an operator must provide a service of essential importance to critical activities, dependent on network and information systems, and an incident can have a significant disruptive effect. The significance of the disruptive effect depends on the amount of affected users, the dependence of the activities, the consequences of an incident, market share, geographical area and the importance of the OES for the maintenance of an adequate level of service.⁷³⁷ In order to ensure that the essential entities are not the target for attacks, they were informed by their sectoral agencies individually.⁷³⁸

Digital service providers comprise of any and all information society services as defined under EU Directive 2015/1535. They consist of online marketplaces, online search engines and cloud computing providers.⁷³⁹ Digital service providers have lighter reporting obligations than OES. This will be discussed below. It must be noted that none of the obligations apply to any operator of a digital service that is a micro-enterprise or small enterprise as defined under Commission Recommendation 2003/361/EC.⁷⁴⁰ This greatly diminishes the coverage of cybersecurity

⁷³² See Art. 6, 9° NIS Act.

⁷³³ Art. 6, 13°-14° NIS Act.

⁷³⁴ Art. 3, 14° CIC Act.

⁷³⁵ See Art. 3 NIS Act.

⁷³⁶ Art. 3, 11° NIS Act. These sectors are energy (electricity, gas, oil), transport (air, rail, water, road), finance (financial institutions, including credit institutions, and financial trading platforms), healthcare, drinking water, and digital infrastructure (IXPs, DNS services, registries for TLD domains). These sectoral authorities have been identified in the Articles 3-4 Royal Decree of 12 December 2019 implementing the NIS Act, MB 18 July 2019.

⁷³⁷ Art. 12 and 13 NIS Act.

⁷³⁸ See for more information: <https://ccb.belgium.be/nl/nieuws/nis-wetgeving-eerste-identificatiefase-van-aanbieders-van-essenti%C3%ABle-diensten-belgi%C3%AB>.

⁷³⁹ Annex 2 NIS Act.

⁷⁴⁰ Art. 32 NIS Act. These refer to enterprises that employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed 10 million EUR: Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises, OJ.L. 124, p. 36-41.

regulation, as the majority of companies nowadays are SMEs which could still cause real damage. Therefore, an increase in the coverage is essential.

Due to the increased digitisation and interconnectedness of network and information systems, these sectors no longer represent the service providers which are currently essential.⁷⁴¹ For example, cloud providers have become more important in recent years. Therefore, the Proposal for the NIS 2 Directive extends the sectors which are considered essential.⁷⁴² Moreover, rather than maintaining the distinction between OES and digital service providers and rather creates two categories of responsible entities: essential and important entities.⁷⁴³ These have more or less the same obligations under this proposal. This is welcome, as convergence will only increase. In light of the increasing dependence on technologies, the obligations for any entity may increase, as they can provide essential risks depending on the service they provide.

The CIC Act applies only to the sectors of transport and energy for the protection of national and European critical infrastructures, with the exception of nuclear installations and air transport. Critical infrastructures are defined as assets, systems or parts thereof which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.⁷⁴⁴ European critical infrastructures are critical infrastructures where the disruption would have a significant impact in at least two Member States.⁷⁴⁵ Like essential entities, the designation of critical infrastructure is determined by each sectoral agency in concertation with the General Direction Crisis Centre, which determines its own criteria. Intersectoral criteria which must be taken into account are the amount of potential victims, the potential economic impact and the potential impact on the population.⁷⁴⁶ This scope is maintained in the Proposed Directive on the Resilience of Critical Entities.⁷⁴⁷

- The Obligations of OES and Digital Service Providers

OES are required to take all appropriate and proportionate technical and organisational measures to control risks for the security of its network and information systems, ensuring a risk-based security. Similarly, the OES is to take appropriate measures which prevent incidents or minimize their consequences, in order to ensure business continuity.⁷⁴⁸ This general security obligation contains no appropriate guidance as to what to do.

To document its security measures, an OES is required to implement a security policy for its network and information systems within twelve months of its designation, where the measures are to be implemented within twenty-four months after designation. To provide some guidance, the information security plan is considered to be in conformity with the security requirements if it complies with ISO 27001 or any standard which is recognised by Royal Decree as being equivalent. Thus, a prior security audit is required.⁷⁴⁹ This conformity is proven by issuance of a certificate of

⁷⁴¹ See the NIS 2 Proposal, p. 5.

⁷⁴² Pursuant to the Annex to the NIS 2 Proposal, these sectors now include energy (electricity, district heating and cooling, oil, gas, hydrogen), transport (air, rail, water, road), banking, financial infrastructure, health, drinking water, waste water, digital infrastructure (not only IXP providers, DNS providers and TLD name registries, but also cloud computing service providers, data centre service providers, content delivery network providers, trust service providers, providers of public electronic communications networks), public administration and space. See EC, Annex to the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across, the Union, repealing Directive 2016/1148, COM(2020) 823 final.

⁷⁴³ See Art. 17 *et seq.* NIS 2 Proposal.

⁷⁴⁴ Art. 3, 4^o-6^o CIC Act.

⁷⁴⁵ *Ibid.*

⁷⁴⁶ See Art. 5-11 CIC Act.

⁷⁴⁷ See Art. 5 CIC Proposal.

⁷⁴⁸ Art. 20 NIS Act.

⁷⁴⁹ M. FIERENS, S. ROYER and P. VALCKE, "Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels", *o.c.*, p. 328.

conformity.⁷⁵⁰ Note that, like the presumption of safety in product safety laws, this presumption is rebuttable: compliance with the standard does not make one's network and information systems secure. This can become relevant for AI-systems, insofar as the speed of technical development or the specific nature of AI-systems can make ISO 27001 obsolete.

Digital service providers must comply with similar security obligations, but are subject to lighter obligations. The reduction in scope regarding SMEs was already discussed. Article 33 NIS Act only obliges digital service providers to identify the security risks for the systems they use and take appropriate and proportional measures to mitigate these risks. These must take into account the security of systems, the treatment of incidents, business continuity management, control and testing and compliance with international norms. Furthermore, incidents must be prevented and their consequences minimized in order to safeguard the continuity of their services.⁷⁵¹ The required security elements are further clarified under Regulation 2018/151.⁷⁵² The required elements are listed in very general terms and comprise, amongst other things, that all network and information systems be mapped and appropriate policies must be established on the management of information security, including risk analysis, HR, security architecture, encryption, access controls, etc.

This requires further implementation through standardisation for certain systems. This approach should contain a horizontal baseline for AI-systems and sector-specific applications where necessary. The still-developing nature of this framework has already been mentioned. It is therefore that the NIS Directive requires Member States to encourage standardisation.⁷⁵³ Whereas there is a real risk of overregulating the security of AI-systems, regulation is best dealt with at the early stages of technology, in order to avoid the Collingridge dilemma.⁷⁵⁴ Nonetheless, regulations should aid efficient behavior. All too often, regulations and measures are sidestepped because the costs of complying with them (time, effort) exceed the gains to be brought in terms of efficiency.⁷⁵⁵ Granted, this can be taken in the calculus of "risk-based" measures for individuals, creating a collective action problem. Both sides of the argument must be addressed in new standards and AI regulation. Industry standards could therefore be the optimal balance, as long as they are adopted swiftly and flexibly enough, with sufficient oversight to avoid that the industry serves only its own interests.

The NIS 2 Proposal provides similar obligations to provide for appropriate and proportional technological and organisational measures, clarifying their contents.⁷⁵⁶ In tandem with the approach championed by fourteen Member States, standardisation and certification will determine the cybersecurity measures for Artificial Intelligence. This places great expectations on ENISA to implement the appropriate certification schemes. These will be discussed further below.

- Control and Sanctions

Annually, an OES must implement an internal audit of the network and information systems on which its essential services depend, to ensure that these measures are correctly implemented.

⁷⁵⁰ Art. 22§1-2 NIS Act.

⁷⁵¹ Art. 33 NIS Act.

⁷⁵² Commission Implementing Regulation 2018/151 laying down rules for application of Directive 2016/1148 of the European Parliament and the Council as regards further specifications for the elements to be taken into account by

⁷⁵³ Art. 19 NIS Directive.

⁷⁵⁴ The Collingridge dilemma described a paradox all technology regulators face: technology's impacts cannot be predicted at the outset, whereas control or change is difficult when the technology has become entrenched. It is taken from J. COLLINGRIDGE, *The Social Control of Technology*, New York, St. Martin's Press, 1980, 200 p.

⁷⁵⁵ This "rational ignorance" is not necessarily out of laziness, but is the behaviour of rational subjects. See e.g. C. HENLEY, "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users", Paper from the Proceedings of the 2009 workshop on New Security Paradigms, September 2009, <https://doi.org/kuleuven.ezproxy.kuleuven.be/10.1145/1719030.1719050>.

⁷⁵⁶ Art. 18 NIS 2 Proposal.

Every three years, an external audit must be performed. Certification audits (such as certification with ISO27001) are made equivalent. At the same time, inspection services can conduct controls at any time by the OES of its security measures and incident reporting obligations. OES are supposed to fully cooperate with these audits.⁷⁵⁷

Digital service providers have similar evaluation obligations. Implementing Regulation 2018/151 provides that the monitoring, auditing and testing shall include the conducting of a planned sequence of observations or measurements to measure performance, inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met, as well as a process to reveal flaws in the security management. Standards may also be used as proof of compliance.⁷⁵⁸ The inspection services have the same competences as they do towards OES.⁷⁵⁹ Digital service providers are required to provide all essential information in time, as well as to correct any identified non-compliance.⁷⁶⁰

For both types of operators, the inspection services may enjoin specific measures.⁷⁶¹ Non-compliance is punished by criminal sanctions.⁷⁶²

The NIS 2 Proposal provides clarification regarding the powers of the inspection services and provides additional rules for penalties for breaches.⁷⁶³

- Obligations of Critical Infrastructures and Critical Entities

The designation of critical infrastructures was already discussed.

Operators of critical infrastructure must take *internal security measures*. These include the implementation of an Operator Security Plan (OSP) to prevent, limit and neutralise any risks of disruption of the functioning or of destruction of the critical infrastructures. This plan contains at the least permanent measures for all circumstances and gradual internal security measures, as a function of the threat. The procedure must contain, at least, an inventory of points of infrastructure which could be hit, a risk analysis, an analysis of the vulnerabilities and an identification of internal security measures for each scenario resulting from the risk analysis. This OSP must be implemented within one year after designation. The measures must be implemented within twenty-four months after designation.⁷⁶⁴

In order to continue to monitor compliance, the operator of critical infrastructure is also required to organise exercises for updating the OSP, as a function of lessons taken from exercises or any change in the relevant risk analysis.⁷⁶⁵

The GDCC and the local mayor may also take additional *external security measures*.⁷⁶⁶

The Proposal for a Directive on the Resilience of Critical Entities clarifies the risk assessment obligations further, stating that all critical entities must assess within six months after having been

⁷⁵⁷ See Art. 38-46 NIS Act.

⁷⁵⁸ Art. 2 Implementing Regulation 2018/151.

⁷⁵⁹ Art. 47 Nis Act.

⁷⁶⁰ Art. 47 §2 NIS Act.

⁷⁶¹ Art. 48-50 NIS Act.

⁷⁶² Art. 51 *et seq.* NIS Act.

⁷⁶³ Art. 28-33 NIS Directive.

⁷⁶⁴ Art. 13 CIC Act.

⁷⁶⁵ *Ibid.*

⁷⁶⁶ Art. 15-17 CIC Act.

notified, and where necessary and at least every four years, all relevant risks that may disrupt their operations. The contents of such risk assessment are also clarified in its Articles 11 *et seq.*⁷⁶⁷

2.3.6. Sectoral Cybersecurity Regulations – Security of the Design

The general NIS Act does not apply to specific sectoral entities, as they fall under their own regimes. These will be discussed here. Note that the NIS 2 Proposal provides general obligations which will also apply to these entities as well.⁷⁶⁸ These each provide their own security obligations. The sector-specific context of these regulations sometimes enables a more granular regulation. This is especially apparent in the financial sector, given the specific requirements imposed on algorithmic trading and future proposals for all financial entities.

For trust service providers, Articles 19 of the e-IDAS Regulation requires them to take appropriate technical and organisational measures to manage all risks to the security of the trust services they provide, thus subjecting them to the same general security regulation as imposed under the NIS Act and GDPR.⁷⁶⁹

For the providers of publicly available electronic communications services, Article 114 of the Electronic Communications Act subjects them to the same general security obligation as well. These measures include at the least measures to ensure access controls, the availability of security policies, as well as preventive measures to ensure that the integrity of their networks is assured and that the availability of their service is ensured as much as possible.⁷⁷⁰ This general security obligation has an EU legal basis in Article 40 of the Electronic Communications Code and Article 4 of the e-Privacy Directive.⁷⁷¹

Similar obligations are also imposed on the providers of payment services and investment firms; however, their security requirements are more specific. As the type of service (and therefore the risks) are better known and identifiable, more granular guidance-based measures are easier to achieve.

Implementing Articles 95 *et seq.* of the Payment Services Directive 2 (PSD2), Articles 49 *et seq.* of the Payment Services Act provide for security obligations. Payment services providers must comply with general and secure communication standards for identification, authentication, communication and for the execution of security measures, in accordance with technical regulations implementing the PSD2 Directive.⁷⁷² Payment services are also required to conduct a detailed analysis of the operational and security risks connected to their services. In order to protect their users, payment services providers must also provide appropriate risk-mitigating measures.⁷⁷³ Regarding, *inter alia*, the regulatory standards for authentication and common and secure open standards of communication, the Commission has implemented Delegated Regulation 2018/389, providing guidance on security measures for strong authentication.⁷⁷⁴ Payment

⁷⁶⁷ Art. 10 *et seq.* CIC Proposal.

⁷⁶⁸ See Art. 2 NIS2 Proposal.

⁷⁶⁹ Art. 19 Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, *OJ.L.* 257, p. 73-114.

⁷⁷⁰ Art. 114 §1-4 Act of 13 June 2005 on electronic communications ("Electronic Communications Act"), *MB* 20 June 2005.

⁷⁷¹ Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, *OJ.L.* 201, p. 37-47; Art. 40 Directive 2018/1972 establishing the European Electronic Communications Code, *OJ.L.* 312, p. 36-214.

⁷⁷² Art. 49 Act of 11 March 2018 on the legal status of and the supervision on payment services providers and the institutions for electronic money, access to the business of payment services provider and the activity to issue electronic money, and access to payment systems, *MB* 26 March 2018; Art. 97 and 98 Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, *OJ.L.* 337, p. 35-127.

⁷⁷³ Art. 50-52 Payment Services Act; Article 95 PSD2 Directive.

⁷⁷⁴ Art. 4 *et seq.* Commission Delegated Regulation 2018/389 of 27 November 2017 supplementing Directive 2015/2366 of the European Parliament and the Council with regard to regulatory standards for strong customer authentication and common and secure open standards of communication, *OJ.L.* 69, 133.2018, 23-43.

services providers are required to have transaction monitoring mechanisms in place to detect unauthorized or fraudulent payment transactions.⁷⁷⁵ The security measures must be periodically reviewed and audited.⁷⁷⁶

Similar rules are in place for *investment firms* and more specific rules are already in place especially for one technique which has already been using AI for longer, i.e. *algorithmic trading*. Investment firms, APAs, CTPs and ARMS are required to have sound security mechanisms in place to guarantee the security of the means of transfer information, minimize the risk of data corruption and unauthorized access and to prevent information leakage before publication.⁷⁷⁷ Implementing the MiFiD II Directive, the MiFiD II Act provides for the obligation to ensure that, *inter alia*, regulated markets have in place effective systems, procedures and arrangements to ensure that their systems are resilient, have sufficient capacity to deal with peak order and message volumes, are able to ensure orderly trading under conditions of severe market stress, are fully tested to ensure such conditions are met and are subject to effective business continuity arrangements to ensure continuity in the event of failure.⁷⁷⁸ In other words, investment firms are subject to extensive and detailed obligations to ensure security throughout their lifecycle.

Some technical measures for algorithmic trading systems are referred to under Delegated Regulation 2017/589.⁷⁷⁹ These measures include the following, amongst others:

- Prior to deployment, investment firms must establish clearly delated methodologies to develop and test any system, algorithm or strategy it wishes to deploy. The deployment is authorized by a member of senior management of the investment firm. The algorithms must be tested in accordance with their specific market prior to deployment and in the vent of substantial updates. Moreover, Article 5(4) of the Delegated Regulation explicitly requires that the algorithm does not behave in an unintended manner, complies with the invest firm's obligations under the Regulation, complies with the rules and systems of the trading venues accessed by the investment firm an does not contribute to disorderly trading conditions.⁷⁸⁰
- Investment firms must establish and monitor their trading systems and algorithms through a clear and formalized governance arrangement, including clear lines of accountability, and procedures to approve updates and solutions regarding the algorithms used in trading;
- Investment firms must ensure that their compliance staff have at least a general understanding of how the algorithmic trading systems of an investment firm operate and remain in continuous contact with the technical staff;
- Clear testing methodologies must be implemented to develop and test algorithmic trading systems, algorithms or strategies.
- Testing environments must be separate from the production environments;
- An investment firm must annually perform a self-assessment and validation process and issue a validation report. As a part of said self-assessment, the investment firm must check if the algorithms can withstand increased order flows or market stresses.⁷⁸¹
- Several design features are imposed to increase resilience, such as:

⁷⁷⁵ Art. 2.1. and 2.2. Commission Delegated Regulation 2018/389.

⁷⁷⁶ Art. 3 Commission Delegated Regulation 2018/389.

⁷⁷⁷ Art. 22, 46, 65, 67 MiFiD II Act.

⁷⁷⁸ Art. 48 MiFiD II Directive; Art. 22 Act of 21 November 2017 on the Infrastructure for the Markets for Financial Instruments Implementing Directive 2014/65/EU (MiFiD II Act), MB 7 December 2017. Also see K. VRANCKAERT et al., *Ethische principes en (Niet)-bestaande juridische regels voor AI: een praktische gids*, o.c., p. 22.

⁷⁷⁹ Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organizational requirements of investment firms engaged in algorithmic trading, OJ.L. 87, p. 417-448.

⁷⁸⁰ Art. 5 Commission Delegated Regulation 2017/589.

⁷⁸¹ Art. 9 et seq. Commission Delegated Regulation 2017/589.

- A kill functionality;⁷⁸²
- An automated surveillance system to detect market manipulation;⁷⁸³
- Business continuity arrangements;
- Real-time monitoring of all algorithmic trading taking place under the code of the investment firm, including that of its clients, for signs of disorderly trading;⁷⁸⁴
- Post-trade controls;
- Access restrictions;⁷⁸⁵
- Etc.

On 24 September 2020, the European Commission adopted a digital finance package. This includes a digital finance strategy and legislative proposals on crypto-assets and digital resilience. The latter consists of a new directive updating some of the abovementioned security regulations, as well as a proposal for a regulation on Digital Operational Resilience in the Financial Sector.⁷⁸⁶ The Proposed Regulation provides uniform regulation for all financial services providers. It requires them to have a sound, comprehensive and well-documented ICT risk-management framework, which must be updated once a year. It contains detailed requirements as to what parts this framework must consist of. One important example that will be discussed further below is that requirement to have anomaly detection systems in place.

On 5 March 2021, ENISA published a report providing an overview of all existing policy initiatives in the pipeline regarding cybersecurity in the financial sector.⁷⁸⁷

2.3.7. Certification Under the EU Cybersecurity Act

As previously mentioned, many of the rules refer to the implementation of international standards. Some standards which apply to ICT systems in general can be implemented where possible and can, where possible, also be used to prove compliance (or at least create a rebuttable presumption) of security. However, unlike e.g. the certification mechanisms for physical products, there is not yet much available in the way of cybersecurity certification of ICT products, ICT services and ICT processes. Nonetheless, it was often observed that the security of such processes was lacking.⁷⁸⁸ It is therefore that the EU adopted the Cybersecurity Act.⁷⁸⁹

It was already mentioned that, under the EU Cybersecurity Act, cybersecurity is defined in such a way as that it can comprise both traditional cybersecurity in the form of the CIA triad and AI safety. The EU Cybersecurity Act mandates ENISA to create a European certification scheme for ICT products, processes and services, in order to increase trust in digital technology. In order to do so, the competences of ENISA are increased.

⁷⁸² Art. 12 Commission Delegated Regulation 2017/589.

⁷⁸³ Art. 13 Commission Delegated Regulation 2017/589.

⁷⁸⁴ Art.17 Commission Delegated Regulation 2017/589.

⁷⁸⁵ Art. 18 Commission Delegated Regulation 2017/589.

⁷⁸⁶ I. JANDA, T. ŠČERBA and A. STÁRKOVÁ, "A Few Words on DORA – Proposal for Regulation on Digital Operational Resilience in Financial Sector", 25 November 2020, available at <https://www.whitecase.com/publications/article/few-words-dora-proposal-regulation-digital-operational-resilience-financial>; European Commission, Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 60/2014 and (EU) No 909/2014, COM(2020)595 final.

⁷⁸⁷ ENISA, "EU Cybersecurity Initiatives in the Finance Sector", 5 March 2021, https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector/at_download/fullReport

⁷⁸⁸ M. FIERENS, S. ROYER and P. VALCKE, "Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels", *o.c.*, p. 329 *et seq.*

⁷⁸⁹ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation 526/2013 (Cybersecurity Act), *OJ.L.* 151, p. 15-69.

The Cybersecurity Act has as its purpose to ensure that ICT products, services and processes are secure throughout their entire lifecycle. ICT products, services and processes must not contain known vulnerabilities and must be equipped with mechanisms for updates. New vulnerabilities must be tracked and documented. Logging by design must also be included. Security by design and security by default are listed as express objectives of any EU cybersecurity certification scheme.⁷⁹⁰

A European cybersecurity scheme may specify one of three assurance levels: basic, substantial or high.⁷⁹¹ These provide a definition of the risk that the AI-system may pose. All must ensure that they have been evaluated at a level intended to minimize known security risks and the risks of incidents and cyberattacks. The risk level also determines the kind of conformity assessment: for example, for basic risk systems, self-assessment is permitted, while this is not the case for other forms of risk. The risk level is based on the scenario of the hypothetical attacker and depends on the estimated resources of such attackers.⁷⁹²

It must be noted that certification is required to be voluntary. Certification only creates a presumption of compliance.⁷⁹³ The reason for this choice is that certification is a costly process that can lead to higher prices for consumers. Nonetheless, there remains the possibility for later laws to require certification. Simultaneously, certification creates an incentive in the same way as certification and standardisation do without any legal requirements to do so; even if they are not mandatory, compliance with a standard or certification creates a presumption of conformity, which can create trust.⁷⁹⁴ As previously mentioned, however, certification does not substitute for compliance. Certification and compliance with a standard only creates a rebuttable presumption of compliance with the legal obligation.

At the time of writing, ENISA has published its draft cybersecurity scheme, focusing on general ICT product cybersecurity, called EUCC, to serve as a successor to the existing SOG-IS.⁷⁹⁵ Recently, a certification scheme for Cloud Services has also been published, for which a consultation has been opened from 22 December 2020 to 7 February 2021.⁷⁹⁶

The Cybersecurity Act provides for the possibility to impose sanctions.⁷⁹⁷ It remains to be seen what sanctions Belgium will provide. At first sight, it seems recommended that in its choice, a convergence is chosen with the product safety and NIS framework, i.e. that certification may be linked to a presumption of compliance, where that compliance is required on pain of, amongst others, criminal liability. This can trigger civil liability, even in the presence of contractual liabilities.

2.4. Legal Requirements Governing the Security of the AI-System Post-Release

2.4.1. Introduction

Once released, AI-systems can develop themselves, creating risks post-release. Insofar as these have not been identified and prevented in the design, mechanisms have to be in place to monitor changes in risk and to respond accordingly. In the event that risk materialises, then corrective measures must be taken to minimise the risk. This pattern is found both in product safety laws as security-based regimes. We will discuss the obligation to prevent risks from happening post-

⁷⁹⁰ Art. 51 Cybersecurity Act.

⁷⁹¹ Art. 52 Cybersecurity Act.

⁷⁹² See Art. 52.5-7 Cybersecurity Act.

⁷⁹³ See Art. 56.1-56.2 Cybersecurity Act.

⁷⁹⁴ See M. FIERENS, S. ROYER and P. VALCKE, "Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels", *o.c.*, p. 332.

⁷⁹⁵ See <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme>.

⁷⁹⁶ See <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>.

⁷⁹⁷ Art. 65 Cybersecurity Act; M. FIERENS, S. ROYER and P. VALCKE, "Cyberbeveiliging: een blik op het amalgaam van Europese en Belgische regels", *o.c.*, p. 332.

release. The different fields of law will be treated in the same order as under the previous part (part 2.4.2.). The study will then examine the obligations to take in the event a risk has materialised (part 2.4.3.).

2.4.2. Monitoring and Preventing Risk Post-Release

In the following parts, several regimes will be discussed. Once we have examined the contract law framework (part A.), tort law (part B.) as well as product safety legislation are analysed (part C.). We will also assess risk-management under data protection law (part D.) as well as non-sectoral (part E.) and sectoral cybersecurity rules (part F.).

A. General Risk-Management under General and Specific Contract Law

Under general contract law, it may be agreed that certain services are to be delivered to prevent risks from occurring. This depends on the content of the arrangement. Typical for most sales contracts, for example, is that risks that materialise after release are not covered under the regimes for conform delivery, nor for the regime for hidden defects. Defects have to have been present at the time of the passing of risk and not later.⁷⁹⁸ This can exonerate AI-suppliers. This is mitigated somewhat by presumptions of anteriority of certain defects. For consumer sales, Article 1649quater CCL mandates that the salesman is liable for any defect that manifests itself within two years of delivery, with a presumption of anteriority in the event the defect materialises within six months.⁷⁹⁹ Court sometimes accept a presumption of anteriority in the event the buyer has normally used the good.⁸⁰⁰ For services contracts, the obligation of the service provider depends on the Service Level Agreement, which contractually can define certain levels of security. What constitutes the obligation to ensure security, depends fully on the service provided and may arise from either common practice or common standards in the market. It must be noted that both computer programmers and security firms are considered to take on themselves only an obligations of best efforts. Therefore, liability for security incidents can only be proven in the event of a defect or in the event it can be argued that they did not take adequate care to minimize security or safety risks.⁸⁰¹

New rules of consumer protection law are set to change this regime. Article 8 Directive 2019/770 requires, as part of the objective conformity of digital content, that the trader must ensure that the consumer is informed of and supplied with updates, including security updates, that are necessary to keep the digital content or digital service in conformity, either for the period during which the digital content or digital service is provided, or the time that the consumer may reasonably expect. Liability for not doing so is only avoided in the event that the trader informed the consumer about the lack of availability of updates and the consequences of non-installation, and the consumer failed to install or incorrectly installed the update due to reasons other than shortcomings in the instructions of the trader.⁸⁰² The same obligation is provided for any digital content sold with physical consumer goods.⁸⁰³ However, this provision only refers to the safety and security the consumer may reasonably expect, which is a vague and open-ended question.

⁷⁹⁸ B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht*, o.c., p. 332 et seq.

⁷⁹⁹ Art. 1649quater CCL.

⁸⁰⁰ B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht*, o.c., p. 334.

⁸⁰¹ F. BURSSSENS, *Handboek Aannemingsrecht*, Antwerp, Intersentia, 2018, p. 120.

⁸⁰² Art. 8.4. Directive 2019/770. Also see I. CLAEYS and N. DE WEERDT, “De conformiteit van digitale inhoud en digitale diensten” in E. TERRY and I. CLAEYS (eds.), *Nieuw recht inzake koop & digitale inhoud en diensten*, Antwerp, Intersentia, 2020, p. 137 et seq. and 152 et seq.

⁸⁰³ Art. 7.3-4 Directive 2019/771.

B. General Tort Law

Previously, we discussed the general duty of care of any AI-providers regarding the supply of products. This duty of care may extend to certain after-sales services. However, this again requires that the duty of care is clearly defined and well-known, which is often not the case.⁸⁰⁴ At the same time, the more control is relinquished to an AI-system, the more difficult it becomes to attribute control to said entity. That is the reason that strict liability for high-risk AI-systems is suggested.⁸⁰⁵ It is, therefore, also not a surprise that many of the preventive rules on product safety and cybersecurity are imposed on pain of sanctions, which clarifies their liability.

With regard to product liability law, it must be noted that product liability allows for a defence if the defect developed after release of the product.⁸⁰⁶ For adaptive AI-systems, this is problematic. The development defence creates a double block for liability under this regime, as producers can also escape liability whenever the defect could not have been known at the time of release, on the basis of the state of the art. It must be noted that the latter defence often fails. Nonetheless, the above-mentioned legal gaps have moved towards proposals for a strict liability for “high-risk” AI-systems. Therefore, the Expert Group on Liability and New Technologies has recommended that a strict liability regime is created for both operators and for producers of AI-systems.⁸⁰⁷ For producers, the development risk defence should not be applicable according to the Expert Group. On 20 October 2020, the European Parliament adopted a Resolution on Civil Liability for Artificial Intelligence, to which it joined a proposal for a Regulation on Liability for the operation of Artificial Intelligence Systems. It creates a strict liability regime for all high-risk AI-systems, which are to be listed exhaustively in an Annex to the final Regulation. For other AI-systems, the regular fault liability system is maintained.⁸⁰⁸

C. General Risk Management Under Book IX of the Code on Economic Law and Sectoral Product Safety Legislation

Article IX.8 CEL requires that producers inform the user of any information that provides the user with the possibility to make an assessment of the risks inherent to this products, and to protect the user of the risks associated with this product. This obligation may be difficult to comply with all the time, because the risks of e.g. unsupervised learning systems are unknown at the time of release. Nonetheless, this would impact the safety principle, which could impose limitations on the design in and of itself (see above 2.3.)

Article IX.8 CEL also requires that producers of products, within the limits of their activities must take any measures commensurate with the characteristics of the products they impose, to 1° be informed of any risks these products may pose and b) choose to take appropriate action to avoid these risks, including withdrawal from the market and warning consumers or even a recall of the product at hand.⁸⁰⁹ These measures include indication of the identity and the details of the producer and the product reference, as well as, in all cases where appropriate, the carrying out of

⁸⁰⁴ See TJONG TJIN TAlet al., *o.c.*

⁸⁰⁵ See part 2.3.2. section B; Expert Group on Liability and New Technologies, “Liability for Artificial Intelligence and Other Emerging Technologies”, *o.c.*, p. 39-44.

⁸⁰⁶ Art. 12.b) Product Liability Act.

⁸⁰⁷ Expert Group on Liability and New Technologies, Liability for Artificial Intelligence and other Emerging Technologies, *o.c.*, recommendations 6 and 8.

⁸⁰⁸ European Parliament, Resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence, P9_TA(2020)0276, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html.

⁸⁰⁹ Art. IX.8§2 CEL; Art. 5.1 Product Safety Directive.

sample tests of marketed products, investigating and, if necessary, keeping a register of complaints and keeping distributors informed of such monitoring.⁸¹⁰

For autonomous systems, it was already mentioned that the risks continuously evolve as a result of the algorithm. Insofar as such changes are possible, it therefore becomes necessary to include automated logging of algorithmic changes and the reasons in the design to ensure that this compliance is met. So far, there is no knowledge of a standard which imposes this specifically for AI-systems. Such logging by design was, nonetheless, recommended by the Expert Group on New Technologies in its report on liability for AI.⁸¹¹ This needs further research. One possible gap that may arise is that mere logging of the changes may not provide enough information as to why a certain decision altered. Moreover, once information has been learned in a way which is undesirable, how can one make an AI-system unlearn by way of corrective measures?

Distributors are also required to contribute to help to ensure compliance with the applicable safety requirements, in particular by not supplying any products which they know or should have presumed, on the basis of the information in their possession as professionals, do not comply with these requirements. Moreover, they must also participate in the monitoring of any risks of products placed on the market by passing on information on product risks, keeping and providing documentation necessary for tracing the origin of products and cooperating in any action taken by the producers and competent authorities to avoid any risks.⁸¹² As the focus of the products relates to physical products, this is easy to monitor. For software systems, very often automated control is possible. Nonetheless, it must be noted that, as distributor, the information about the AI-system and the underlying algorithm of any distributor is likely often even lower than that of the producer.

For the purpose of traceability, often sectoral regulations require that the producers keep the technical file for the products they release for a certain time, usually ten years.⁸¹³ The focus of the security obligation of e.g. machine manufacturers, however, is focused on pre-release and not post-release. For some products providers, however, risk-management will also be provided. One such examples includes the producers of medical devices. These are required to ensure that manufacturers shall not only keep the relevant documentation, but that they are also required to maintain a quality management system, which contains processes for monitoring and measurement of output, data analysis and product improvement.⁸¹⁴

D. General Risk-Management under Data Protection Law

The general obligation of controllers to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk was already discussed in part 2.3.4. As previously mentioned, what measures are “appropriate” is highly dependent on the risks and context. Not much guidance is given by the GDPR. It does clarify that appropriate measures include, as appropriate, “the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services” and “a process for regularly testing, assessing and

⁸¹⁰ *Ibid.*

⁸¹¹ Expert Group on Liability and New Technologies, “Liability for Artificial Intelligence and Other Emerging Technologies”, o.c., recommendation 9.

⁸¹² Art. IX.8 §3 CEL; Art. 5.2 Product Safety Directive.

⁸¹³ See e.g. the Royal Decree of 12 August 2008 on the Marketing of Machines. Also see K. VRANCKAERT *et al.*, *Ethische principes en (Niet)-bestaande juridische regels voor AI: een praktische gids*, o.c., p. 24-25.

⁸¹⁴ See e.g. Art. 10 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, OJ.L. 117, p. 175. It must be noted that the entry into force of said regulation has been moved to May 2021 as a result of the COVID-19 outbreak. Its provisions may, therefore, be left inapplicable until the time the COVID-19 pandemic is over in Europe.

evaluation the effectiveness of technical and organisational measures for ensuring the security of the processing”.⁸¹⁵

In order to know what processing operations go on, the records of processing is a helpful tool.⁸¹⁶ It is essential to know the data flows that are available in an organisation – and within the AI-system – to ensure compliance with security. This requires, *inter alia*, access logging, but also logging of what data is being processed by the algorithm. As AI-systems are more and more capable of inferring personal data from certain data sets, anonymisation is becoming ever more difficult.⁸¹⁷

Furthermore logging by design is also required in order for timely notifications of any personal data breaches. These are discussed in part 2.4.3. section C. The guidelines of the EDPB regarding some AI systems (such as virtual voice assistants and connected vehicles) have been mentioned above.⁸¹⁸

E. General Risk-Management under Non-Sectoral Cybersecurity Rules – NIS and CIC

In part 2.3.5, we already discussed the general obligations imposed upon OES and digital service providers to provide for appropriate and proportionate technical and organisational measures to control any risks for the security of network and information systems, as well as to minimize the consequences of an incident. These measures not only include preventive measures, but also ensure that, throughout the management of the network and information system. The precise content of these measures is left to standardisation and implementing acts. For OES, the information security plan is considered compliant if it has been certified in accordance with ISO 27001.⁸¹⁹ For digital service providers, Commission Implementing Regulation 2018/151 provides for clarifications regarding the security elements, which include incident handling measures such as detection processes, reporting of weaknesses and identifying weaknesses in the system, as well as a response in accordance with established procedures.⁸²⁰ Also business continuity management measures must be provided, as well as additional monitoring.⁸²¹

Under the NIS 2 Proposal, cybersecurity risk-management measures that are taken by essential and important entities are further clarified. The appropriate measures must at least include incident handling (detection, prevention, response to incidents), business continuity and crisis management, security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure and policies and procedures to assess the effectiveness of such measures.⁸²²

Similarly, for critical infrastructures, monitoring obligations must be implemented in the OSP that is to be submitted and re-evaluated by any entity designated by the sectoral entity as a critical

⁸¹⁵ Art. 32.1, (b)-(d) GDPR.

⁸¹⁶ Art. 30 GDPR; T.GILS et al, *o.c.*, p. 49-50.

⁸¹⁷ An example includes the teenage girl whose pregnancy was detected on the basis of her purchase behaviour: K. HILL, “How Target Figured Out a Teen Girl was Pregnant Before her Father Did”, *Forbes*, 16 February 2012, available at <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>.

⁸¹⁸ See 2.3.4.

⁸¹⁹ Art. 22 NIS Act.

⁸²⁰ See Article 2 Commission Implementing Regulation 2018/151 laying down rules for application of Directive 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, *OJ.L.* 31.1.2018, p. 48-51.

⁸²¹ Art. 2 Commission Implementing Regulation 2018/151.

⁸²² Art. 18 NIS 2 Proposal.

infrastructure.⁸²³ Similarly, under the Proposed Directive on the Resilience of Critical Entities, the resilience measures to be taken by critical entities are further clarified, although they are kept in a very general phrasing. The OSP will thus likely be further updated, while the actual measures imposed will not have to change.⁸²⁴

F. General Risk Monitoring and Management under Sectoral Cybersecurity Rules

The general cybersecurity obligations of *trust services providers* have already been discussed in part 2.3.6. Qualified and non-qualified trust providers are required to take appropriate technical and organisational measures to manage the risks posed to the security of the services they provide. These obligations last throughout their service.⁸²⁵ This also includes an obligation to monitor risks.

Electronic communications providers are also required to observe the same general security obligations.⁸²⁶ These include risk monitoring throughout the provision of the service. Providers are, amongst others, required to take all necessary measures, including preventive measures, in order to ensure the integrity of their networks for the purposes of ensuring continuity, and to ensure the availability of public telephone services in the event the network breaks down or in the case of force majeure.⁸²⁷

Nonetheless, both regulations remain very general, and leave the practical details to standards.

For payment services providers, the general requirement to comply with common and secure open communication standards was already referred to part 2.3.6. So was the obligation to implement a security policy. Payment services providers are required to conduct a detailed analysis of all operational and security risks connected to their services and must provide the EBA every year with an updated risk assessment.⁸²⁸ They must take measures to protect users against fraud and illegal use of personal data, in accordance with standards established in accordance with the PSD2 Directive.⁸²⁹ Payment services must take appropriate risk mitigating measures and control mechanisms to ensure that all operational and security risks are prevented and/or mitigated.⁸³⁰ Likewise, the Commission Delegated Regulation (EU) 2018/389 lays down specific requirements for security, which include preventive monitoring and detection.

For investment firms, the governance framework included a repeatedly evaluated governance framework and several preventive measures, including a kill switch. These were already discussed in part 2.3.6.

The proposed Regulation on digital operational resilience for the financial sector promises to introduce more detailed monitoring obligations for all financial entities, and not just those whose activities are limited to algorithmic trading. The Regulation explicitly mentions the obligation to introduce an ICT risk-management framework and describes its components in a detailed manner. One such component is in Articles 8 and 9 of the Proposal. Financial entities are obligated to continuously monitor and control the functioning of the ICT systems and tools and must minimise the impact of such risks.⁸³¹ Financial entities will be obligated to have in place mechanisms to

⁸²³ See Art. 13§2 CIC Act.

⁸²⁴ Art. 11 et seq. Proposed Directive on the Resilience of Critical Entities.

⁸²⁵ Art. 19 eIDAS Regulation.

⁸²⁶ Art. 114§1 Electronic Communications Act.

⁸²⁷ Art. 114§3 Electronic Communications Act.

⁸²⁸ Art. 50 Payment Services Act.

⁸²⁹ Art. 51 Payment Services Act.

⁸³⁰ Art. 53 Payment Services Act.

⁸³¹ Art. 8 Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector.

promptly detect anomalous activities, including ICT network performance issues and ICT-related accidents.⁸³² These must be regularly tested.

2.4.3. Corrective and Reporting Measures With Regard to AI-systems

As mentioned above, prevention alone is not enough: sometimes, risks do materialise. In such events, it is necessary to ensure that the measures are corrected. This can be done either by taking the necessary measures to prevent the risk from occurring, as well as to notify the user and/or the authorities of any incidents that may happen. These obligations will be discussed accordingly in the order used in the previous parts. This implies that general contract and tort law will first be examined (part A) after which product safety will be discussed (part B). Notification requirements and corrective obligations on the basis of data protection law are also analysed (part C). Non-sectoral (part D) as well as sectoral cybersecurity rules (part E) will be examined.

A. General Contract and Tort Law

By its nature, the obligation to notify the user is not based on general contract law. In the event that a lack of security of the product is considered a defect, the buyer has the right to either obtain the right to return the defective good against return of the price or to have the price refunded. Repairs are traditionally excluded.⁸³³ In any case, the seller is then liable for damages. In the event the seller is of good faith, the seller is only liable for the price; in the event the seller is considered to have known the defect, he has to repay all damage the buyer has suffered as a result of the defect. Professional salesmen are considered to have known any defect, unless if they can prove that the defect could not possibly be detected.⁸³⁴ This places the seller of an AI-system at a disadvantage. At the same time, as previously mentioned, the problem is mostly the difficulty of the anteriority of the defect in the event that the defect arises as a result of adaptations to an algorithm by an autonomous system.

In the event of a sale to consumers, Article 1649*quinquies* CC gives to the consumer the explicit right to request for repairs, unless if said repair would be impossible or out of proportion. In the event of AI-system, the problem is that learned systems are often difficult to unlearn something. It therefore remains to be seen how these provisions will be applied in the future.

In the event of a contract for the supply of a service, the restoration duties completely depend on the contract itself or the (to judges often unknown) rules of the art. As mentioned above, such rules of the art may consist of what is specified in a standard, it being understood that standards only constitute the bare minimum, and do not take into account the specific circumstances of every instance. Therefore, standards only create a presumption of compliance (and thus against liability); this presumption can be rebutted.⁸³⁵

As previously mentioned, the seller will be required to provide updates to ensure that digital content or any consumer good that contains digital content, during the time that the service is provided or during the time that the consumer may reasonably expect. In the event the seller does not comply with any of said obligations, liability is to ensue.⁸³⁶ The consumer shall have the right to have the digital content, digital service or the good placed in conformity, unless if this would be

⁸³² Art. 9 Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector.

⁸³³ Art. 1644 CCL; B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht, o.c.*, p. 345-347.

⁸³⁴ Art. 1644 CCL; B. TILLEMANN, *Deel 2.A. Koop – Gevolgen van de koop in Beginselen van Belgisch privaatrecht, o.c.*, p. 372-377.

⁸³⁵ F. BURSENS, *Handboek Aannemingsrecht*, Mortsel, Intersentia, 2019, 107-109.

⁸³⁶ Art. 11 Directive 2019/770; Art. 10 Directive 2019/771.

impossible or if it would impose disproportionate costs.⁸³⁷ This will provide a step in the right direction, but – as previously mentioned – external legislation will remain important.

B. Product Safety Legislation

In the event that a risk materialises, all producers of products are required to adopt commensurate measures to avoid any risks that may materialise, including withdrawal from the market, warning consumers or a recall of the product from consumers. It is clarified under the General Product Safety Directive that the recall of a product should be taken as a last resort, when other measures fail.⁸³⁸ Distributors are likewise obligated to cooperate with such actions.

There is little guidance regarding how such a measure should be organised, which is in line with the New Legislative Framework as well: as risks change, regulations should specify the bare minimum, whereas the guidance is to be taken from either standards or from the actors themselves. The Commission provides some guidance in the form of the Corrective Action Guide.⁸³⁹ Note that in the event of a recall, the consumers must also be informed as soon as possible of any defects that may arise.

Producers and distributors are also required to inform the Central Notice Point for Producers once they know, or should have known, that a product that they marketed provides risks that are incompatible with the general safety requirements or any decision taken by the government in this regard. They must at least provide information which allows to identify the product, the risk, to trace the product and the steps to prevent risks.⁸⁴⁰ If asked, producers and distributors must cooperate with the authorities to avoid risk.⁸⁴¹

As previously mentioned: in order to comply with this obligation, logging by design will likely be a necessary – although not a sufficient – condition. This has been recognised by the Expert Group on Liability and New Technologies.⁸⁴² Similarly, notices must be sent to the Rapid Alert System provided at EU level.⁸⁴³ Moreover, it must again be noted that the measures mainly focus on the recall of physical products. In the field of software, other measures are usually required, such as software patches. This is e.g. required in the new Digital Content Directive.⁸⁴⁴

In order to comply with the abovementioned regulation, it may be necessary to ensure that AI-systems contain exact logging systems that explain the changes to humans. In doing so, it must be ensured that the logging is actually trackable by humans. Therefore, using an automated monitoring system or pre-established systems may become necessary to ensure that the abovementioned obligations are properly observed.

⁸³⁷ Art. 14 Directive 2019/770; Art. 13 Directive 2019/771.

⁸³⁸ Article 5.1 paragraph 3, 2nd sentence Directive 2001/95 on general product safety: *“Recall shall take place as a last resort, where other measures would not suffice to prevent the risks involved, in instances where the producers consider it necessary or where they are obliged to do so further to a measure taken by the competent authority.”*

⁸³⁹ PROSAFE, “Consumer Product Safety in Europe – Corrective Action Guide”, November 2011, available at https://www.prosafe.org/images/Documents/EMARS/Corrective_Action_Guide_Final-published.pdf. The steps for a recall project are also provided in S. VAN CAMP, “Productveiligheid en product recall”, *TBH* 2010, p. 472-482.

⁸⁴⁰ Art. IX§4 CEL.

⁸⁴¹ Art. IX§5 CEL.

⁸⁴² Expert Group on Liability and New Technologies, “Liability for Artificial Intelligence and Other Emerging Technologies”, o.c., recommendation 9.

⁸⁴³ See https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/index_en.htm.

⁸⁴⁴ Art. 8.2 Directive 2019/770 ; see above 2.3.2.

C. Notification Requirements and Corrective Obligations on the Basis of Data Protection Law

As previously mentioned, Article 32 GDPR requires that the controllers for data protection operations take appropriate measures to ensure a level of security which is appropriate to the risks involved. Such appropriate measures also include the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.⁸⁴⁵ Again, the exact contents of such measures are wholly dependent on the choices of the controller and/or of applicable standards and/or codes of conduct, which may act as proof of compliance.⁸⁴⁶

In the event of a personal data breach, the controller is also required to notify said breach without delay and, where feasible, not later than 72 hours after having become aware of it, to the data protection authority, unless if the personal data breach is unlikely to result in a risk to the rights and freedom of natural persons.⁸⁴⁷ As a result of the security obligation enshrined within Article 32 GDPR, the time during which the controller may be unaware may be reduced, especially in the event that automated detection mechanisms are present.⁸⁴⁸ To determine the risk depends on the circumstances of the breach, the data at hand and the ease with which individuals may be identified in the breach. Guidance is offered by ENISA in the form of its Recommendations for a methodology of the assessment of severity of personal data breaches.⁸⁴⁹ Given the age of these recommendations, updates may be required, as less data could lead to higher risks due to AI-based analyses. Recently, the EDPB gave new guidelines with examples, which are only general and do not focus on AI specifically.⁸⁵⁰

The notification must contain at the very least the elements to determine the exact risk and the name and contact details of the data protection officer from whom more information can be obtained. Similarly, the measures that were already taken to address the personal data breach must be provided.⁸⁵¹ Any personal data breaches must also be documented to permit the supervisory authority to verify compliance.⁸⁵²

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Article 34 GDPR requires the controller to communicate the personal data breach not only to the data protection authority, but also to the data subject, unless if a) the controller has implemented appropriate technical measures, b) the controller has taken subsequent measures to mitigate the risk and c) it would involve disproportionate effort.⁸⁵³ On 19 January 2021, the European Data Protection Board published guidelines with examples regarding the notification of data breaches.⁸⁵⁴

⁸⁴⁵ Art. 32.1(c) GDPR.

⁸⁴⁶ Art. 32.3 GDPR.

⁸⁴⁷ Art. 33.1. GDPR.

⁸⁴⁸ ARTICLE 29 WORKING PARTY, *Guidelines on Personal Data Breach Notification under Regulation 2016/679*, WP250, 10-13.

⁸⁴⁹ ENISA, "Recommendations for a methodology of the assessment of the severity of personal data breaches", December 2013, available at <https://www.enisa.europa.eu/publications/dbn-severity>.

⁸⁵⁰ European Data Protection Board, "Guidelines 01/2021 on Examples regarding Data Breach Notification", 19 January 2021, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

⁸⁵¹ Art. 33.3 GDPR.

⁸⁵² Art.33.5. GDPR.

⁸⁵³ Art. 34 GDPR.

⁸⁵⁴ European Data Protection Board, *Guidelines 01/2021 on Examples regarding Data Breach Notification*, 19 January 2021, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

D. Non-Sectoral Cybersecurity Laws

Under the NIS Act, both the operators of essential services and digital services providers are required to notify any incidents with a significant impact without delay. OES are even required to provide such notification in the event that they only have partial information on the significance of the incident, whereas digital service providers are only required to notify any incidents if they have the necessary information in order to determine the severity of the incident.⁸⁵⁵ In both cases, the notification takes place through an online notification platform to the national Computer Security Incident Response Team (CSIRT), as well as to the General Direction Crisis Centre of the Ministry of Internal Affairs.⁸⁵⁶ The national CSIRT will also inform the CSIRTs of other EU member states, in order to prevent further damage caused by the incident.

Regarding corrective measures, these form part of the appropriate and necessary measures as provided under the NIS Act. These were previously discussed in part 2.3.5.

Under the NIS 2 Proposal, the abovementioned notification requirements are retained and elaborated upon for essential and important entities as defined in Article 20 of the Proposal. Both essential and important entities must notify, without undue delay, the competent authorities or the CSIRT of any incident having a significant impact on the provision of their services.⁸⁵⁷ Where appropriate, the users will also be notified. Guidance is also given as to what determines the significance of the incident. For the purpose of notification, it is also explicitly stated that essential and important entities must provide an initial notification which indicates whether or not the incident was caused by unlawful or malicious action, an intermediate report and a final report indicating the type of threat that likely triggered the incident and applied and ongoing measures. Conversely, national authorities will be required to provide guidance on the measures to take in response to the notification within 24 hours as well. In light of the increased speed and scale of attacks caused by AI-systems, this is more than welcome.⁸⁵⁸

Critical infrastructure entities are required to implement risk mitigation measures as a part of their OSP. This was already discussed in part 2.3.5. Without prejudice to legal or regulatory provisions indicating otherwise, any sector is required to inform the *Communicatie- en informatiedienst van het arrondissement* (SICAD), the sectoral agency and the General Direction Crisis Centre of any event that may threaten a critical infrastructure. This is either done through the infrastructure directly or through the federal police.⁸⁵⁹

Under the Proposed Directive on the Resilience of Critical Entities, Member States are obliged to ensure that critical entities take measures to ensure their resilience, including measures which are necessary to resist and mitigate the consequences of incidents, as well as to recover from incidents.⁸⁶⁰ Similarly, critical entities will continue to be required to notify to the competent authorities any incidents and information to understand its nature, cause and possible consequences.⁸⁶¹

E. Sectoral Cybersecurity Laws

For trust service providers, aside from the general obligation to take any risk-appropriate measures, qualified and non-qualified trust service providers are also required to notify their

⁸⁵⁵ Art. 24 and 35 NIS Act. See the Royal Decree of 12 July 2019 implementing the NIS Act, MB 18 July 2019.

⁸⁵⁶ Art. 60 NIS Act.

⁸⁵⁷ Art. 20 NIS 2 Proposal.

⁸⁵⁸ Art. 20 NIS 2 Proposal.

⁸⁵⁹ Art. 14 CIC Act.

⁸⁶⁰ Art. 11.1, (b)-(d) Proposed Directive on the Operational Resilience of Critical Entities.

⁸⁶¹ Art. 13 Proposed Directive on the Operational Resilience of Critical Entities.

supervisory body and, where applicable, other relevant bodies, of any breach of security or loss of integrity that has a significant impact on the trust service provided or the personal data maintained therein. Where the breach of security or the loss of integrity is likely to adversely affect a natural or legal person, said person shall also be informed.⁸⁶²

Providers of electronic communications services are required to take all risk-appropriate measures in order to ensure the integrity of their networks to ensure business continuity, as well as the availability of their service in the event the network breaks down or in the event of force majeure.⁸⁶³ In the event there is a specific risk of security, the providers of public electronic communications services are required to immediately inform their subscribers and the Belgian Institute for Postal Services and Telecommunications (BIPT) of any such risks and the means to counteract it, with an estimate of the costs. Moreover, the BIPT must also be informed of any security breach or any loss of integrity with an important impact on the exploitation of networks and services.⁸⁶⁴ For the latter, a decision of 14 December 2017 provides specific thresholds to help assessments as well as the practical modalities.⁸⁶⁵

For the notification of such personal data breaches, a specific delay of 24 hours within which the provider must notify all personal data breaches to the competent authority, i.e. the Data Protection Authority.⁸⁶⁶ In the event the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall, in addition to the notification to competent authorities, notify the subscriber or individual of the breach, unless if appropriate technological protection measures have been taken and applied to the data by the security breach, which must render the data unintelligible to any person who is not authorised to access it.⁸⁶⁷ Data shall be considered unintelligible if it has been securely encrypted with a standardised algorithm, the key used to decrypt the data has not been compromised in any security breach, and the key used to decrypt the data has been generated so that it cannot be ascertained by any available means by any person not authorised to access the key, or if it has been replaced by its hashed value calculated with a standardised cryptographic hash function; the key used to hash the data not being compromised in any breach.⁸⁶⁸ It must be noted that the prescription of these measures is highly specific. This creates the question whether these measures are capable to withstand AI-based attacks, which – as previously mentioned in part 2.2.2. – increase the availability of sophisticated tools for cyberattacks.

Payment services providers are required to ensure that security incidents and safety-related complaints from customers are monitored, dealt with and followed up on. In the event of a large operational or security incident, the payment institutions must inform the National Bank of

⁸⁶² Art. 19 Regulation 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, *OJ L 257/73*.

⁸⁶³ Art. 114 Electronic Communications Act.

⁸⁶⁴ Art. 114/1 Electronic Communications Act.

⁸⁶⁵ Decision of the Council of the BIPT of 14 December 2017 regarding the thresholds and modalities for notification of security incidents with the electronic communications sector, available at https://www.bipt.be/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/e1f8fe1aebb0d26e6f328867f9d5a57554a22da6/Besluit_14-12-2017_kennisgeving_veiligheidsincidenten-NL.PDF.

⁸⁶⁶ Art. 2 Commission Regulation (EU) 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, *OJ.L. 173*, p. 2-8.

⁸⁶⁷ Art. 3-4 Commission Regulation (EU) 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, *OJ.L. 173*, p. 2-8.

⁸⁶⁸ Art. 4.2. Commission Regulation 611/2013.

Belgium without undue delay. After receipt of said data, the relevant data are communicated to the European Central Bank.⁸⁶⁹

The security obligations of investment firms have been discussed in part 2.3.6.

In the proposed Regulation for Digital Operational Resilience in the Financial Sector, financial entities will all be required to put in place a dedicated and comprehensive ICT Business Continuity Policy as an integral part of the operational business continuity policy. This provides detailed requirements on the components, requiring systems that record all incidents, ensure the continuity of critical functions and quickly, appropriately and effectively must respond to all ICT-related incidents to limit damage, activate containment measures, etc. Backup policies are also required, as there is a requirement to have in place capabilities and staff, suited to their size, business and risk profiles to gather information on vulnerabilities and cyber threats, ICT-related incidents, and to analyse their impact, as well as to provide post-factum review.⁸⁷⁰

2.5. Using AI to Support (Cyber)security

As mentioned above in part 2.2.1., AI-systems can be used both to cause harm to individuals or systems and to support security and safety. Lawmakers are acting accordingly. For example, in its Joint Communication on its Cybersecurity for the Digital Decade, the European Commission underlines that AI can be used to support practitioners. Based on this, it proposed to build a network of Security Operations Centres, which allows efficient sharing of intelligence. Support will be made through state-of-the-art AI.⁸⁷¹

Indeed, AI detection tools could increase the speed and scale at which entities defend themselves. Their effectiveness makes it useful, if not recommended or – in the future – even the standard to comply with one's cyber-defence obligations. Nonetheless, there are potential risks thereto. This part attempts to provide a short overview of a few selected issues. First, we will discuss what rules could obligate entities to use AI for intrusion detection systems (part 2.5.1.). Second, we will discuss the limits the GDPR poses on all forms of automated decision-making (part 2.5.2.). Third, we will provide an overview of some other rules and rights that may be impacted by intrusion detection systems (part 2.5.3.). Finally, we will discuss one paradox, i.e. that the use of AI-based technology for the purpose of cybersecurity creates a risk of dependence on technology to defend technology (part 2.5.4.).

2.5.1. Can the Use of Automated Intrusion Detection Systems for Safety and/or Security be Mandated by Current Rules?

As mentioned in parts 2.3. and 2.4. several rules impose several actors to take measures to ensure that harm does not occur. General tort law requires all of us to take adequate care to avoid harm. Product safety law requires all producers to ensure that only safe products are marketed, and that those risks are managed by commensurate risks. Controllers of data processing operations and several digital entities are required by the GDPR to take risk-preventing measures. The same goes for the operators of essential services, digital service providers, electronic communications providers, ...

⁸⁶⁹ Art. 53 Payment Services Act. The standards for such notification are established in Commission Implementing Regulation (EU) 2019/410 of 29 November 2018 laying down implementing technical standards with regard to the structure of the information to be notified, in the field of payment services, by competent authorities to the European Banking Authority, OJ.L. 73, p. 20-83.

⁸⁷⁰ See Art. 9-14 Proposed Regulation on Digital Operational Resilience in the Financial Sector.

⁸⁷¹ European Commission, "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade", JOIN(2020)18 final, p. 6-7.

The abovementioned rules all provide a formulation of a general duty of care, adapted to the risks posed and with regard to the resources made available to them. For example, Recital 83 GDPR clarifies that the technical and organisational measures required by Article 32 GDPR should ensure an appropriate level of security, taking into account the state of the art and the costs of implementation in relation to the risks. This means that, as automated intrusion detection tools are being introduced, they will be required to be used. Likewise, it may very well be possible that, in order to discharge oneself from contract or tort liability, the use of AI-based detection tools may become the standard of care.⁸⁷²

In part this will depend on standardisation. At the time of writing, there appears to be no standard requiring the use of automated tools. Nonetheless, this may change in the future. Moreover, even without clear standardisation frameworks, certain types of practices may become a *de facto* standard and therefore still be required. For example, Article IX.3 §2 defines several bases for the presumption of safety which can be used, including the state of the art.

More specifically, we see that the use of (automated) intrusion detection systems has already been implemented. For example, Commission Regulation 2018/151 requires digital service providers to implement detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous systems.⁸⁷³ Especially in financial regulation, we see the use of automated intrusion detection tools implemented. For investment firms engaged in algorithmic trading, investment firms are required to monitor all trading activity for signs of potential market manipulation, for which the investment firm must maintain an automated surveillance system.⁸⁷⁴ In the Proposed Regulation on the Digital Operational Resilience for the Financial Sector, financial entities will also be obliged to have in place mechanisms to promptly detect anomalous activities, which by their wording are clearly meant to be automatic.⁸⁷⁵

While the use of AI-based tools is not always specifically required, it is often not prohibited and sometimes implied. For example, one can use automated detection tools as a part of customer due diligence on the basis of anti-money laundering law.⁸⁷⁶ This can create questions for some providers of ICT services, namely those which also qualify as information society services. Following Article 15 of the E-commerce Directive, Article XII.20 clarifies that internet service providers (ISPs) are not required to conduct any general monitoring to research the information on their networks; they are only required to notify the authorities and to take action to remove access once they have become aware of it.⁸⁷⁷ However, the use of AI to ensure that specific monitoring obligations are complied with more effectively is not prohibited and indeed encouraged. For example, in *Eva Glawischnig-Pieczczek v. Facebook*, the CJEU ruled that it is possible to order the removal of terms which are equivalent in meaning, precisely because of the availability of automated filtering tools.⁸⁷⁸ Similarly, in the proposed Digital Services Act, voluntary investigations are explicitly permitted – and thus even encouraged.⁸⁷⁹ The new Directive on Copyright in the Single Market, large online-content sharing service providers are also liable for acts of communication to the public if they do not engage in best efforts to ensure the

⁸⁷² This has been argued for US tort law by, *inter alia*, R. ABBOTT, “The Reasonable Computer: Disrupting the Paradigm of Tort Liability”, *Geo. Wash. L. Rev.* 2018, 86 *et seq.*

⁸⁷³ Art. 2.2 Commission Regulation 2018/151.

⁸⁷⁴ Art. 13 Commission Regulation 2017/589.

⁸⁷⁵ Art. 9 Proposed Regulation on the Digital Operational Resilience in the Financial Sector.

⁸⁷⁶ See Book II, Titles 3 and 4 Act of 18 September 2017 on the prevention of money laundering and terrorist financing and to limit the use of cash, BS 6 October 2017; see Chapter II Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the use of money laundering, or terrorist financing, as reviewed by Directive 2018/843 of 30 May 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849&qid=1617112059850>.

⁸⁷⁷ Art. 15 E-commerce Directive; Art. XII.20 CEL.

⁸⁷⁸ CJEU, 3 October 2019, *Eva Glawischnig-Pieczczek v. Facebook Ireland Limited*, ECLI:EU:C:2019:821, §46.

⁸⁷⁹ Art. 6 DSA Proposal.

unavailability of specific works and other subject matter, as well as to prevent their future uploads.⁸⁸⁰ The use of AI could be necessary to achieve that goal.

2.5.2. Limits on Automated Decision-Making on the Basis of the GDPR

Like any autonomous agent, intrusion detection software makes decisions autonomously. Therefore, limitations on automated decision-making which are inscribed in rules can limit the technology's potential. One prime obstacle therefore is the GDPR and its rules on automated decision-making. Whenever an AI-system is processing personal data – which it often does to support its decisions – the GDPR applies.⁸⁸¹

“Profiling” is defined in the GDPR as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.⁸⁸² Therefore, it must always relate to an evaluation of a person's e.g. behaviour, such as fraudulent payments. Mere classification will not lead to profiling, however.⁸⁸³

Profiling occurs when there are three components:

- The processing is automated;
- The processing is related to personal data;
- The purpose of profiling is to evaluate aspects of a natural person.

“Automated decision-making” has a broader scope and relates to all decisions which are made without human intervention. Therefore, most – if not all – AI-systems use automated decision-making. This stems from the definition of AI.⁸⁸⁴

Like all forms of personal data processing, an intrusion detection system will, therefore, have to comply with all applicable data protection principles, as well as have a legal basis.⁸⁸⁵ This legal basis can be provided on the basis of contractual necessity or on the basis of a legal obligation (for example, in order to comply with Regulation 2017/589). The legal basis of legitimate interest may provide a basis for security-based operations, but depending on the impact, this is unlikely. The latter depends on factors such as the level of detail of a profile, the comprehensiveness of the profile, the impact of the profile and the safeguards maintained.⁸⁸⁶

It must be noted that the requirements regarding legal basis are supplemented with the requirements for special categories of data. It must be noted that, depending on the data which is processed by the intrusion detection system, sensitive data may be derived. For example, payment information may betray political affiliation of a certain individual. Given the possibilities that AI has to offer in this regard, this category will become especially risky, given the fact that a recommender

⁸⁸⁰ Art. 17.4 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

⁸⁸¹ See T.GILS, E. WAUTERS, B. BENICHO, J. DE BRUYNE and P. VALCKE, *Artificiële intelligentie en gegevensbescherming: een verkennende gids*, o.c., p. 97 et seq.

⁸⁸² Art. 4(11) GDPR.

⁸⁸³ ARTICLE 29 WORKING PARTY, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, 3 October 2017, p. 7.

⁸⁸⁴ High-Level Expert Group on Artificial Intelligence, “A definition of AI: Main capabilities and scientific disciplines”, o.c., p. 9: “Artificial Intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that... deciding the best action(s) to take to achieve the given goal.

⁸⁸⁵ Art. 5-6 GDPR.

⁸⁸⁶ ARTICLE 29 WORKING PARTY, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, o.c., p. 11.

system was capable of detecting the pregnancy of a teenage girl based on her purchasing behaviour.⁸⁸⁷

Moreover, before the collection of data, the data subject has the right to receive information about the existence of automated decision-making, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.⁸⁸⁸ “Meaningful logic” means that the controller should find simple ways to tell the data subject about the rationale behind and the criteria of the systems, but not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm.⁸⁸⁹

Under Article 22 GDPR, the data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly affects him or her. The definition of the right to objection carries within it two limitations. First, Article 22 GDPR does not apply in the event the decision is not made solely by humans. Therefore, if one allows human intervention, so long as it is meaningful (i.e., one in which the human can still consider all the relevant data), then Article 22 GDPR does not apply.⁸⁹⁰ This creates an obstacle for the speed and scale of such defence tools when used by private entities. Second, Article 22 GDPR does not apply in the event that the decision does not produce legal (or equivalent effects). Examples include an automatic refusal of an online credit application or e-recruiting practices without human intervention. Exclusion is nonetheless an indicator of effects of such severity.⁸⁹¹ Therefore, some intrusion detection tools could result in decisions that are made that result in automated decision-making, giving the data subject a right to object.

Even in the event there is automated decision-making, Article 22.2 GDPR provides three exceptions under which automated decision-making with significant effects is still allowed. The first is if said processing is necessary for entering into, or performance of, a contract.⁸⁹² The third is in the event that the data subject has given his/her explicit consent.⁸⁹³ The second is if Union or Member State law allows it which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interest.⁸⁹⁴ One may, for example, think of the legal obligation to conduct analyses of market manipulation in financial regulation (see parts 2.3.6. and 2.4.3 section E). Also note that the processing of sensitive data is prohibited, unless in the event of the data subject's consent or in the context of medicine and suitable measures to protect the data subject's rights and freedoms and legitimate interests are in place. This can create problems, as AI-systems can – even unwillingly – detect such data from seemingly innocuous datasets.⁸⁹⁵ The “Target” example shows this clearly.⁸⁹⁶ This should therefore be addressed in the design of the process by adhering to data protection by design and data protection by default (see 2.3.4.).

⁸⁸⁷ K. HILL, “How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did”, *Forbes*, 16 February 2012, <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>.

⁸⁸⁸ Art. 13.2(f) and 14.2(g) GDPR.

⁸⁸⁹ ARTICLE 29 WORKING PARTY, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, 3 October 2017, p. 25.

⁸⁹⁰ Art. 22 GDPR; see ARTICLE 29 WORKING PARTY, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, o.c., p. 20-21.

⁸⁹¹ *Ibid.*, p. 21-22.

⁸⁹² Art. 22.2(a) GDPR.

⁸⁹³ Art. 22.2(c) GDPR.

⁸⁹⁴ Art. 22.2(b) GDPR.

⁸⁹⁵ Art. 22.4 GDPR.

⁸⁹⁶ K. HILL, “How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did”, *Forbes*, 16 February 2012, <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>.

Given the severe impact of automated decision-making, it should come as no surprise that automated decision-making which systematically and extensively profiles individuals based on profiling and produces legal effects requires a DPIA to be made, by virtue of Article 35.3 GDPR.

2.5.3. Automated Intrusion Detection and Other Human Rights (Examples): Non-Discrimination, Due Process and Freedom of Expression

The use of automated intrusion detection systems also creates risks of infringements with other rights. Especially their data-driven and opaque nature have led to concerns of fundamental rights. These will be discussed cursorily.

Since the *Gender Shades* report from MIT, J. BUOLAMWINI et al. proved that facial recognition algorithms and gender classification systems performed more effectively (with lower false match rates) on some ethnic groups than others and some gender groups than others.⁸⁹⁷ This was caused by a lack of diverse training data, which perpetuated algorithmic bias. For any security application – be it based on facial recognition, be it based on names, be it based on behaviour – effectiveness depends on the proper application of the algorithm to all groups equally. For example, when attempting to detect passport forgeries, it is unjustified if some ethnic groups are easier to accuse than others, or just harder to accuse than others, because of their facial features.

When looking at data quality requirements in law, it must be noted that specific requirements are scant. Most laws prohibit, in highly general terms, any form of unjustified discrimination. Whether this discrimination is conducted through automated means or not does not matter. Insofar as safety and/or security is threatened by a lack of data quality, then the responsible entities are obliged to prevent or manage this risk (see parts 2.3 and 2.4). Data quality is also subject to standardisation, and may therefore become a part of a European cybersecurity certification scheme.⁸⁹⁸ However, so far, the only real requirement of data quality specific to AI-systems is to be found in the AI HLEG's Ethics Guidelines for Trustworthy AI.⁸⁹⁹ For more specific risks of algorithmic bias in itself, more action will be expected from the EU's proposed Regulation on Artificial Intelligence.

Given the opacity, it may be difficult to implement these changes. The need for logging by design and the need for explainable AI has already been mentioned. For algorithmic trading, for example, the investment firm is required to assess what parameters are still adequate, must be able to read, replay and analyse order and transaction data on an ex-post basis, in order to prevent any risks of due process violations from occurring. Post-trade controls have the same purpose.

Algorithmic decisions can also impact due process and the presumption of innocence. An automated intrusion detection system could detect an attack, but could also be used to detect market manipulation, without the possibility of contesting the system. Currently, the GDPR allows for the right of the data subject to object to automated decision-making for exactly this purpose. It must be noted that, in the event of profiling by law enforcement authorities, logs are kept for the collection, consultation, disclosure including transfers, combination and erasure.⁹⁰⁰ This also contributes to explainable AI-systems for these purposes. This allows logging by design.

⁸⁹⁷ J. BUOLAMWINI, "Gender Shades: intersectional phenotypic and demographic evaluation of face datasets and gender classifiers", MIT Thesis, 2017, available at <https://dspace.mit.edu/handle/1721.1/114068>.

⁸⁹⁸ An example may include ISO/IEC 25024

⁸⁹⁹ AI HLEG, "Ethics Guidelines for Trustworthy AI", o.c., p. 18-19.

⁹⁰⁰ Art. 56 Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (Belgian Data Protection Act).

Other risks related to security relate to freedom of speech. AI-systems can be used to detect illegal speech, such as hate speech.⁹⁰¹ Thus, the use of AI-systems may become tempting to fight yet another AI-based threat: online disinformation or any other type of opinion that the authorities do not like.⁹⁰² This could very well harm freedom of speech.⁹⁰³ The main response to this is the discussion on the Digital Services Act; therefore, this part will not go into further detail on this topic.

2.5.4. Who Will Defend the Defenders? On the Security of Autonomous Intrusion Detection Systems

A paradox is that, as AI-based intrusion detection systems become more commonplace, they make detection more efficient – which is necessary to ensure safety and security – but at the same time makes us more dependent on said technology. This spiral is somewhat unavoidable and is not specific to artificial intelligence: we have used antivirus software and firewalls to protect us from attackers before. The scale and speed of such offence and defence are increasing rapidly and likely exponentially, however. Nonetheless, the aforementioned observation necessitates that automated intrusion detection systems will have to be subjected to the utmost care and to the highest standard. At the same time, their flexibility will have to be ensured in order to keep up with ever-evolving threats. And at the same time, respect for fundamental rights must be ensured. Much is therefore to be expected from certification schemes and of the proposed Regulation on Artificial Intelligence.

2.6. Overview of the Identified Gaps

Given that technology – and with it, risks/threats and control possibilities – are constantly changing, the rules governing the safety and security of such systems must follow a strict balance. On the one hand, they need to provide sufficient guidance to give those subject to the rule some certainty on what they should do. On the other hand, the rules themselves should be as open and technology-neutral as possible.

After analysing the regulatory framework in Belgium for product safety and information security, we have made the following observations:

- Fragmentation of the regulatory framework locks us into fragmented piecemeal solutions: a first look at the regulatory framework regarding safety and security shows that the rules are highly fragmented. This is not necessarily undesirable, as specific products, services and sectors have risks that they each need to cover. At the same time, especially if the criteria of separation (no longer) qualify, lock-in must be avoided in order to ensure that the rules can adapt to new realities with them. In other words, fragmented regulations creates fragmented solutions that do not capture the full scope of the problem. This is the case when discussing the current regimes. Product safety rules only focus on physical products and therefore can miss risks that are caused by non-embedded software. Only in a few cases is this averted, as e.g. with medical devices. At the same time, the security rules focus mostly on attacks and, therefore, focus on only one risk. In order to ensure sufficient safety, technology neutrality must be covered adequately for non-embedded

⁹⁰¹ For example, Antwerp-based start-up Textgain can detect speech which belongs to Islamist hate groups. See: <https://www.textgain.com/portfolio/automatic-detection-of-online-jihadist-hate-speech/>. Textgain was, therefore, selected to establish the European Observatory of Online Hate. See: <https://www.tijd.be/ondernemen/technologie/antwerps-ai-bedrijf-leidt-europees-onderzoek-naar-online-haatspraak/10278452>.

⁹⁰² M. BRUNDAGE *et al.*, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation*, o.c., p. 47-48.

⁹⁰³ For a blogpost on this topic, see K. VRANCKAERT, “ISP Liability: How Censorship By Robots May Become the New Normal”, 25 August 2020, available at <https://www.law.kuleuven.be/citip/blog/isp-liability-how-censorship-by-robots-may-become-the-new-normal/>.

software as well. This is currently being evaluated by the EU. Belgium should support this review.

- Flexibility requires good standardisation for the design of AI-systems and risk management throughout their use: both security measures (e.g. GDPR, some sectoral regulations, NIS and the rule on critical infrastructures) and safety rules follow an approach which is highly reminiscent of the New Legislative Framework: leave the rules as open as possible, while creating a presumption of conformity by compliance with standardisation. This ensures flexibility, albeit at the cost of the possibility of guidance. All depends on the efficiency of the standardisation process. We have observed that not all standards are lost when it comes to AI-systems; similarly, we have observed that AI standards are developing at a rapid rate. At the same time, the question arises whether we wholly want techno-regulation to define what we must do to ensure the safety of AI-systems. A specific problem of standardisation is that the rules are made by who has the information. However, the rules are also written by those with a vested interest in the industry. Belgium should ensure that standardisation goes as transparently as possible, not only at the national level, but also at the European level. The same goes for access to the standards themselves: being copyrighted, most standards are only available through payment. While this is not a large problem for large business, for SMEs – which are the majority of Belgium’s businesses – the cost of buying many standards adds up quickly. Therefore, arrangements must be supported which make access to standards easier. Moreover, the standards themselves must be design in such a way that they are complied with in order to avoid loss of security due to rational ignorance of users. Guidance by regulators – including guidelines on incident reporting – can provide a flexible solution in this regard.
- Product safety: new concept of and approach to safety required. We have identified that the definition of a safe product is a product that does not cause any real physical harm. At the same time, studies are showing that digital applications, including those in the field of “emotional AI”, can cause emotional distress, decrease in cognitive performance, etc. As a result, the concept of safety may be redefined, if not in the law, then in standardisation. Moreover, constant updates now also require that safety of a product is no longer defined purely during marketing, but is defined throughout the entire lifespan of the product. So far, the legal regimes covers this, but at the very least, more guidance will come. This can arise from standardisation.
- Standardisation will carry the market and therefore merits attention: given the other observations, it speaks for itself that standardisation should be a high priority. It must also be noted that standards must be designed in such a way that the general public is capable of understanding them. Given the increased scale of potential attacks or other threats, this will become even more paramount than it already is.
- Templates in financial regulation? A large contrast can be observed between the more general regimes for safety and security and the sector-specific regimes for the financial sector. Likely because the risks are quite known and because there is already some experience with using algorithms, the regulations are much more advanced and detailed. The process is kept flexible, as the general standards are quite vague and the more specific technical standards are left to Commission Delegated Regulations. This can provide a solid source of inspiration for regimes in other sectors.

3. Data-Economy (WP 4.2.)

3.1. Introduction

As a matter of fact, the development and use of AI-systems⁹⁰⁴ require the processing of, and hence the access to, massive amounts of data.⁹⁰⁵ Therefore, this part of the study focuses on the analysis of existing legislation, recent legislative proposals and to some extent soft law regarding the legal framework for data economy in relation to AI at the Belgian and EU levels.⁹⁰⁶

Access to and use of data in relation to AI may take place on the basis of voluntary agreements or on the basis of legal obligations. In this regard, several actions were already taken, mainly at the EU level, which provided both guidance for voluntary data sharing and legal obligations for data sharing.⁹⁰⁷ Additional data sharing obligations relevant to AI might also be adopted in a near future as the European Commission recently made several proposals that will directly affect the data economy.

In the following parts, the study considers such existing and potential future legal rules, and to some extent soft law, from two different perspectives. Firstly, data sharing rules are analysed in the case where they apply with a limited range, that is to say where data sharing deals with a limited number of individuals, entities or objects, through the mechanism of data portability (part 3.2.). Secondly, data sharing rules and relevant soft law principles are examined in the case where they apply with a broader range, that is to say where data sharing applies regarding numerous individuals, entities or objects (part. 3.3.).⁹⁰⁸ Throughout this part of the study, several types of data sharing and correlative legal rules are thus identified and subject to analysis. The analysis will end with an overview of some gaps (part 3.4.).

As a preliminary remark, it should be noted that several sector-specific rules might impose further data sharing obligations than those examined below.⁹⁰⁹ For instance, such sector-specific rules may notably impose data sharing in the automotive sector,⁹¹⁰ in the electricity supply sector,⁹¹¹ in the electronic communications sector⁹¹² and in the postal sector.⁹¹³ Given the wide number of

⁹⁰⁴ In the following parts, the notion of AI should be understood as machine learning technology, as other types of AIs (such as expert systems) do not raise specific questions regarding data economy.

⁹⁰⁵ Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space", COM(2018) 232 final, 25 April 2018, p. 3; Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European strategy for data", COM(2020) 66 final, 19 February 2020, p. 2-3.

⁹⁰⁶ The study analyses Belgian laws, where such rules exist. Where no Belgian laws exist (yet), EU rules are analysed instead. At this stage, very little rules have been adopted at the Belgian level regarding the data economy. Hence, most of the rules studied hereafter come from the EU. Given the fact that legal definitions might vary depending on the legal order considered, and depending on the applicable set of rules, applicable legal definitions are provided within each chapter, section and subsection where relevant.

⁹⁰⁷ Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European strategy for data", o.c., p. 4.

⁹⁰⁸ This structure is based on T. TOMBAL, "Compulsory B2B data sharing: A tale of trade-offs", *PhD thesis research*, UNamur, 2021, to be published.

⁹⁰⁹ On such sector specific data sharing obligations, see R. FEASEY and A. DE STREEL, "Data sharing for digital markets and contestability, towards a governance framework", *Centre on Regulation in Europe Report*, September 2020, p. 44-51.

⁹¹⁰ Art. 61-66 Regulation 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, OJ L 151.

⁹¹¹ Art. 23 Directive 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity, OJ L 158.

⁹¹² Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321.

⁹¹³ Directive 97/67 of the European Parliament and of the Council of 15 December 1997 on common rules for the development of the internal market of Community postal services and the improvement of quality of service, OJ L 15/14, 2 as amended by Directive 2002/39, Regulation 1882/2003 and Directive 2008/6.

sector-specific rules that may potentially apply in this regard, and given the fact that such rules are not specific to AI, this part of the study does not analyse them. Hence, when considering data sharing within these specific sectors, attention should be paid to applicable sets of rules.⁹¹⁴

In addition, it should also be noted that other sets of rules, besides the data economy legal framework, might apply to data, and thereby have an impact on data sharing agreements or obligations. For instance, the rules of intellectual property might apply to data sharing if contents to be shared are copyrighted, part of protected databases, constitute trade secrets, etc.⁹¹⁵ Similarly, the rules of data protection and competition law might apply where, respectively, personal data are shared or anti-competitive behaviours are found to exist. Whenever it is the case, such rules apply alongside data sharing rules, and might add constraints to data sharing operations.⁹¹⁶ Hence, when considering data sharing on data protected by other bodies of law, specific attention should be paid to all applicable sets of rules.

3.2. Data Portability (B2C and B2B)

In this part, the data sharing rules that are analysed apply on data transfers regarding a limited number of individuals, entities or objects, through the mechanism of data portability, in businesses to consumers (B2C) as well as between businesses (B2B) relations. Such type of data sharing mainly pursues an objective of empowerment of individuals or entities that benefit of a right to require such data transfers.⁹¹⁷

With regard to AI and the massive amounts of data required to train and use it, such limited data transfers might prove useful when considering their cumulative effects. Indeed, AI-systems designers or operators might *ab initio* not have access to sufficient data to train or exploit such systems. The mechanism of data portability could, to some extent, provide a remedy to this issue, although it only implies data sharing regarding a limited number of individuals, entities or objects.⁹¹⁸

The following paragraphs describe the applicable sets of rules in terms of data portability regarding respectively personal (part 3.2.1.) and non-personal data (part 3.2.2.). Yet, part of the literature criticises this distinction as they consider that the delineation between personal and non-personal data is not always clear. This might lead to issues on the application of relevant legal rules.⁹¹⁹ Scholars notably point out that it might be difficult to know what set of rules should apply in the

⁹¹⁴ Additionally, several potential new sector specific data sharing rules are currently 'work in progress' at the EC, and might hence be the object of legislative proposals in a near future. In this regard, see the DGA Proposal.

⁹¹⁵ See in this regard also Chapter 2, which relates to the rules of intellectual property in relation to AI.

⁹¹⁶ R. FEASEY and A. DE STREEL, "Data sharing for digital markets and contestability, towards a governance framework", *op cit.*, p. 51-53.

⁹¹⁷ See notably I. GRAEF, T. TOMBAL and A. DE STREEL, "Limits and enablers of data sharing – An analytical framework for EU Competition, Data Protection and Consumer Law", *TILEC discussion paper*, November 2019, p. 21-22, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3494212. The authors state this objective regarding the data sharing obligations imposed within Art. 20, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, O.J. L119 and within Art. 16, Directive 2019/770. See also Article 29 Working Party, "Guidelines on the right to data portability", *WP 242rev.01*, 27 October 2017, p. 15.

⁹¹⁸ This could take place through contractual agreements based on the data portability principle, or on spontaneous data portability (e.g. a data subject that spontaneously requires to an AI developer A, to transfer his/her personal data to an AI developer B).

⁹¹⁹ See notably J. DREXL, "Data access and control in the era of connected devices", *Study on behalf of the European Consumer Organisation BEUC*, April 2018, p. 48, available at https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf, J. KRAMER, P. SENELLART and A. DE STREEL, "Making data portability more effective for the digital economy", *Centre on Regulation in Europe Report*, June 2020, p. 17.

case where several types of data are processed in which it is unclear if it is personal or non-personal data.⁹²⁰ The EC's Proposal for a Digital Markets Act will also be examined (part 3.2.3.).

3.2.1. Personal Data Portability

Regarding personal data portability, relevant rules primarily arise from data protection law, that is to say, the GDPR.⁹²¹ Thereby, the content of these rules is analysed firstly (part A.). Personal data portability may also arise from sector-specific rules. For instance, such types of requirements are contained within the Second Payment Service Directive, which are detailed in the second part (part B.).

A. Data Protection

According to the GDPR, data subjects⁹²² have the right to receive from data controllers⁹²³ all the personal data⁹²⁴ concerning them that they provided to the later "in a structured, commonly used and machine-readable format"⁹²⁵ (i.e. by a B2C process). Data subjects also "have the right to transmit those data to another controller",⁹²⁶ which allows for indirect data sharing between data controllers through the mechanism of data portability (i.e. by a B2C2B process).

Yet, this right to data portability only applies where the processing⁹²⁷ of personal data is based on data subjects' consent⁹²⁸ or on contractual grounds, and where the processing is made through automated means.⁹²⁹ In addition, when the conditions of application of this right are met, data subjects "have the right to have the personal data transmitted directly from one controller to another, where technically feasible".⁹³⁰ This implies a direct data sharing between data controllers through the mechanism of data portability (i.e. by a B2B process).

Legal scholars point to several limitations of this right to portability, which might prove relevant in relation to access to and use of data by AI-systems. Among other things, the conditions that have to be met for the right to portability to apply are criticised (i.e. processing has to be based on consent or contract, and to be carried out by automated means).⁹³¹ When data processing is based

⁹²⁰ *Ibid.* See also Communication from the European Commission to the European Parliament and the Council, "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union", COM(2019) 250 final, 29 May 2019, p. 7-11.

⁹²¹ Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, O.J. L119.

⁹²² According to Art. 4, (1) GDPR: "an identifiable natural person [, i.e. a natural person] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

⁹²³ According to Art. 4, (7) GDPR: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

⁹²⁴ According to Art. 4, (1) GDPR: "any information relating to an identified or identifiable natural person".

⁹²⁵ Art. 20, § 1 GDPR.

⁹²⁶ Art. 20, § 1 GDPR.

⁹²⁷ According to Art. 4, (2) GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

⁹²⁸ According to Art. 4 (11) GDPR: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

⁹²⁹ Art. 20, § 1 GDPR.

⁹³⁰ Art. 20, § 2 GDPR.

⁹³¹ R. FEASEY and A. DE STREEL, "Data sharing for digital markets and contestability, towards a governance framework", o.c., p. 45-46.

on other grounds, such as the legitimate interest of the data controller or performance of a legal obligation, the right to portability does not apply.⁹³²

In addition, this right only applies to data provided by a data subject to the controller. This notion includes data actively and knowingly provided by the data subject (e.g. name, address, phone number, etc.), as well as observed data provided by the data subject through the use of the controller's service or device (e.g. search history, location data, etc.). However, inferred data and derived data are not encompassed (e.g. a data subject's profile as created by a data controller, a risk assessment for a loan, etc.).⁹³³ Yet, such data might prove valuable for the training and/or use of AI-systems.

Finally, the direct transmission of personal data from one controller to another is limited to situations in which it is technically feasible.⁹³⁴ Thereby, data controllers may avoid directly transferring personal data to other controllers due to interoperability issues,⁹³⁵ which might often be the case in relation to AI.

B. Payment Services

A sector-specific application of the right to personal data portability contained within the GDPR exists in PSD2,⁹³⁶ as well as in its Belgian transposition.⁹³⁷ Due to this set of dispositions, providers of payment initiation service⁹³⁸ and providers of account information services⁹³⁹ have the right to directly receive from banks payment account⁹⁴⁰ information of users of their services, if such users have explicitly consented to it.

This constitutes a sector-specific application of the right to portability that arises from the GDPR, as "it compels the banks (original controllers) to make this direct transmission of the data subjects' personal banking information to recipient controllers"⁹⁴¹ (i.e. by a B2B process). Furthermore, this set of dispositions forces the banks to transfer (i.e. make portable) data in any case, without limiting the portability obligation to situations where it is technically feasible.⁹⁴²

Where providers of payment initiation service and providers of account information services use AI-systems to perform their tasks, such data portability obligations will undoubtedly prove useful. However, part of scholarship points at a limitation of this sector-specific right to portability, which might prove relevant in relation to access and use of data for AI. PSD2 does not provide rules on

⁹³² J. KRAMER, P. SENELLART, A. DE STREEL, "Making data portability more effective for the digital economy", *o.c.*, p. 20.

⁹³³ Article 29 Working Party, "Guidelines on the right to data portability", *o.c.*, p. 9-11. See also J. DREXL, "Data access and control in the era of connected devices", *o.c.*, p. 107-110.

⁹³⁴ B. MARTENS, A. DE STREEL, I. GRAEF, T. TOMBAL and N. DUCH-BROWN, "Business to Business data sharing: An economic and legal analysis", *Joint Research Centre Technical Report*, 2020, Working paper 2020-05, p. 40-41.

⁹³⁵ R. FEASEY and A. DE STREEL, "Data sharing for digital markets and contestability, towards a governance framework", *o.c.*, p. 46. See also M. KNOCKAERT and J.-N. COLIN, "Le droit à la portabilité des données, coup d'oeil juridique et technique", *DPO News* 2019, n°1, p. 3-5.

⁹³⁶ Art. 66, § 4, and 67, § 3, PSD2. See also European Data Protection Board, "Guidelines 06/2020 on the interplay of the Second Payment Directive and the GDPR", 15 December 2020.

⁹³⁷ Act of 19 July 2018 modifying and inserting dispositions regarding payment services within several books of the CEL, M.B., 30 July 2018. The relevant dispositions for the data portability rules at stake are Art. VII. 35 and 36 of the CEL.

⁹³⁸ According to Art. I.9, 33/11° CEL, this notion can be defined as a service that consists in initiating a payment order, at the request of the payment service user, with respect to a payment account held by another provider of payment services.

⁹³⁹ According to Art. I.9, 33/12° CEL, this notion can be defined as an online service that consists in providing consolidated information on one or more payment accounts, which are held by the payment service user, with another payment service provider or more than one other payment service provider.

⁹⁴⁰ According to Art. I.9, 8° CEL, this notion can be defined as an account which is held in the name of one or more users of payment services, and which is used in order to make payment transactions.

⁹⁴¹ I. GRAEF, T. TOMBAL, A. DE STREEL, "Limits and enablers of data sharing – An analytical framework for EU Competition, Data Protection and Consumer Law", *o.c.*, p. 19, and J. KRAMER, P. SENELLART and A. DE STREEL, "Making data portability more effective for the digital economy", *o.c.*, p. 32.

⁹⁴² *Ibid.*

the technical means that should be used by banks to provide data to providers of payment initiation services and to providers of account information services. Neither does the Belgian transposition of the Directive. Hence, each bank that has to provide data could chose to use its own technical solutions, leading to potential interoperability issues for providers of payment initiation service and providers of account information services.⁹⁴³ This might prove problematic where providers of payment initiation services and providers of account information services rely on the use of AI-systems to perform their tasks as such systems might not be able to exploit the data received from banks in diverse formats.

3.2.2. Non-Personal Data Portability

Regarding non-personal data portability, relevant obligations notably arise from Directive 2019/770 on the supply of digital content and services (Directive 2019/770).⁹⁴⁴ The study will first analyse the content of these rules (part A.). Where non-personal data is ported, Regulation 2018/1807 on the free flow of non-personal data (Regulation 2018/1807)⁹⁴⁵ provides information on the manner in which such porting should be made (part B.).

A. Supply of Digital Content or Service

According to Directive 2019/770, in the event of the termination of a contract between a trader⁹⁴⁶ and a consumer,⁹⁴⁷ where the object of the contract was a digital content⁹⁴⁸ or service⁹⁴⁹, the consumer has the right to recover the non-personal data that he/she created or provided through the content or service (i.e. by a B2C process).⁹⁵⁰ More specifically, “the trader shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader”.⁹⁵¹

Furthermore, the consumer is entitled to “retrieve that digital content free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format”.⁹⁵²

This right to non-personal data portability, however, is limited in some cases, that is to say where data (i) is of no use, out of the digital content or service provided by the trader; (ii) solely relates to consumer’s activity when using the digital content or service; or (iii) has been aggregated with

⁹⁴³ T. TOMBAL and M. KNOCKAERT, “Quels droits sur les données?” in H. JACQUEMIN and B. MICHAUX (ed.), *Actualités en droit du numérique*, Anthémis, Limal, 2019, p. 80.

⁹⁴⁴ Directive 2019/770.

⁹⁴⁵ Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, O.J., L 303.

⁹⁴⁶ According to Art. 2, (5) Directive 2019/770: “any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person’s name or on that person’s behalf, for purposes relating to that person’s trade, business, craft, or profession, in relation to contracts covered by this Directive”.

⁹⁴⁷ According to Art. 2, (6) Directive 2019/770: “any natural person who, in relation to contracts covered by this Directive, is acting for purposes which are outside that person’s trade, business, craft, or profession”.

⁹⁴⁸ According to Art. 2, (1) Directive 2019/770: “data which are produced and supplied in digital form”.

⁹⁴⁹ According to Art. 2, (2) Directive 2019/770: “(a) a service that allows the consumer to create, process, store or access data in digital form; or (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service”.

⁹⁵⁰ This right to data portability is limited to non-personal data only, as the GDPR’s right to data portability is to apply for personal data. On the interplay between both sets of rules, see J. KRAMER, P. SENELLART and A. DE STREEL, “Making data portability more effective for the digital economy”, o.c., p. 25.

⁹⁵¹ Art. 16, § 4, al. 1 Directive 2019/770.

⁹⁵² Art. 16, § 4, al. 2 Directive 2019/770.

other data by the trader, and the trader is not able to disaggregate it without disproportionate efforts.⁹⁵³ In such cases, consumers are not entitled to retrieve their non-personal data.

Part of the literature on this topic criticises the limitation of beneficiaries of this right, as it does not allow for a direct transmission of the data ported to other traders. This critique may prove relevant in relation to access and use of data for AI as traders might thereby not be able to directly process consumers non-personal data with their AI-systems. However, as consumers should retrieve their non-personal data in a commonly used and machine readable format, Directive 2019/770 allows in this case for an indirect data sharing between traders, through the mechanism of data portability (i.e. by a B2C2B process).⁹⁵⁴

B. Free Flow of Non-Personal Data

Regulation 2018/1807 does not encompass material rules regarding non-personal data sharing as such. However, it states that the Commission should contribute to the development of EU codes of conduct, which should facilitate the porting of non-personal data.⁹⁵⁵

More precisely, the Regulation states that such codes of conduct should allow data to be ported, in B2B relations, “in a structured, commonly used and machine-readable format including open standard formats where required or requested by the service provider receiving the data”.⁹⁵⁶ The objective here is notably to facilitate the switch between cloud service providers for users^{957,958}

Since the adoption of the Regulation in 2018, two draft codes of conduct were adopted by the ‘Switching cloud service providers and Porting Data’ (SWIPO) Working Group.⁹⁵⁹ Both codes of conduct should be assessed by the EC by the end of 2022.⁹⁶⁰

3.2.3. European Commission’s Proposal for a Digital Markets Act

Within its DMA Proposal, the EC proposed a new data portability obligation. As this legislative proposal is still at its first stage, and will likely be modified through the legislative process, the following paragraphs only provide a short overview of the relevant proposed substantive rule, rather than a detailed analysis.

⁹⁵³ Art. 16, § 4, al. 1 Directive 2019/770.

⁹⁵⁴ I. GRAEF, T. TOMBAL and A. DE STREEL, “Limits and enablers of data sharing – An analytical framework for EU Competition, Data Protection and Consumer Law”, *o.c.*, p. 20, R. FEASEY and A. DE STREEL, “Data sharing for digital markets and contestability, towards a governance framework”, *o.c.*, p. 47. See also European Commission, Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634, 9 December 2015, p. 22.

⁹⁵⁵ According to Art. 3, (1) Regulation 2018/1708: “data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679”.

⁹⁵⁶ Art. 6, § 1 Regulation 2018/1708.

⁹⁵⁷ According to Art. 1, (7) Regulation 2018/1708: “a natural or legal person, including a public authority or a body governed by public law, using or requesting a data processing service”.

⁹⁵⁸ B. MARTENS, A. DE STREEL, I. GRAEF, T. TOMBAL and N. DUCH-BROWN, “Business to Business data sharing: An economic and legal analysis”, *o.c.*, p. 43.

⁹⁵⁹ On this matter, see R. FEASEY and A. DE STREEL, “Data sharing for digital markets and contestability, towards a governance framework”, *o.c.*, p. 48, and J. KRAMER, P. SENELLART and A. DE STREEL, “Making data portability more effective for the digital economy”, *o.c.*, p. 26-27.

⁹⁶⁰ Art. 8, § 1, (c), Regulation 2018/1708.

The proposal of the EC states that “[i]n respect of each of its core platform services⁹⁶¹ [...], a gatekeeper⁹⁶² shall: [...] provide effective portability of data⁹⁶³ generated through the activity of a business user⁹⁶⁴ or end user⁹⁶⁵ and shall, in particular, provide tools for end users to facilitate the exercise of data portability, in line with Regulation EU 2016/679, including by the provision of continuous and real-time access”.⁹⁶⁶

It is interesting to note that this provision does not differentiate on basis of the nature of the data that is the object of the portability requirement (i.e. personal or non-personal data). Hence, it would likely apply to both personal and non-personal data. Regarding access to and use of data for AI, this evolution could prove useful, as the same regulatory regime would then apply without making a difference of treatment based on the nature of the data, where the conditions of application of the provision are met. It might also be interesting to note that the proposal refers to the provision of continuous and real-time data portability, while these elements are not provided for within the wording of Article 20 of the GDPR, nor within Article 16 of Directive 2019/770. In relation to AI, this evolution might also be useful as it would increase the amount of data that can potentially be shared through this portability mechanism.

3.3. Data Sharing Regarding Numerous Individuals, Entities or Objects (G2B, B2G and B2B)

In this part, the study focuses on large-scale data sharing between the public sector and businesses (G2B) (part 3.3.1.), between businesses and the public sector (B2G) (part 3.3.2.) and within a B2B context (part 3.3.3.).⁹⁶⁷ Such types of data sharing mainly pursue economic objectives such as enhancing innovation,⁹⁶⁸ allowing for the contestability of markets,⁹⁶⁹ etc. With regard to AI, these types of data sharing are particularly relevant as they may allow for direct access to and use of massive amounts of data.

⁹⁶¹ According to Art. 3, § 7 DMA Proposal: “For each gatekeeper [...] the Commission shall [...] list the relevant core platform services that are provided within that same undertaking and which individually serve as an important gateway for business users to reach end users”. According to Art. 2, (2) DMA Proposal, core platform services can be “(a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communication services; (f) operating systems; (g) cloud computing services; or (h) advertising services [...]”.

⁹⁶² According to Art. 3, § 1 DMA Proposal: “A provider of core platform services shall be designated as gatekeeper if: (a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future”.

⁹⁶³ According to Art. 2, (19) DMA Proposal: “any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording”.

⁹⁶⁴ According to Art. 2, (17) DMA Proposal: “any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users”.

⁹⁶⁵ According to Art. 2, (16) DMA Proposal: “any natural or legal person using core platform services other than as a business user”.

⁹⁶⁶ Art. 6, § 1, (h) DMA Proposal.

⁹⁶⁷ The rules described hereafter notably encompass data cooperatives.

⁹⁶⁸ In this regard, see notably Recitals 8 and 9, Directive 2019/2024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), O.J., L 172.

⁹⁶⁹ In this regard, see notably Recital 3 and 54, DMA Proposal.

3.3.1. G2B Data Sharing

Regarding G2B data sharing, Directive 2019/1024 on open data and the re-use of public sector information (Open Data Directive – ODD)⁹⁷⁰ creates a legal framework that imposes the obligation upon public sector bodies to allow for the re-use of their data by private entities under certain conditions. Such rules are analysed (part A.). The same Directive also contains rules regarding voluntary B2G data sharing for specific types of public entities such as public undertakings and libraries or museums in some cases. These rules are also examined alongside with the EC's proposal for a Regulation on European data governance (proposal Data Governance Act – DGA),⁹⁷¹ which also contains rules on voluntary data sharing in G2B relations (part B.).

A. Compulsory Sharing of Public Sector Information

The Open Data Directive imposes the obligation upon public sector bodies⁹⁷² to make several types of documents⁹⁷³ re-usable⁹⁷⁴ by private entities,⁹⁷⁵ for both commercial and non-commercial purposes.⁹⁷⁶ Public libraries, museums and archives are covered by the notion of public sector bodies, and hence have to respect the rules contained within the Directive, at least as long as they do not hold intellectual property rights on documents to be re-used.⁹⁷⁷

⁹⁷⁰ According to Art. 17 ODD, Member States have to transpose the Directive by 17 July 2021 at the latest. As this Directive is a recast, the rules contained within its previous versions were already transposed in Belgian law, notably through the following Acts: Loi du 4 mai 2016 relative à la réutilisation des informations du secteur public, *M.B.*, 3 June 2016; Decreet van 12 juni 2015 tot wijziging van het decreet van 27 april 2007 betreffende het hergebruik van overheidsinformatie en het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, *M.B.*, 30 June 2015; Ordonnance du 27 octobre 2016 visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *M.B.*, 10 November 2016; Dekret vom 29 juni 2015 zur Abänderung des Dekrets vom 18. Dezember 2006 über die Weiterverwendung öffentlicher Dokumente, *M.B.*, 17 July 2015; Décret du 12 juillet 2017 relatif à la réutilisation des informations du secteur public et visant à l'établissement d'une politique de données ouvertes (« Open Data »), *M.B.*, 7 August 2017; Décret conjoint du 12 juillet 2017 relatif à la réutilisation des informations du secteur public et visant à l'établissement d'une politique de données ouvertes (« Open Data ») pour les matières visées à l'article 138 de la Constitution, *M.B.*, 7 August 2017; Décret conjoint de la Région wallonne et de la Communauté française du 19 juillet 2017 relatif à la réutilisation des informations du secteur public et visant à l'établissement d'une politique de données ouvertes (« Open Data »), *M.B.*, 13 September 2017.

⁹⁷¹ European Commission, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final, 25 November 2020.

⁹⁷² According to Art. 2, (1) ODD: “the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law”. According to Art. 2, (2), ODD, “bodies governed by public law” means bodies that have all of the following characteristics: (a) they are established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; (b) they have legal personality; and (c) they are financed, for the most part by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law”.

⁹⁷³ According to Art. 2, (6) ODD: “(a) any content whatever its medium (paper or electronic form or as a sound, visual or audio-visual recording); or (b) any part of such content”.

⁹⁷⁴ According to Art. 2, (11) ODD: “re-use means the use by persons or legal entities of documents held by: (a) public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced, except for the exchange of documents between public sector bodies purely in pursuit of their public tasks; or (b) public undertakings, for commercial or non-commercial purposes other than for the initial purpose of providing services in the general interest for which the documents were produced, except for the exchange of documents between public undertakings and public sector bodies purely in pursuit of the public tasks of public sector bodies”.

⁹⁷⁵ Or by public sector bodies having commercial activities, which fall out of their public tasks, according to Art. 11, ODD.

⁹⁷⁶ Art. 3, § 1 ODD.

⁹⁷⁷ Art. 3, § 2 ODD. See also T. TOMBAL and M. KNOCKAERT, “Quels droits sur les données?”, *o.c.*, p. 83.

Documents to which the ODD applies encompass all existing documents held by public sector bodies and research data,⁹⁷⁸ but excludes among others: (i) documents which are supplied outside the scope of the public task of the public sector bodies; (ii) documents for which third parties hold intellectual property rights; (iii) sensitive data on the protection of national security, statistical confidentiality, or commercial confidentiality, which are excluded from national access regimes on that basis; (iv) documents that include personal data, and which are excluded from national access regime on that basis; and (v) documents held by cultural establishments other than libraries, museums and archives.⁹⁷⁹ In addition to these exclusions from its scope of application, the Directive states that its dispositions are without prejudice to data protection law⁹⁸⁰ and to intellectual property rights.⁹⁸¹ Hence, where such protections apply to data that is the object of data sharing, all applicable sets of rules have to be taken into account and respected.⁹⁸²

When the scope of application of the Directive is met, public sector bodies are required to make their documents available “in any pre-existing format or language and, where possible and appropriate, by electronic means, in formats that are open,⁹⁸³ machine-readable,⁹⁸⁴ accessible, findable and re-usable, together with their metadata”.⁹⁸⁵

In addition, specific rules are provided for dynamic data⁹⁸⁶ and high-value datasets.⁹⁸⁷ Regarding dynamic data, the Directive makes clear that it should be made available for re-use immediately after its collection through Application Programming Interfaces (APIs) and as bulk download.⁹⁸⁸ High-value datasets are required to be made available in machine-readable formats through APIs and as bulk download.⁹⁸⁹

Where the Directive requires public sector data to be available for re-use, such re-use has to be free of charge⁹⁹⁰ and to be provided without imposing conditions on the re-use.⁹⁹¹ Yet, in some cases, it might be necessary for public sector bodies to impose conditions on the re-use of its data,

⁹⁷⁸ According to Art. 2, (9) ODD: “documents in a digital form, other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results”. According to Art. 10, § 2, ODD, the re-use of such documents is however limited to cases where research is publicly funded, and insofar as “researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository”.

⁹⁷⁹ Art. 1 ODD. For a full list of documents excluded from the scope of application of the Directive, see Art. 1, § 2, ODD.

⁹⁸⁰ Art. 1, § 4 ODD.

⁹⁸¹ Art. 1, § 5 ODD.

⁹⁸² In this regard, the EC recently released a proposal that could be tackling some of the issues related to the application of intellectual property rights and data protection law, in the case of B2G data sharing. See part 4.3.1. section B.

⁹⁸³ According to Art. 2, (14) ODD: “a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents”.

⁹⁸⁴ According to Art. 2, (13) ODD: “a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure”.

⁹⁸⁵ Art. 5, § 1 ODD. See also M. KNOCKAERT, “La réutilisation des informations du secteur public: l’open data et les organismes publics”, *J.T.* 2018, n°6739, p. 617-618.

⁹⁸⁶ According to Art. 2, (8) ODD: “documents in a digital form, subject to frequent or real-time updates, in particular because of their volatility or rapid obsolescence; data generated by sensors are typically considered to be dynamic data”.

⁹⁸⁷ According to Art. 2, (10), ODD: “documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and of the number of potential beneficiaries of the value-added services and applications based on those datasets”.

⁹⁸⁸ Art. 5, § 5 ODD.

⁹⁸⁹ Art. 5, § 6 ODD.

⁹⁹⁰ Art. 6, § 1 and 6, ODD. However, Art. 6, § 1, al. 2, ODD, states that “the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymization of personal data and measures taken to protect commercially confidential information may be allowed”. The same Article also allows for several other exceptions to the ‘free of charge’ principle, within its § 2, notably for public libraries, museums, and archives.

⁹⁹¹ Art. 8, § 1, al. 1 ODD.

notably to preserve public interest objectives.⁹⁹² In such cases, conditions set out for re-use have to be objective, proportionate, non-discriminatory and justified on the basis of the pursued public interest.⁹⁹³ Conditions respecting these principles may notably be imposed through standard licences.

Finally, the Directive requires Member States to “make practical arrangements facilitating the search for documents available for re-use, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and portal sites that are linked to the asset lists”.⁹⁹⁴

Some scholars highlight the fact that at this stage, the Open Data Directive is the most comprehensive existing data governance framework in EU law.⁹⁹⁵ Regarding AI-systems, this legal framework seems to allow for a broad access to, and use of, public sector data in B2G relations where its scope is met. Yet, it does not apply to several types of data that may be relevant for training and using AI such as documents for which third parties hold intellectual property rights (e.g. copyright, database *sui generis* right, etc.).⁹⁹⁶

B. Voluntary Sharing of Public Sector Information

The Open Data Directive also provides a legal framework for voluntary G2B data sharing. Public undertakings,⁹⁹⁷ as well as public libraries, museums and archives where they hold intellectual property rights on documents, may decide whether they allow the re-use of their documents or not.⁹⁹⁸ If they decide to allow such re-use of their documents, public libraries, museums, and archives holding intellectual property rights, as well as public undertakings, have to respect the obligations set out in the Directive as described above (see part 4.3.1 section A). Yet, public undertakings, libraries, museums and archives may charge entities which re-use their data above the marginal costs incurred “for the reproduction, provision and dissemination of documents as well as for anonymization of personal data and measures taken to protect commercially confidential information”, while public sector bodies may not do so (see part 3.3.1 section A).⁹⁹⁹

Here as well, the dispositions of the Directive are without prejudice to data protection law¹⁰⁰⁰ and to intellectual property rights.¹⁰⁰¹ Hence, where such protections apply to data, in the case of a data sharing operation, all applicable sets of rules have to be respected too.

⁹⁹² According to Recital 31, ODD, examples of public interest objectives notably include public health and safety. According to Recital 44, ODD, conditions imposed to re-users of public sector data might include “conditions [...] dealing with issues such as liability, the protection of personal data, the proper use of documents, guaranteeing non-alteration and the acknowledgement of source”.

⁹⁹³ Art. 8, § 1, al. 1, ODD. In Belgium, case law arose on this matter, and the ‘Banque Carrefour des Entreprises’ (hereafter BCE) has been condemned by the Brussels Court of Appeal for imposing to re-users, to share their own data with the BCE in exchange of BCE’s data. For further details, see Brussels, 19 November 2009, R.D.C.-T.B.H., 2009/8, p. 835-844.

⁹⁹⁴ Art. 9, § 1 ODD.

⁹⁹⁵ R. FEASEY and A. DE STREEL, “Data sharing for digital markets and contestability, towards a governance framework”, *op cit.*, p. 48.

⁹⁹⁶ See in this regard Chapter 2, which relates to the rules of intellectual property in relation to AI.

⁹⁹⁷ According to Art. 2, (3) ODD: “any undertaking active in the areas [(i) defined in Directive 2014/25/EU; (ii) acting as public service operators pursuant to Article 2 of Regulation (EC) No 1370/2007; (iii) acting as air carriers fulfilling public service obligations pursuant to Article 16 of Regulation (EC) No 1008/2008; or (iv) acting as Community ship-owners fulfilling public service obligations pursuant to Article 4 of Regulation (EEC) No 3577/92] over which the public sector bodies may exercise directly or indirectly a dominant influence by virtue of their ownership of it, their financial participation therein, or the rules which govern it. A dominant influence on the part of the public sector bodies shall be presumed in any of the following cases in which those bodies, directly or indirectly: (a) hold the majority of the undertaking’s subscribed capital; (b) control the majority of the votes attaching to shares issued by the undertaking; (c) can appoint more than half of the undertaking’s administrative, management or supervisory body”.

⁹⁹⁸ Art. 3, § 2 ODD.

⁹⁹⁹ Art. 6, § 2 ODD.

¹⁰⁰⁰ Art. 1, § 4 ODD.

¹⁰⁰¹ Art. 1, § 5 ODD.

Regarding access to and use of data for AI, this type of voluntary G2B data sharing might prove useful. Yet, the price that may be charged by public undertakings, libraries, museums and archives for the re-use of their data might potentially cause issues as the Directive does not provide for ceilings or limits for such prices.

In addition to the rules contained within the Open Data Directive, new requirements regarding G2B voluntary data sharing might arise in a near future. That is because the EC recently published its DGA Proposal.¹⁰⁰² As this legislative proposal is still at its first stage, and will most likely be modified at some point through the legislative process, the following paragraphs only provide a short overview of the relevant proposed substantive rules.

The proposed Act should in principle complement the Open Data Directive framework because its objective is notably to facilitate a higher level of public sector data sharing across the EU,¹⁰⁰³ while it does not intend to “create any obligation on public sector bodies to allow re-use of data”.¹⁰⁰⁴ Regarding its scope of application, the proposal aims to apply to data¹⁰⁰⁵ held by public sector bodies¹⁰⁰⁶, which are protected on the basis of (i) commercial confidentiality; (ii) statistical confidentiality; (iii) third parties intellectual property rights; or (iv) data protection.¹⁰⁰⁷ Several types of data are excluded from its scope of application, such as data held by public undertakings, by cultural and educational establishments or documents which are supplied outside the scope of the public task of the public sector bodies.¹⁰⁰⁸

Where its scope of application is met, the proposal sets out the conditions that public sector bodies may impose for the re-use of public sector data. Such conditions should be “non-discriminatory, proportionate and objectively justified with regard to categories of data and purposes of re-use and the nature of the data for which re-use is allowed”.¹⁰⁰⁹ Among other things, the proposed Act states that “[p]ublic sector bodies may impose an obligation to re-use only pre-processed data where such pre-processing aims to anonymize or pseudonymise personal data or delete commercially confidential information, including trade secrets”.¹⁰¹⁰

In addition, according to the proposal, “[p]ublic sector bodies may impose obligations (a) to access and re-use the data within a secure processing environment provided and controlled by the public sector; (b) to access and re-use the data within the physical premises in which the secure processing environment is located, if remote access cannot be allowed without jeopardising the rights and interests of third parties”.¹⁰¹¹

¹⁰⁰² European Commission, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final, 25 November 2020 (hereafter proposal Data Governance Act).

¹⁰⁰³ European Commission, “Impact assessment report accompanying the document Proposal for a Regulation of the Parliament and of the Council on European data governance (Data Governance Act)”, SWD(2020) 295 final, 25 November 2020, p. 19.

¹⁰⁰⁴ Art. 3, § 3, DGA Proposal.

¹⁰⁰⁵ According to Art. 2, (1) DGA Proposal: “any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording”.

¹⁰⁰⁶ According to Art. 2, (11) DGA Proposal: “the State, regional or local authorities, bodies governed by public law or associations formed by one or more such authorities or one or more such bodies governed by public law”. According to Art. 2, (12) DGA Proposal: “‘bodies governed by public law’ means bodies that have the following characteristics: (a) they are established for the specific purpose of meeting needs in the general interest, and do not have an industrial or commercial character; (b) they have legal personality; (c) they are financed, for the most part, by the State, regional or local authorities, or by other bodies governed by public law; or are subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities, or by other bodies governed by public law”.

¹⁰⁰⁷ Art. 3, § 1 DGA Proposal.

¹⁰⁰⁸ Art. 3, § 2 DGA Proposal.

¹⁰⁰⁹ Art. 5, § 2 DGA Proposal.

¹⁰¹⁰ Art. 5, § 3 DGA Proposal.

¹⁰¹¹ Art. 5, § 4 DGA Proposal.

Furthermore, in cases where the re-use of data is not possible on the basis of conditions detailed in the previous paragraphs, public sector bodies might have to support re-users in the process of trying to obtain data subjects' consent for the processing of their personal data and/or permission from legal entities for the processing of data that could jeopardise their interests.¹⁰¹²

Regarding third party intellectual property rights bearing on public sector information, the proposal does not set out conditions that could be applied by public sector bodies for allowing the re-use, but merely provides that such re-use "shall only be allowed in compliance with intellectual property rights".¹⁰¹³ Similarly, where public sector data is considered confidential, the proposal does not set out the conditions that should be applied by public sector bodies to allow its re-use, but only states that "the public sector bodies shall ensure that the confidential information is not disclosed as a result of the re-use".¹⁰¹⁴

Finally, the proposed Act provides information on the prices that may be charged by public sector bodies to allow the re-use of its data. According to the proposal, fees should be non-discriminatory, proportionate and objectively justified.¹⁰¹⁵ Hence, they should be derived from the costs incurred by public sector bodies to process the requests for re-use.¹⁰¹⁶

In terms of access to and use of data for AI, this type of voluntary G2B data sharing might also prove useful. The proposal might bring clarity on the way in which public sector bodies may allow for the re-use of public data that is out of the scope of the Open Data Directive. This is undoubtedly positive. Yet, this proposal does impose compulsory data sharing for the types of data that it applies to. Hence, it might have a limited impact on the development and use of AI-systems.

3.3.2. B2G Data Sharing

Regarding access to and use of data for AI in B2G relations, it should be noted that B2G data sharing for AI-applications is notably considered to allow for enhancing public decision-making, and defining better public policies and actions.¹⁰¹⁷ For instance, the EC considers that B2G data sharing can enhance public decision-making in areas such as urban planning, road safety, traffic management, environmental protection, market monitoring or consumer protection.¹⁰¹⁸ Yet, the legal framework is, at this stage, not composed of any binding rule. However, a few soft law instruments have been issued at the EU level. They will first be analysed in the following paragraphs (part A.). In addition, the EC's Data Governance Act Proposal contains several dispositions that may prove relevant when considering B2G data sharing. These provisions will be briefly examined as well (part B.).

¹⁰¹² Art. 5, § 6 DGA Proposal.

¹⁰¹³ Art. 5, § 7 DGA Proposal.

¹⁰¹⁴ Art. 5, § 8 DGA Proposal.

¹⁰¹⁵ Art. 6, § 2 DGA Proposal.

¹⁰¹⁶ Art. 6, § 5 DGA Proposal.

¹⁰¹⁷ Yet, this type of B2G data sharing does not only concern general interest applications, as there are not any binding rules that exist yet for B2G data sharing. Hence, B2G data sharing could potentially survene for any legally accepted purpose at this stage.

¹⁰¹⁸ See Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space", *o.c.*, p. 12.

A. Soft Law

In 2018, in its communication “Towards a common European data space”, the EC detailed six key principles to provide guidance on and support for the supply of private sector data to the public sector.¹⁰¹⁹ These soft law principles are the following:¹⁰²⁰

- Proportionality in the use of private sector data

Requests for the supply of private sector data, under preferential conditions, made by public bodies should be justified by demonstrable public interest.¹⁰²¹ In addition, the cost and effort required for the supply of such data by the public sector should be proportionate regarding the expected public benefits.

- Purpose limitation

The purposes and duration for which the private sector data are to be used should be clearly defined and limited within B2G contractual agreements. Public sector should provide guarantees that private data are not used for other unrelated purposes, such as administrative or judicial procedures.

- ‘Do no harm’

The re-use of private data by public bodies should be made in a manner that prevents to cause harm to the legitimate interests of private entities who share their data. This notably means that trade secrets and commercially sensitive information should not be disclosed through the re-use. Additionally, B2G data sharing should not prevent private entities to monetise the data they hold regarding other interested parties.

- Conditions for data re-use

The conditions set out in B2G agreements for the re-use of private data should provide public sector bodies with a preferential treatment regarding other customers of such data, as the public re-use of private data pursues public interests. This should notably be reflected in the prices charged to public sector bodies for the re-use of data.

- Mitigate limitations of private sector data

Private companies when providing public sector bodies with their data should offer support to assess the quality of the data provided regarding the purposes for which the data are re-used by public sector bodies. This requirement notably aims to avoid selection bias as private data might have been collected for other purposes than those pursued by public bodies, and hence might not necessarily be fully fit for the public purposes at stake.

- Transparency and societal participation

Some information regarding B2G data sharing agreements should be made publicly available such as information on the parties to the agreements or the objectives pursued by the data sharing.

Despite the issuance of these soft law principles, the EC noted in its Communication “A European Strategy for Data” of 2020 that “[t]here is currently not enough private sector data available for

¹⁰¹⁹ Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Towards a common European data space”, o.c., p. 13.

¹⁰²⁰ *Ibid.*, p. 13-14.

¹⁰²¹ In this regard, the Communication notably states that “[d]ata held by companies, such as telecoms operators, online platforms, car manufacturers, retailers or social media is highly relevant in this context. Its use can, for example, lead to a more targeted response to epidemics, better urban planning, improved road safety and traffic management, as well as better environmental protection, market monitoring or consumer protection” (p. 12).

use by the public sector [...]”.¹⁰²² Based on this finding, the EC requested a High Level Expert Group to provide recommendations to increase B2G data sharing.¹⁰²³

In its report, the High Level Expert Group provided recommendations within three main areas. Firstly, the report proposes to improve the governance of B2G data sharing across the EU, notably by putting in place national governance structures or by creating a recognised function called “data stewards”.¹⁰²⁴ Secondly, the report contains recommendations on transparency, citizen engagement and ethics. This notably includes making B2G data sharing more citizen-centric, establishing ethical guidelines or investing in education on B2G data sharing.¹⁰²⁵ Thirdly, the High Level Expert Group proposes to create operational models, structures and technical tools for B2G data sharing. This consists, among other things, in creating incentives for companies to share their data or providing support at the EU level for the development of technical infrastructures for B2G data sharing.¹⁰²⁶

Regarding access to and use of data for AI, such soft law principles and recommendations seem *prima facie* relevant and useful. However, the lack of binding rules and a comprehensive legal framework might cause legal uncertainty and/or discourage private undertakings to share their data with public sector bodies for the purpose of training and using AI.

B. European Commission’s Proposal for a Data Governance Act

In addition to the soft law principles and recommendations the B2G data sharing legal framework might include binding rules in a near future as well. That is because the EC recently issued its DGA Proposal.

Indeed, several of the provisions contained in the Act may prove relevant for B2G data sharing, as it intends to create a set of rules for data altruism¹⁰²⁷ and for data altruism organisations. Yet, as this legislative proposal is still at its first stage, and will probably be modified through the legislative process, the following paragraphs only provide a short overview of the proposed rules.

According to the proposal, organisations (i) that are legal entities constituted to meet objectives of general interest;¹⁰²⁸ (ii) which operate on a non-profit basis; and (iii) which perform its data altruism activities through a structure legally independent from other activities it undertakes, qualify as data altruism organisations.¹⁰²⁹ When such legal qualification is met, organisations may be registered as such within a register of recognised data altruism organisations.¹⁰³⁰ To pursue their objectives of general interest, such private organisations might notably share the data that they collect with public sector bodies, through B2G data sharing. The proposal seeks to impose a few obligations to data altruism organisations, notably through transparency requirements,¹⁰³¹ and

¹⁰²² Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “A European Strategy for Data”, o.c., p. 7.

¹⁰²³ *Ibid.*, p. 7-8.

¹⁰²⁴ High Level Expert Group, *Towards a European Strategy on Business to Government data sharing for the public interest*, Publications Office of the European Union, Luxembourg, 2020, p. 37-41.

¹⁰²⁵ *Ibid.*, p. 54-58.

¹⁰²⁶ *Ibid.*, p. 67-70.

¹⁰²⁷ According to Art. 2, (10) DGA Proposal.: “the consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services”.

¹⁰²⁸ According to Recital 35 DGA Proposal.: “[purposes of general interest] include healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics or improving the provision of public services. Support to scientific research, including for example technological development and demonstration, fundamental research, applied research and privately funded research, should be considered as well purposes of general interest”.

¹⁰²⁹ Art. 16 DGA Proposal.

¹⁰³⁰ Art. 15 DGA Proposal.

¹⁰³¹ Art. 18 DGA Proposal.

through measures designed to safeguard the rights and interests of data subjects and entities that agree to share their data under data altruism schemes.¹⁰³²

In terms of transparency requirements, the proposal requires registered data altruism organisations to transmit to national authorities records containing among other things (i) information on the activities of the organisations; (ii) a description of the manners in which general interest purposes have been pursued by the organisations, with the data collected; (iii) a summary of the results obtained through the use of the data; and (iv) information on the revenues of the organisations, specifically where such revenues resulted from allowing access to data collected.¹⁰³³

In relation to safeguard measures, the proposal provides that data altruism organisations should notably “inform data holders: [...] about the purposes of general interest for which it permits the processing of their data by a data user in an easy-to-understand manner [...]”.¹⁰³⁴ Data altruism organisations should also take measures to “ensure that the data is not be used for other purposes than those of general interest for which it permits the processing”.¹⁰³⁵

This proposal specifically aims at providing access to, and use of, data for AI, which should be welcomed, as it states that “[t]his [proposal for a] Regulation aims at contributing to the emergence of pools of data made available on the basis of data altruism that have a sufficient size in order to enable data analytics and machine learning, including across borders in the Union”.¹⁰³⁶

3.3.3. B2B Data Sharing

With regard to B2B data sharing, several elements seem relevant to analyse in this part of the study, that is to say, some EU soft law principles (part A.) as well as binding existing requirements (part B.). Attention is also given to the EC’s Proposal for a Data Governance Act (part C.) and the Proposal for a DMA (part D). The provisions may, if adopted, create new B2B data sharing rules and obligations. Here again, as the legislative proposals are still at their early stage, and will probably be modified during the legislative process, the following developments only provide a short overview of the proposed rules, rather than a detailed analysis. . It is also worth noting that the European Commission plans to propose a legislative instrument specifically aimed at fostering B2B (and B2G) data sharing, in the end of 2021.

A. Soft Law

In terms of soft law, the EC in 2018 adopted five key principles for guidance on and support for B2B data sharing for non-personal data produced by Internet of Things devices in its communication “Towards a common European data space”.¹⁰³⁷ These soft law principles can be summarised as follows:

- Transparency

Contractual B2B data sharing agreements should clearly identify (i) the persons and/or entities that have access to data, (ii) the types of data at stake, and (iii) the purposes pursued while using data.

- Shared value creation

¹⁰³² Art. 19 DGA Proposal.

¹⁰³³ Art. 18, § 2 DGA Proposal.

¹⁰³⁴ Art. 19, § 1 DGA Proposal.

¹⁰³⁵ Art. 19, § 2 DGA Proposal.

¹⁰³⁶ Recital 35 DGA Proposal.

¹⁰³⁷ Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “Towards a common European data space”, o.c., p. 10.

Where data is generated as a by-product of a product or service, contractual B2B data sharing agreements should acknowledge that several parties have contributed to creating the data.

- Respect of each other's commercial interests

Both data holders and data users should have their commercial interests and secrets protected through contractual B2B data sharing agreements.

- Ensure undistorted competition

B2B data sharing agreements should not distort competition when exchanging commercially sensitive data.

- Minimised data lock-in

Where private entities offer products or services that generate data as a by-product, they should enable data portability where possible.

At that point in time, the EC already considered that additional binding rules might prove necessary to ensure B2B data sharing. Indeed, the EC stated in the same Communication that the "Commission will continue to assess whether such [...] principles and possible codes of conduct prove to be sufficient in order to maintain fair and open markets and will address the situation if necessary by taking appropriate action",¹⁰³⁸ such as sector-specific measures.

B. Transparency in B2B Data Sharing

In 2019, the EU imposed transparency requirements to online intermediation services in relation to their data sharing practices towards business users.¹⁰³⁹ According to Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services (the P2b Regulation), providers of online intermediation services¹⁰⁴⁰ have to inform their business users¹⁰⁴¹ of the conditions that they set out for the access to data provided or generated by consumers,¹⁰⁴² or by business users themselves.

More specifically, online intermediation services have to describe within their terms and conditions¹⁰⁴³ the technical and contractual access, where applicable, "of business users to any personal data or other data, or both, which business users or consumers provide for the use of the

¹⁰³⁸ Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space", o.c., p. 10.

¹⁰³⁹ Art. 9, Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, O.J. L 186.

¹⁰⁴⁰ According to Art. 2, (2) and (3), P2b Regulation: "any natural or legal person which provides, or which offers to provide" "services which meet all of the following requirements: (a) they constitute information society services within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (12); (b) they allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded; (c) they are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers".

¹⁰⁴¹ According to Art. 2, (1), P2b Regulation: "any private individual acting in a commercial or professional capacity who, or any legal person which, through online intermediation services offers goods or services to consumers for purposes relating to its trade, business, craft or profession".

¹⁰⁴² According to Art. 2, (4), P2b Regulation: "any natural person who is acting for purposes which are outside this person's trade, business, craft or profession".

¹⁰⁴³ According to Art. 2, (10), P2b Regulation: "all terms and conditions or specifications, irrespective of their name or form, which govern the contractual relationship between the provider of online intermediation services and its business users and are unilaterally determined by the provider of online intermediation services, that unilateral determination being evaluated on the basis of an overall assessment, for which the relative size of the parties concerned, the fact that a negotiation took place, or that certain provisions thereof might have been subject to such a negotiation and determined together by the relevant provider and business user is not, in itself, decisive".

online intermediation services concerned or which are generated through the provision of those services”.¹⁰⁴⁴

Although this provision does not impose B2B data sharing obligations as such, it could be useful for business users in order to acquire certainty on B2B data sharing operations that they could perform through the services of online intermediation platforms. Hence, this provision might prove relevant in relation to the access to and the use of data for AI. That is because business users using AI-systems could choose their intermediation service providers based on their data sharing policies. Business users could also be incentivised to use AI-solutions if their intermediation service providers allow for broad access to and use of AI by such business users.

C. European Commission’s Proposal for a Data Governance Act

Turning to the EC’s recent DGA Proposal, the document aims to apply to several types of data¹⁰⁴⁵ sharing¹⁰⁴⁶ services, that is to say (i) intermediation services between data holders¹⁰⁴⁷ that are legal persons, and potential data users¹⁰⁴⁸; (ii) intermediation services between data subjects that want to make their personal data available, and potential data users; and (iii) services of data cooperatives^{1049,1050}

The provision of such data sharing services should, according to the proposal, be subject to a notification regime,¹⁰⁵¹ and be subject to few conditions.¹⁰⁵² These are, among others, the following. Providers of data sharing services should (i) not use the data for which they provide their services, for other purposes than placing the data at the disposal of data users; (ii) ensure that the access to their services are fair, transparent and non-discriminatory, notably regarding prices charged; (iii) have procedures in place to prevent fraudulent and/or abusive practices from data users seeking access of their services; (iv) take measures to ensure a high level of security, for both the storage and the transmission of data; and (v) ensure data subject’s best interest, whenever personal data is at stake, notably regarding the exercise of data subjects’ rights.

In terms of the access to and the use of data for AI, this proposed legal framework for B2B data sharing might prove very useful. The proposal, if adopted, might bring clarity on the manner in which private sector undertakings may act as intermediaries for data sharing operations, which is undoubtedly positive. In addition, it should be noted that B2B data sharing might also take place through data altruism mechanisms. In this regard, the same principles as described above and the accompanying comments regarding the access to and the use of data for AI equally apply (see part 3.3.2. section B).

¹⁰⁴⁴ Art. 9, § 1, P2b Regulation.

¹⁰⁴⁵ According to Art. 2, (1) DGA Proposal: “any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording”.

¹⁰⁴⁶ According to Art. 2, (7) DGA Proposal: “the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary”.

¹⁰⁴⁷ According to Art. 2, (5) DGA Proposal: “a legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control”.

¹⁰⁴⁸ According to Art. 2, (6) DGA Proposal: “a natural or legal person who has lawful access to certain personal or non-personal data and is authorised to use that data for commercial or non-commercial purposes”.

¹⁰⁴⁹ According to Art. 9, § 1, (c) DGA Proposal: “services supporting data subjects or one-person companies or micro, small and medium-sized enterprises, who are members of the cooperative or who confer the power to the cooperative to negotiate terms and conditions for data processing before they consent, in making informed choices before consenting to data processing, and allowing for mechanisms to exchange views on data processing purposes and conditions that would best represent the interests of data subjects or legal persons”.

¹⁰⁵⁰ Art. 9, § 1 DGA Proposal.

¹⁰⁵¹ *Ibid.*

¹⁰⁵² Art. 11 DGA Proposal.

D. European Commission's Proposal for a Digital Markets Act

Within its proposal for a Regulation on contestable and fair markets in the digital sector, the EC proposed two new B2B data sharing obligations.

Firstly, the proposal states that “[i]n respect of each of its core platform services¹⁰⁵³ [...], a gatekeeper¹⁰⁵⁴ shall: [...] provide business users,¹⁰⁵⁵ or third parties authorised by a business user, free of charge, with effective, high-quality, continuous and real-time access and use of aggregated or non-aggregated data,¹⁰⁵⁶ that is provided for or generated in the context of the use of the relevant core platform services by those business users and the end users¹⁰⁵⁷ engaging with the products or services provided by those business users”.¹⁰⁵⁸

It is interesting to note that the proposal refers to the provision of continuous and real-time data sharing, bearing on both aggregated and non-aggregated data. Furthermore, the data sharing should also encompass data inferred from the use made by business users and end users of platforms core services.¹⁰⁵⁹ In terms of the access to and the use of data for AI, this proposal might prove particularly useful, as it would strongly expand the possibilities for business users to deploy such data through AI-systems.

Secondly, the proposal states that “[i]n respect of each of its core platform services [...], a gatekeeper shall: [...] provide to any third party providers of online search engines,¹⁰⁶⁰ upon their request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymization for the query, click and view data that constitutes personal data”. Although the scope of application of this proposed provision is very limited (i.e. it only targets gatekeepers in their relations to providers of online search engines), it may be very useful regarding the development and use of AI in the search engines sector.

3.4. Overview of the Identified Gaps

In this part of the study, the main question was to examine which legal rules apply (or might apply in a near future) to data sharing. This question is important because AI-systems need to access to massive amounts of data for training and development purposes. In addition, AI-systems also

¹⁰⁵³ According to Art. 3, § 7 DMA Proposal: “For each gatekeeper [...] the Commission shall [...] list the relevant core platform services that are provided within that same undertaking and which individually serve as an important gateway for business users to reach end users”. According to Art. 2, (2) DMA Proposal, core platform services can be “(a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communication services; (f) operating systems; (g) cloud computing services; or (h) advertising services [...]”.

¹⁰⁵⁴ According to Art. 3, § 1 DMA Proposal: “A provider of core platform services shall be designated as gatekeeper if: (a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future”.

¹⁰⁵⁵ According to Art. 2, (17) DMA Proposal: “any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users”.

¹⁰⁵⁶ According to Art. 2, (19) DMA Proposal: “any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording”.

¹⁰⁵⁷ According to Art. 2, (16) DMA Proposal: “any natural or legal person using core platform services other than as a business user”.

¹⁰⁵⁸ Art. 6, § 1, (i) DMA Proposal. Regarding Personal data, the same provision states that a gatekeeper shall “provide access and use only where directly connected with the use effectuated by the end user in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end user opts in to such sharing with a consent in the sense of the Regulation (EU) 2016/679”.

¹⁰⁵⁹ Recital 55 DMA Proposal.

¹⁰⁶⁰ According to Art. 2, (6) DMA Proposal: “a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found”.

require access to data to perform their tasks. Thereby, although data sharing rules are not necessarily designed to target AI-technologies, they do have an important impact on the development and use of such technologies. Hence, the focus of this part of the study was placed on the description of existing (and potential future) rules, and on their scope of application, considering in each case their implications for AI.

On the basis of the analysis conducted, the following main gaps, which have (or might have) an impact regarding AI, should be highlighted:

- The right to personal data portability provided for within Article 20 of the GDPR only applies when several conditions are met (i.e. automated processing, based on consent or contract), and does not bear on all types of personal data (i.e. inferred data and derived data are excluded). Furthermore, the direct transmission of personal data from one controller to another is limited to situations in which it is technically feasible.
- The personal data portability obligation provided for within Article 66 and 67 of Directive 2015/2366 (i.e. PSD2, transposed within Article VII. 35 and 36 of the Code of Economic Law) does not provide rules on the technical means that should be used by banks to provide data to providers of payment initiation service and to providers of account information services. This might cause interoperability issues.
- The right to non-personal data portability provided for within Article 16 of Directive 2019/770 only applies between traders and consumers. Hence, other traders may not directly receive the non-personal data from the trader under the obligation to provide data portability. It is up to consumers to provide their non-personal data to other traders.
- Directive 2019/1024 (PSI Directive - Recast) does not apply to several types of public bodies data, which might prove relevant for AI training and use, such as documents for which third parties hold intellectual property rights (e.g. copyright, database sui generis right, etc.). Furthermore, regarding voluntary data sharing schemes, the price that may be charged by public undertakings, libraries, museums and archives for the re-use of their data might potentially cause issues, as the Directive does not provide for ceilings for such prices.
- Chapter 2 of the proposal Data Governance Act does not impose compulsory data sharing for the types of data that it applies to (i.e. public data that is out of the scope of the Directive 2019/1024, PSI Directive - Recast). Hence, it might have limited impacts on the development and use of AI-systems.
- Regarding access to and use of data for AI in B2G relations, the legal framework is at this stage not composed of any binding rule. However, Chapter 3 of the proposal Data Governance Act which contains provisions regarding data altruism schemes, might to some extent tackle this gap.

4. Electronic Identification and Trust Services for Electronic Transactions (eIDAS Regulation) (WP 4.3.)

4.1. Introduction

When it comes to formalities in the digital environment, one must ask to what extent AI can be used. First, we will analyse the Regulation on Electronic identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation) (part 4.2.).¹⁰⁶¹ Then, we will look at whether that regulation contains obstacles to the use of AI by trust service providers by analysing its four main principles (part 4.3.). It will then be examined how AI can be used to detect

¹⁰⁶¹ Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, O.J. L 257/79.

fraud (part 4.4.). Finally, we will briefly explain the phenomenon of batch signing (part 4.5.). The analysis is concluded with an overview of the gaps (part 4.6.).

4.2. The eIDAS Regulation

With the rise of technologies, came the desire on the part of public actors (authorities and administrations) and private ones (businesses) to dematerialise their procedures in order to facilitate it and reduce their costs. However, there are a lot of legal formal requirements, whether required for probative or validity purposes, imposed throughout Belgian national legislations. Those requirements were envisaged in the paper-based environment. The dematerialisation can only happen if it is legally permissible to use electronic procedures and if with those numeric procedures, the legal requirements are still fulfilled. Actors must be assured that the processes used in the digital environment will have the same legal effect as the corresponding means in the paper environment.

In an open environment, there is a need to build trust in the relationships between individuals who do not necessarily know each other but need to interact. It may require the identification and authentication of the parties involved in that relation. The intervention of a trusted third party is the way chosen by the European legislator to ensure that trust. As a matter of fact, the legislator intervened to regulate the activities of those third parties who provide services to enhance the trust in those relationships. It has been done initially in the Electronic Signature Directive adopted in 1999. After that, it became clear that the electronic signature was not the only formality requiring regulation. For that reason, the European legislator replaced that directive by the eIDAS Regulation.

The eIDAS Regulation oversees electronic identification and trust services for electronic transactions in the European Union. It aims at providing a system building the trust in the use of electronic services. This Regulation establishes *inter alia* general principles, the designation of a supervisory body and an obligation to prior authorisation. The eIDAS Regulation entered into force on the 1st of July 2016. As it left some margin of manoeuvre to the Member States, the Belgian legislator adopted on the 21st of July of the same year, a Belgian law called "the Digital Act".¹⁰⁶² On this occasion, the Articles XII.24 and following were introduced in the Belgian Code of Economic Law. Those articles complement the regime established by the eIDAS Regulation and introduce a specific regime for the electronic archiving. The eIDAS Regulation provides a legal framework for the intervention of trusted third parties to encourage the dematerialisation of various legal requirements. The Regulation aims to install a climate of trust by regulating trust services and trust service providers to encourage citizen to have recourse to those services.¹⁰⁶³

4.3. The Four Guiding Principles Applied to the Use of Artificial Intelligence

In order to remove any formal obstacle to the use of electronic means in the contractual process, some guiding principles are prescribed by Article 9 of the Directive 2000/31 on electronic commerce. Principles are also consecrated by the eIDAS Regulation with regard to specific trust services (electronic signature, electronic seals, electronic time stamps and electronic registered delivery services) and to the electronic documents, and the Belgian provisions of the Digital Act (Book XII of the Belgian Code of Economic Law). The same principles could be applied to the use

¹⁰⁶² Act of 21 July 2016 "mettant en œuvre et complétant le règlement (UE) n° 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, portant insertion du titre 2 dans le livre XII « Droit de l'économie électronique » du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique", M.B., 28 September 2016, p. 67478.

¹⁰⁶³ M. FERNANDEZ GONZALEZ, "Le règlement eIDAS : l'identification électronique et les services de confiance au service du citoyen et du consommateur", *R.E.D.C.* 2016/1, p. 35.

of AI. The following paragraphs will focus on the freedom to (not) use electronics (part 4.3.1.), the functional equivalency (part 4.3.2.), technical neutrality (part 4.3.4.) and the non-discrimination principle (part 4.3.4.).

4.3.1. Freedom to (not) Use Electronics

Pursuant to Article XII.25, § 1er, of the Belgian Code of Economic Law, “in the absence of any legal provisions to the contrary, no one can be compelled to take legal action by electronic means”.¹⁰⁶⁴ The same principle could be applied to the use of AI, at least by consumers. In other words, consumers should remain free not to use AI in specific process (especially with public administration). In order to ensure a high level of legal certainty, the applicable legal framework should be amended accordingly (so that the principle shall also be applicable to AI and not only to formal requirements).

4.3.2. Functional Equivalency

From a practical point of view, every formal requirement imposed in the paper environment cannot be transposed as such in the electronic environment. For this reason, this principle of functional equivalence states that the traditional formal requirement can be done electronically only if its numeric equivalent reaches the same functions than the traditional ones. A form requirement is, therefore, not defined by a particular technical process, but by the functions that it allows to fulfil. As soon as the electronic procedures reach the same functionalities than the paper one, they are deemed equivalents. *In fine*, they can have the same effects. Such principle is expressly consecrated in Article XII.15 of the Belgian Code of Economic Law (in the context of formal requirements).

The same principle could be applied to AI. In other words, a presumption could be introduced in the applicable legal framework, stating that, when the functions expected from the legal requirements applicable to the contractual process are achieved through automated or autonomous systems (or through the use of AI in general), such technological means shall enjoy the presumption of fulfilling the legal requirements.

4.3.3. Technological Neutrality

The principle of technological neutrality means that, when the legal provisions impose the fulfilment of a particular formality, this provision should not refer to a specific technology. With the rapid evolution of technologies, if a regulation imposes a specific one, this regulation will inevitably become obsolete quickly. For that reason, the legislative rules must maintain a technological neutrality. A reference to this principle is currently made in Recitals 26 and 27 of the eIDAS Regulation.

Such principle could also be applied to AI. In order to achieve a high level of legal certainty, a specific provision should be introduced in the legal framework, stating that the legal system shall be technology-neutral and that the legal effects granted should be achievable by any technical means.

4.3.4. Non-discrimination principle

The principle of non-discrimination is prescribed by Article 9 (1) of the Directive 2000/31 on electronic commerce and by various provisions of the eIDAS Regulation. Following this principle, the legal effect or the admissibility as evidence in court cannot be denied to formalities on the sole ground that it has been completed in their electronic form (or for the only reason that the trust

¹⁰⁶⁴ Art. XII.25, §1 CEL.

service used was not qualified). In the eIDAS Regulation, this rule is expressly applied to the electronic signature, the electronic seal, the electronic time stamp, and the electronic registered delivery service.¹⁰⁶⁵ It is also applicable to the electronic document.¹⁰⁶⁶

The same principle could also be applied to the use of AI. For that purpose, a specific provision should be introduced in the legal framework to ensure that the technical means used to fulfil the legal requirements applicable to the contractual process shall not be denied legal effect and admissibility as evidence on the sole grounds that they have been made through automated or autonomous systems (or AI-applications). This new provision should also be consistent with Article 12 of the UNCITRAL Convention on the Use of Electronic Communication in International Contracts (New York, 2007).¹⁰⁶⁷

4.4. Using AI to Fight Fraud in the Context of Trust Services

When promoting the dematerialisation of procedures, there are risks that come with it. Indeed, relying on the digital equivalents of paper-based formalities comes with the risks associated with the digital environment. It is true that the issue of cybercrime arises. In a traditional context, the parties may have contacts and meet in person. What is special about trust services is that they help to create trust in the relationship between parties who do not know each other. In this configuration, the framework is more propitious to cybercrime such as fraud, identity theft, phishing, data theft, etc.

AI could be used for malicious purposes and AI-based forgery. To combat these practices, one can, in principle, have recourse to the legislation against cybercrime. Some AI-systems and algorithms are capable of intercepting operations and redirect them, alter the data, impersonate an individual (bots impersonating as humans), forge documents, etc. The widespread occurrence of malicious use of AI could have the effect of diminishing the trust in the numeric environment that the eIDAS Regulation aims to bring. As the eIDAS Regulation has been drafted for the purpose of promoting the dematerialisation, forgery and impersonations could cause injury to the trust of the citizen in the functioning of that regulation. Hence, individuals might not want to use electronic services to fulfil their legal formal obligations.

As soon as AI can be used for malicious purposes, AI can just as well also serve as an efficient technical tool to detect fraudulent actions. AI technologies can be used to counter those risks. For example, signature forgery can also happen in the paper environment with hand-made signatures. However, in the digital world, AI is able to compare and identify even the slightest differences between the original signature and the forged one. Moreover, electronic formalities are secured through asymmetric cryptography or various processes of encryption increasing the security in comparison with conventional ones.

In conclusion, the use of AI-technologies brings risks, but the same technologies can help tackle those risks at the same time. As soon as AI is its own tool to counter the danger of its use, it has countervailing effect so that the use of AI is not a problem in itself. In addition, nothing in the eIDAS Regulation constitutes an obstacle to the use of AI-systems for this purpose (being agreed that the applicable legal framework – GDPR, Code of Criminal Procedure, etc. – shall be respected).

4.5. The Phenomenon of Batch Signing

Batch signing is the technique whereby an individual can sign multiple documents compiled in a single file using one digital signature. The procedure of signing can be time consuming when there

¹⁰⁶⁵ Art. 25, § 1 ; 35, § 1 ; 41, § 1 and 43, § 1 eIDAS Regulation.

¹⁰⁶⁶ Art. 46. eIDAS Regulation.

¹⁰⁶⁷ See United Nations Convention on the Use of Electronic Communications in International Contracts, available at https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

are a lot of documents to sign. It can also be complicated if each document needing the approval of the signing person is separated and filed at different places. Batch signing is more practical as it allows to send or receive these documents as a package and sign it all at once. Artificial intelligence could be used in this context so that all or part of the process is automated. There is not any legal obstacle in the eIDAS Regulation to the use of AI in this context (the Regulation should indeed be technology neutral).

Since the batch signature is merely an application of the electronic signature, the applicable rules on electronic signature (especially in the eIDAS Regulation) shall be taken into account, being agreed that the advantages and risks of electronic signatures are exacerbated when it comes to signing batches.¹⁰⁶⁸ However, it is questionable whether the function of the signature to approve the content of the document is respected when several documents are signed all at once with only one signature. In addition, a malicious software capable of stealing or forging a signature will, in this case, directly alter the approval of the batch of documents, and not only alter a single document. It takes less effort to an ill-intentioned person to cause more detrimental consequence to the authenticity of documents.

4.6. Overview of the Identified Gaps

On the basis of the analysis conducted, the following main gaps, which have (or might have) an impact regarding AI should be highlighted. The guiding principles of (i) freedom to use electronic, (ii) non-discrimination, (iii) functional equivalence and (iv) technological neutrality (consecrated in the eIDAS Regulation, Book XII of the Belgian Code of Economic Law and Directive 2000/31/EC on electronic commerce) should also be applied to AI (in new dedicated legal provision). The introduction of such provision should indeed contribute to ensuring a higher level of legal certainty.

On the other hand, AI could be used in order to fight against fraud or to contribute to the automation of some processes (such like batch signing) in the context of trust services. There is not any obstacle in the eIDAS Regulation to the use of AI (being agreed that such use of AI, shall be compliant with GDPR or any applicable legal framework).

5. E-Commerce (WP 4.4.)

5.1. Introduction

The E-commerce Directive¹⁰⁶⁹ provides for an overarching legal regime for the functioning of online services. The importance of online services is only increasing due to the digitalisation of our society. The E-commerce Directive is a horizontal instrument that establishes some important and basic obligations upon online intermediaries.

The E-commerce Directive aims at promoting the free movement of online services in the internal market. The Directive also seeks to achieve a proper balance between different fundamental rights, especially in the context of the fight against illegal online content. The moderation of online content has a significant effect on the fundamental rights of several stakeholders concerned. On the one hand, the absence of any control over online content would open the door to abuses such as defamatory, discriminatory, racist and xenophobic content, or even content that violates intellectual property rights. On the other hand, the suppression of a legal content may constitute a violation of the content provider's freedom of expression but also of the user's right to

¹⁰⁶⁸ FORCS, "What is Batch Signing and how it can be done with Digital Signature", 26 May 2020, available at <https://www.forcs.com/en/what-is-batch-signing-and-how-it-can-be-done-with-digital-signature/>.

¹⁰⁶⁹ Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, O.J., L.178, p. 1-16.

information.¹⁰⁷⁰ In that context, the purpose is to avoid any excessive and unjustified interference with fundamental rights of individuals.

The Directive provides for a liability regime for EU intermediaries when the information they stock or transmit appears to constitute illegal content. In the context of liability, the E-commerce Directive contains four main rules: “(i) the 'country of origin' principle, which is the cornerstone of the Digital Single Market; (ii) an exemption of liability for hosting platforms which remain passive and neutral and which remove the illegal content online as soon as they are made aware of it; (iii) the prohibition of general monitoring measures to protect fundamental rights; and (iv) the promotion of self- and co-regulation as well as alternative dispute resolution mechanisms”.¹⁰⁷¹ This study focuses on the provisions concerning the liability regime for intermediaries. That is because AI is most relied upon to control online content.

The definition of illegal online content is to be found in EU and national law. Four types of contents are considered illegal throughout all EU Member States as they are defined as such by EU law, namely terrorist content, child sexual abuse material, racist and xenophobic hate speech and content infringing intellectual property rights. Beyond those four types of illegal content, “there is no EU harmonisation of the illegal content online. Thus, the same type of content may be considered illegal, legal but harmful or legal and not harmful across the Member States”.¹⁰⁷² Despite the lack of harmonisation, other content is illegal once it is criminalised by domestic law. As a general rule, what is considered illegal offline must be qualified illegal online as well.¹⁰⁷³

Moderation of content is essential to prevent content that infringes the rights of internet users. To this end, online service providers may rely on AI-applications. Although automated systems are used to detect and react to illegal online content, the use of AI comes with risks and requires the adoption of safeguards to remedy those risks. AI-tools are inherently obscure, especially when machine learning is involved. AI might be used by intermediaries to make a decision about a user's content. In this case, it is essential that the user is informed of the use of AI. In addition, AI-systems also have limitations. Firstly, the functioning of the AI-application may be defective. This is the case when the algorithm has been trained with data of insufficient quality and acquired bias. Secondly, AI-applications cannot be aware of all the specific circumstances regarding the content. This can lead to misinterpretation and errors on the part of the AI-systems.¹⁰⁷⁴

In 2000, online platforms were only in their infancy. Our society, however, is facing an unprecedented and ongoing technological evolution. As a result, the online services envisaged by the E-commerce Directive have, since its adoption, substantially evolved and the concept of platform economy has emerged.¹⁰⁷⁵ For those reasons, the content of the Directive must be adapted accordingly. The need for legislative action has resulted in a Proposal by the Commission of the DSA. The EU legal framework dealing with illegal content is a multi-layered regulatory framework. As the E-commerce Directive provides for a horizontal regime of liability for online

¹⁰⁷⁰ *Ibid.*, p. 9.

¹⁰⁷¹ A. DE STREEL et al., “Online Platforms' Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)” Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, June 2020, p. 19, available at [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU\(2020\)652718_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf).

¹⁰⁷² *Ibid.*, p. 16.

¹⁰⁷³ European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future”, COM (2020) 67 final, Brussels, 19 February 2020 available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0067&from=EN>

¹⁰⁷⁴ A. DE STREEL et al, *o.c.*, p. 59.

¹⁰⁷⁵ H. SCHULTE-NOLKE et al., “The legal framework for e-commerce in the Internal Market: State of play, remaining obstacles to the free movement of digital services and ways to improve the current situation (Study requested by the IMCO committee)”, Policy Department for Economic, Scientific and Quality of Life Policies , May 2020 available at [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652707/IPOL_STU\(2020\)652707_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652707/IPOL_STU(2020)652707_EN.pdf).

service providers in the event of illegal content, it still needs to be articulated with other sources of legislation. National legislation defines what constitutes illegal content and how to assess the attribution of liability. Moreover, other international and European legal instruments exist on the moderation of illegal online content and/or on the activities of online service providers. Those vertical legal instruments are each applicable to a specific type of content.¹⁰⁷⁶

In the following paragraphs, we will present the legislative state of play that is the E-commerce Directive. First, we will address two main principles that are of significant importance when it comes to AI, namely transparency and harmonisation (part 5.2.). Second, the scope of the E-commerce Directive will be discussed (part 5.3.). Third, we will focus on the liability exemption and the conditions to benefit from it (part 5.4.). Fourth, the study will examine the compatibility between the prohibition of the general obligation to monitor and the use of AI by intermediaries (part 5.5.). Once the study has provided some concluding considerations on the use of AI by intermediaries (part 5.6.), some gaps that need further research will be identified (part 5.7.). Throughout this overview, we will identify the shortcomings of the E-commerce Directive, while setting out the position taken by the Commission in the DSA Proposal. However, one should keep in mind that the DSA is only in a proposal state and still subject to modifications. We, therefore, confine ourselves to a brief review of its content.

5.2. Preliminary Remarks General Safeguards

5.2.1. Transparency

One fundamental safeguard to ensure that a proper balance is reached between fundamental rights is transparency. Legislation affecting fundamental rights must be clear and predictable.¹⁰⁷⁷ Transparency must also apply regarding the activities of the online services providers. Their terms of services must make users aware of the conditions of functioning of the service. In this regard, Article 5 of the E-commerce Directive provides a list of general information to be delivered by the service provider to its customers. Since the adoption of the E-commerce Directive, the legislator has made efforts to increase transparency in general. Some transparency requirements imposed by other regulatory acts are potentially applicable to AI. These obligations are (also) analysed in other parts of the study. However, there is no general obligation of transparency as such.¹⁰⁷⁸

In order to ensure the effectiveness of the current legal regime, it is necessary to deploy a mechanism to assess the intermediaries' responsiveness and compliance with the regime provided for in the legislation.¹⁰⁷⁹ The Commission promotes an obligation of transparency coupled with an obligation to issue transparency reports on the implementation of the legal framework.¹⁰⁸⁰ The

¹⁰⁷⁶ Directive 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, O.J. L. 88, p. 6-21; Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, O.J. L.335, p.1-14.; Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, O.J., L.328, p. 55-58; Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, O.J. L.130, p. 92-125; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, O.J. L.119, p. 1-88; P2b Regulation; Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, O.J. L.303, p. 69-92.

¹⁰⁷⁷ See Art. 10.2 ECHR.

¹⁰⁷⁸ Art. 9, P2b Regulation.

¹⁰⁷⁹ A. DE STREEL et al, "Online Platforms' Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)", o.c., p. 54.

¹⁰⁸⁰ Commission Recommendation on Measures to Effectively Tackle Illegal Content Online, Brussels, 1 March 2018, C(2018) 1177 final, p. 12 available at <https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online>.

DSA Proposal aims at providing an adequate level of transparency. According to the DSA Proposal, the terms of services of the providers shall include “information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear and unambiguous language and shall be publicly available in an easily accessible format”.¹⁰⁸¹ In addition to this obligation of information, the DSA imposes a reporting obligation in relation to the removal and the disabling of content considered to be illegal under the law or prohibited under the provider’s terms of services.¹⁰⁸² This obligation to issue compliance reports is included in Article 13 of the DSA proposal, which applies to all providers. The reports from providers of online platforms must also contain information about “any use made of automatic means for the purpose of content moderation, including a specification of the precise purposes, indicators of the accuracy of the automated means in fulfilling those purposes and any safeguards applied”.¹⁰⁸³

Transparency is all the more important when it comes to artificial intelligence. Considering that AI is inherently obscure, transparency is a way for individuals to better understand AI and enhance their trust in AI-applications. For that reason, the obligation of transparency must ensure that the service providers inform users when using AI, give indications on the functioning of the AI-applications and on the rights of users. By doing so, the European legislator can find inspiration in the applicable data protection legislation.¹⁰⁸⁴ To be effective, information should be given in a way ensuring that the user has easily access to it and can understand it. Finally, sanctions must be legally established for the violation of this obligation.

5.2.2. Harmonisation

The main deficiency of the E-commerce Directive stems from its implementation. The regime provided for by the Directive suffered from legal fragmentation due to the different interpretation given by the EU Member States.¹⁰⁸⁵ The initial purpose of defining a single set of rules imposed by the European legislator needs to be maintained. If those questions are left to the discretion of national legislators, the legal fragmentation risks to become even worse. The legal fragmentation hinders the development of internal market and constitutes a heavy burden on the service providers acting in different Member States. They would potentially be subject to diverging (if not contradictory) legal provisions, which undermines the establishment of the internal market and freedom of movement. The latter are particularly important in the digital environment in which physical borders lose their significance.

A single regime is also preferable for internet users. On the one hand, it must be clear for the victims of a prejudicial content what they can do about it. On the other hand, Member States must cooperate in the fight against illegal content. Moreover, the same safeguards must be enforced across the EU to ensure that there is no discrimination between individuals using the same service.¹⁰⁸⁶

AI is used by intermediaries whose activities extend across borders. In practice, the use of AI by intermediaries creates the same risks for every user irrespective of its location. As a result, the same rules must be applied to every intermediary and the same safeguards must be available to

¹⁰⁸¹ Art. 12 DSA Proposal.

¹⁰⁸² Art. 13 DSA Proposal and recital 39 DSA Proposal.

¹⁰⁸³ Art. 23.1, c) DSA Proposal.

¹⁰⁸⁴ See GDPR, art. 22.

¹⁰⁸⁵ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, Brussels, 28 September 2017, COM(2017) 555 final, p. 5 available at <https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms>.

¹⁰⁸⁶ A. DE STREEL et al, “Online Platforms’ Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)”, o.c., p. 59.

every user regardless of the location where he/she is. This explains the importance of the harmonisation of the regulatory framework.

Ideally, the updated legal framework should take the form of a regulation to ensure harmonisation by the implementation of a common regime applied similarly throughout the entire EU.¹⁰⁸⁷ If the updated legal framework is adopted in the form of a directive, there is a risk of legal fragmentation as was the case for the E-Commerce Directive. To remedy legal fragmentation, it should at least be a full harmonisation directive that leaves no margin to Member State in the transposition of the rules. In addition, its provisions must be clear enough not to allow for different interpretations. In practice, those concerns have been taken into account by the Commission. Indeed, with the DSA, “the Commission has decided to put forward a proposal for a Regulation to ensure a consistent level of protection throughout the Union and to prevent divergences hampering the free provision of the relevant services within the internal market, as well as guarantee the uniform protection of rights and uniform obligations for business and consumers across the internal market”.¹⁰⁸⁸

5.3. Scope and Intermediaries Activities

The E-commerce Directive defines what activities it is aimed at. The Directive applies irrespective of the type of illegal content. The exemption of liability regime only applies to three types of activities expressly identified: the supply of mere conduit services, caching services (part 5.3.1.) and hosting services (part 5.3.2.).

The categories of intermediaries must be defined in a technologically neutral manner in order to be futureproof, otherwise, the legislation will quickly become out-dated. Technologies become obsolete very rapidly due to the rapid evolution in the digital environment in which new evolutions constantly overhaul and replace the former ones. Besides, it allows for possible future technologies with the same functions and risks to fall under the scope of this legislation. The terminology is then based on the functional aspect of the activities performed by the intermediary and not the technology used.

The evolution of the digital environment was accompanied with the need to change or adapt the scope of the liability regime with the new types of intermediaries. These new actors are currently overlooked by the current legal framework such as “search engines, hyperlinking, domain name authorities, possibly also social media – most of these services have been included in the scope of the Directive through case law but application and interpretation differences still occur across the EU”.¹⁰⁸⁹

The existing typology designed by the E-Commerce Directive is maintained in Articles 3-5 of the DSA Proposal.

5.3.1. Mere Conduit and Caching

The “mere conduit service” consists of the “transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network”.¹⁰⁹⁰ The “caching” service is defined as “the automatic, intermediate and temporary storage of information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request”.¹⁰⁹¹ When considering

¹⁰⁸⁷ This is what has been done regarding the data protection legislation. The 1992 directive has been reformed in a 2016 Regulation to ensure the uniformity of the application of the rules. See Recital 13 GDPR.

¹⁰⁸⁸ Explanatory Memorandum of the DSA Proposal, p. 7.

¹⁰⁸⁹ See also the Legal study on the implementation of the e-commerce directive (part 2) commissioned by the FPS Economy, SMEs, Self-Employed and Energy, 3 June 2020, p. 37.

¹⁰⁹⁰ Art. 12 E-commerce Directive; Art. 3 DSA Proposal.

¹⁰⁹¹ Art. 13 E-commerce Directive; Art. 4 DSA Proposal.

the exemption of liability for these intermediaries, the European legislator envisaged them as passive technical intermediaries whose role is limited to the transmission of information.

In practice, it are mainly the hosting providers that use artificial intelligence, not the providers of mere conduit or caching services. However, if these services use artificial intelligence to detect illicit contents among the information that they transmit, the question arises whether they still benefit from the exemption. It is clear that an intermediary that obtains control over the content transmitted cannot benefit from the exemption of liability. Indeed, it can be considered that the provider would no longer qualify as mere conduit or caching service provider as described in the Directive. Moreover, Recitals 42 and 43 of the same Directive preclude such actors from benefiting from the exemption.

However, the question remains as to whether the use of AI to detect illegal content is by itself sufficient to automatically consider that the intermediary has control over the information transmitted. This question is not addressed by the directive nor the DSA Proposal¹⁰⁹² but should be dealt with in the updated legal framework.

5.3.2. Hosting Services

Article 14 of the E-Commerce Directive applies “where an information society service is provided that consists of the storage of information provided by a recipient of the service”.¹⁰⁹³ Problems especially arise with regard to Article 14.

To begin with, the problems identified concerning the E-commerce Directive are still present when it comes to Article 14. In addition to this, hosting providers often have recourse to AI to fulfil their obligations.

The legal uncertainty surrounding the concepts of hosting services is not negligible as it casts doubt on its scope. There are differing interpretations as to which intermediaries fall within the scope of Article 14 and what is actually expected of them. The legal uncertainty induces intermediaries being too prudent. In order to avoid their liability being triggered due to the presence of illegal content on their platform, providers could systematically remove any content that could be suspicious. They could indeed prefer to err on the side of caution by removing potentially illegal content that may in fact be perfectly legal. If this approach is implemented with the help of artificial intelligence, it can result in general filters screening any content available on the platform. This is undoubtedly constituting a general monitoring of content. Regarding the prohibition of general monitoring obligations of Article 15 of the EC directive, it poses immeasurable risks to fundamental rights. When content is deleted even though it is perfectly legal, the content provider suffers from a violation of his or her fundamental right of expression.

5.4. Focus on Liability Exemption for Hosting Services

It is important – yet not easy – to know exactly which intermediary falls under the definition of a hosting service provider that can benefit from the liability regime provided for by the E-commerce Directive. One reason for this is that technology is constantly changing and “new” services are continually emerging (i.e. social networks services).

It was envisaged to distinguish between platforms according to their services, size or number of users.¹⁰⁹⁴ In the sake of proportionality, it is understandable that different graduated obligations should apply to these intermediaries. This is the approach followed by the DSA Proposal, which

¹⁰⁹² Art. 3 and 4 DSA Proposal.

¹⁰⁹³ Art. 14 E-commerce Directive; Art 5 DSA Proposal.

¹⁰⁹⁴ A. DE STREEL et al, “Online Platforms’ Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)”, o.c., p. 12.

provides for general obligations applying to every platform and additional obligations imposed only on large platforms.¹⁰⁹⁵ Indeed, the obligations justified for large platforms could constitute a disproportionate burden for small platforms that lack the necessary resources and would be unable to comply with it.

The conditions for benefiting from the exemption of liability are also subject to interpretation. Article 14 of the E-Commerce Directive provides for an exemption of liability for hosting service providers for content uploaded to their platforms by users only if they can be qualified as passive (part 5.4.1) and if these hosts do not have "actual knowledge" of the illegal content (part 5.4.2.). As soon as the hosting service provider obtains this actual knowledge or is considered active, it must take action to render access to that content impossible or to delete it (part 5.4.3.)¹⁰⁹⁶

5.4.1. The Distinction Between an Active and Passive Hosting Service

The most problematic notion is the distinction between an active and a passive host. Under the interpretation given by the Court of Justice, the hosting provider is required to comply with Recital 42 of the E-commerce Directive.¹⁰⁹⁷ According to Recital 42 of the Directive, the provider must carry out an activity "of a purely technical, automatic, and passive nature".¹⁰⁹⁸ In addition to the condition explained above according to which the host must not have actual knowledge of the content to benefit from the exemption, it must not exercise any kind of control over that content.

This requirement is quite justified for providers of caching and mere-conduct services. They deliver purely technical assistance enabling the routing of information and the functioning of the internet. Their nature fully justifies this requirement of neutrality.¹⁰⁹⁹ Some argue that the recital is not intended to apply to Article 14 and that the hosting service provider does not have to stay neutral in order to benefit from the exemption of liability.¹¹⁰⁰ According to this view, a host that is not totally passive could still benefit from the exemption if the other conditions are met.

As highlighted in a previous Legal study on the implementation of the E-commerce Directive, "in the modern online environment with multi-layered platforms, the traditional hosts that play a static role solely storing content concerns a very small subset of service providers. New types of platforms often adopt a more innovative approach to attract and engage users. Moreover, they are often willing to engage in certain level of moderation in order to protect their users from illegal or harmful content. But, in such a case, they risk losing the immunity of Article 14 by being qualified as active hosts. This is a lose-lose situation".¹¹⁰¹

The Directive does not specify to what extent content moderation by the provider may cause it to lose the benefit of the exemption. From the case law, it becomes apparent that the hosting provider can up to a certain point have an influence on the content without jeopardising the

¹⁰⁹⁵ Chapter 3, Section 1, DSA applies to all providers of intermediary services. Chapter 3, Section 2 only applies to hosting services including online platforms. Chapter 3, Section 3 contains additional obligations for online platforms.

¹⁰⁹⁶ Art 14.1. E-Commerce Directive.

¹⁰⁹⁷ CJEU, *Google France Inc. v. Louis Vuitton Malletier*, Joined Cases C-236, 237 and 238/08, 23 March 2010, §§ 113-114.

¹⁰⁹⁸ Recital 42 E-commerce Directive.

¹⁰⁹⁹ Recital 43 E-Commerce Directive.

¹¹⁰⁰ P. VAN EECKE, "Online Service Providers and Liability: a Plea for a Balanced Approach", *Common Market Law Review* 2011, vol. 48, no. 5, p. 1463.

¹¹⁰¹ Legal Study on the implementation of the e-commerce directive (part 2) commissioned by the FPS Economy, SMEs, Self-Employed and Energy, 3 June 2020, p. 40.

exemption of liability.¹¹⁰² However, it is not explained to what extent moderation by AI tools can take place without risking the exemption.

If the distinction between active and passive hosting service provider is not abolished in the updated legal framework, those notions must be clarified and adapted with regard to hosting services and the use of AI tools. Intermediaries must know what they are entitled to do without risking losing the exemption. As explained above, the vagueness regarding the notion of passivity leads to overly cautious behaviour on the part of the intermediaries. Providers tend to over-remove content which may hamper freedom of expression.¹¹⁰³ In practice, platforms moderate their content according to their terms of services which are often stricter than the national laws.¹¹⁰⁴

Since the drafting of the E-commerce Directive, web hosting providers have been encouraged to take initiatives to tackle illegal content. The updated legal framework is the perfect opportunity to reaffirm it as well as to reassure providers about the maintenance of the exemption when they take such measures. Consideration has been given to the potential introduction into European law of a "Good Samaritan clause". According to that clause, intermediaries would not engage their responsibility when they act on their own initiative to make illegal content inaccessible, even if, by doing so, the intermediary allows other illegal content to pass through.¹¹⁰⁵ The purpose is to encourage intermediaries to act on their own initiative to fight illegal content online. In this case, the exemption of liability would no longer come from the passivity of the provider but from its willingness and good faith to tackle illegal content.

The DSA Proposal does not contain such "Good Samaritan clause". The text maintains the condition of passivity but expressly confirms that taking proactive measures to find illegal content does not preclude the application of the exemption.¹¹⁰⁶

5.4.2. Actual Knowledge

The E-commerce Directive does not give any definition of "actual knowledge" nor does it specify in which situation the host may be considered as having acquired that knowledge.

According to the European Court of Justice, effective knowledge is understood as the knowledge that any diligent intermediary would have had, regardless of the way in which the host becomes aware of the content *in concreto*.¹¹⁰⁷ It is, therefore, irrelevant whether the content is discovered as a result of measures taken by the host on its own initiative or whether the content was brought to its attention by a user or by an administrative or judicial authority.¹¹⁰⁸

¹¹⁰² The European Court of Justice has nevertheless tempered the requirement of passivity to hosting providers. In fact, it has progressively clarified in its case law that the fact that a service has to be paid for is not sufficient to deduce its active character. The same applies when the intermediary sets the conditions of use of its services and thus provides general information to users, the matching between terms inserted in a search bar and the results that will be displayed in response to this request. The host will obviously lose its passive character if it participates in the creation or if it appropriates the illegal content (see CJEU, *L'Oréal v. eBay*, Case C-324/09, 12 July 2011, § 115; CJEU, *Google France Inc. v. Louis Vuitton Malletier*, *op. cit.*, §§ 116-117.

¹¹⁰³ A. DE STREEL et al, "Online Platforms' Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)", *o.c.*, p. 23.

¹¹⁰⁴ *Ibid.*, p. 43.

¹¹⁰⁵ Section 230(c)(2), USA Communications Decency Act (CDA), 1996.

¹¹⁰⁶ Art. 6 DSA Proposal : "Providers of intermediary services shall not be deemed ineligible for the exemptions from liability referred to in Articles 3, 4 and 5 solely because they carry out voluntary own initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation."

¹¹⁰⁷ CJEU, *L'Oréal v. eBay*, *o.c.*, §§120-122.

¹¹⁰⁸ European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms", *o.c.*, p. 7.

Actual knowledge can be obtained through different channels. It may be the result of a decision by a court or authority, a private individual or even measures taken by the host itself on its own initiative. The most common means of obtaining this knowledge is through notification. This is a mechanism made available to users by the hosting provider, allowing them to notify a potentially illegal content. This mechanism must be visible, easy to access and user-friendly.

The updated legal framework must provide more precision concerning the notification process. The European Court of Justice has already stated that it must be “sufficiently precise and adequately substantiated”.¹¹⁰⁹ The legislation must at least provide for the formal requirements that notifications must fulfil in order to generate actual knowledge. The European legislator needs to make a balance. Indeed, too many prerequisites for the validity of the notification are a burden for the person who wishes to declare a content illegal. In application of this balance, it seems legitimate to ask the notification to contain basic elements such as the precise identification of the content that is the subject of the notification and the reason why the user is notifying this content.¹¹¹⁰ Another way to make the notification process more efficient is to prioritise the notification arising from certified notifiers such as NGO’s while sanctioning notifiers indulging in systematic wrongful notification.¹¹¹¹

In the DSA Proposal, Recital 22 indicates that “the provider can obtain such actual knowledge or awareness through, in particular, its own-initiative investigations or notices submitted to it by individuals or entities in accordance with this Regulation in so far as those notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and where appropriate act against the allegedly illegal content”.¹¹¹² In addition, Article 14 regulates the notification process for all providers¹¹¹³ and Article 19 gives precision on how the notification must be handled by the online platform when that notification is made by a trusted flagger.¹¹¹⁴ In conclusion, according to the DSA Proposal, when the notification fulfils all the requirements provided for by those articles, the provider is considered as having acquired actual knowledge of the illegal content. Otherwise, actual knowledge will not be automatically presumed.

5.4.3. Measures Taken by the Hosting Service Provider Against the Illegal Content

When the host acquires actual knowledge of the existence of illegal content, it must either block access to it or delete it if it wishes to benefit from the exemption of liability. The E-Commerce Directive only states that the provider is under the obligation to acts expeditiously to remove or to disable access to the illegal content it has knowledge of. There is no reference to the measures to be taken by the intermediaries to reach such result. In the end, the choice of the measures taken by the provider to combat illegal content is currently left to the discretion of the provider who defines its contours.

The DSA Proposal states that “the rules on such notice and action mechanisms should be harmonised at Union level, so as to provide for the timely, diligent and objective processing of notices on the basis of rules that are uniform, transparent and clear”.¹¹¹⁵ As explained above, the DSA Proposal imposes on every provider of hosting service an obligation to provide for a notice and action mechanism by which any user is able to notify a specific item of information that the

¹¹⁰⁹ *Ibid.*, p. 4 and p. 11.

¹¹¹⁰ *Ibid.*, p. 11.

¹¹¹¹ *Ibid.*, p. 14.

¹¹¹² Recital 22 DSA Proposal.

¹¹¹³ Art. 14 DSA Proposal.

¹¹¹⁴ Art. 19 DSA Proposal.

¹¹¹⁵ Recital 41 DSA Proposal.

user considers illegal.¹¹¹⁶ More details on the reaction that the provider must have upon receiving a notification of illegal content is found in Article 19 in which the DSA Proposal states that priority must be given to notices submitted by trusted flaggers.¹¹¹⁷

The updated legal framework should indeed provide for a clear notice and takedown procedure with an obligation for providers to inform users on how to notify a content. However, the regulation must also explain all the steps to be taken by the provider upon receiving the notification and specify reasonable timeframes.¹¹¹⁸ The blockage of a specific content is an interference in the content provider's right of expression. The interference is acceptable only if the suppression of the content is defined by law. Moreover, the measures taken must be proportional and adequate to achieve the protection of a greater interest.¹¹¹⁹ The notice and action mechanism must be conceived in a way to minimise the interference with fundamental rights. In order to do that, the legislation must set up safeguards to ensure that the measures taken by the intermediaries do not constitute excessive interference with the users' freedom of expression.

Among other things, the person who placed the notified content must be informed that the content has been notified.¹¹²⁰ Moreover, when a decision has been taken regarding that content, this decision must also be notified and explained to the parties involved.¹¹²¹ More importantly, the parties must have the possibility to appeal against the decision (i.e. appeal against an unjust removal by the notified user or against a decision not to remove by the notifying user).¹¹²² Intermediaries are encouraged to set up an internal appeal procedure without prejudice to the possibility for the person affected to go before the courts and tribunals.¹¹²³

It is of the utmost importance that the users are made aware of their rights to respect the rights to a fair hearing, to adversarial proceedings and to equality of arms. The content provider whose content is being contested and the notifier whose notification is not enforced must both have the opportunity to defend themselves. Finally, as already provided for in the EC directive, the content must be re-instated if the decision of removal is overruled.¹¹²⁴ In addition, other remedies can be applied in case of wrongful content removal such as apology, rectification or even damages.¹¹²⁵

Regarding the DSA, the proposal also provides that "where a hosting service provider decides to remove or disable information provided by a recipient of the service, for instance following receipt of a notice or acting on its own initiative, including through the use of automated means, that provider should inform the recipient of its decision, the reasons for its decision and the available redress possibilities to contest the decision, in view of the negative consequences that such decisions may have for the recipient, including as regards the exercise of its fundamental right to freedom of expression. That obligation should apply irrespective of the reasons for the decision

¹¹¹⁶ *Ibid.*

¹¹¹⁷ Art. 19 DSA Proposal.

¹¹¹⁸ Art. 14 DSA Proposal.

¹¹¹⁹ See Art. 12 EHRC.

¹¹²⁰ Council of Europe, Recommendation CM/Rec (2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, 7 March 2018, p. 7 available at [https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14;); Commission Recommendation on Measures to Effectively Tackle Illegal Content Online, o.c., p. 5.

¹¹²¹ European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms", o.c., p. 17.

¹¹²² Commission Recommendation on Measures to Effectively Tackle Illegal Content Online, o.c., p. 11.

¹¹²³ Council of Europe, "Recommendation CM/Rec (2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", o.c., p. 9; Commission Recommendation on Measures to Effectively Tackle Illegal Content Online, o.c., p. 5.

¹¹²⁴ Art. 14.3 E-commerce Directive.

¹¹²⁵ Council of Europe, "Recommendation CM/Rec (2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries", o.c., p. 9.

(...). Available recourses to challenge the decision of the hosting service provider should always include judicial redress".¹¹²⁶

5.5. The Prohibition of the General Obligation to Monitor

Article 15 of the E-Commerce Directive prohibits any obligation on intermediaries to monitor all the content updated by users. This prohibition only applies to general monitoring. Intermediaries can still be the object of an obligation to monitor a specific content (e.g. when an authority issues an order concerning a specific content).¹¹²⁷ Unfortunately, no definition is given of the general obligation to monitor. The distinction between a general and a specific obligation to monitor is unclear and allows for diverging interpretations. Despite the precision given by the Court of justice,¹¹²⁸ it is still unclear how it applies when it aims at preventing the re-upload of illegal content in the future. For the fight against illegal content online to be effective, it is necessary not only to remove the illegal content but also to prevent it from reappearing. The use of automated content detection filters poses a problem with regard to the distinction between general and specific monitoring. The case law has somewhat distinguished what could or could not be done in accordance with Article 15.

An authority or a judicial body can identify content as being illegal and force an intermediary to block access or remove identical contents.¹¹²⁹ The injunction can also require from the intermediary the suppression of "equivalent content" provided that "the monitoring is limited to information conveying a message essentially unchanged, and the differences in the wording of this equivalent content are not such as to oblige the hosting provider to carry out an independent assessment of this content".¹¹³⁰ In contrast, the intermediary cannot be required to set up a general and permanent filtering system that would detect this illegal content among all the information uploaded by Internet users.¹¹³¹

A clear distinction between what constitutes a general and specific control should be introduced in the updated legal framework otherwise those notions could be wrongly interpreted and the prohibition would become merely fictitious. This is surely what will happen if "the monitoring for almost every content is considered as specific and permitted without any restrictions or safeguards".¹¹³² Unfortunately, it has not been done by the DSA proposal.

5.6. Conclusion Regarding the Use of AI

Any legislation intended to be applied to AI must serve a double purpose. It should stimulate the use of AI by private and public actors while ensuring that AI applications are safe and trustworthy. The AI-application is trustworthy when it functions correctly and when individuals can understand the functioning and thus control that functioning. In order to function correctly, the AI-system must be trained and fed with quality and diversified data and not create any bias which would distort the result of the use of AI or the decisions taken by the AI-system.

¹¹²⁶ Recital 42 DSA.

¹¹²⁷ Recital 47 EC Directive.

¹¹²⁸ CJEU, *L'Oréal v. eBay*, § 144 : "The national courts with jurisdiction for the protection of intellectual property rights may order the operator of an online marketplace to take measures to put an end to infringements of intellectual property rights by users of that marketplace, but also to prevent such infringements in the future. Such injunctions must be effective, proportionate, dissuasive and must not create obstacles to legitimate trade".

¹¹²⁹ *Ibid.*, §. 101.

¹¹³⁰ CJEU, *Glawischnig-Piesczek v. Facebook*, Case C-18/18, 3 October 2019, §.53.

¹¹³¹ CJEU, *Scarlet v. SABAM*, Case C-70/10, 24 November 2011; CJEU, *SABAM v. Netlog*, Case C-360/10, 16 February 2012.

¹¹³² Legal study on the implementation of the e-commerce directive (part 2) commissioned by the FPS Economy, SMEs, Self-Employed and Energy, o.c., p. 49.

In addition to promoting the use of AI, there is a need to minimise the risks associated with the use of new technologies. One of the key requirements for the increase of trust in AI is transparency and privacy concerns. In the digitalised society, the amount of data and information available online is always increasing. As a result, it is difficult for providers to assess and moderate all content.¹¹³³ Moreover, AI is capable of inferring supplementary information about Internet users. Some of this information may turn out to be personal data or even sensitive data (e.g. sexual orientation, religious or political beliefs). In that case, the legislation about the protection of personal data will apply.¹¹³⁴

Concerning the use of AI by intermediaries, it has been decided that the mere fact that providers use AI-technologies does not automatically preclude the exemption of responsibility. With the amount of information available online increasing at a phenomenal speed, the use of automated tools is the only way to efficiently tackle illegal content online. In practice, the use of technological tools is the only realistic way to avoid the dissemination of illegal content online.¹¹³⁵

Nothing prevents the use of filtering systems to detect current infringements and to prevent future infringements under the condition that it constitutes specific monitoring *in concreto*. The prohibition in Article 15 is addressed to Member States' legislators who are prohibited from introducing into national law an obligation for intermediaries to monitor all information they store or transmit. In other words, the prohibition of a general obligation to monitor is not an obstacle to the adoption of spontaneous action by the hosting provider. Voluntary monitoring is desirable to combat illegal content and is even encouraged by the European Commission. However, intermediaries will be skeptical to implement general monitoring measures knowing that there is a risk that they lose their neutral character and thus the benefit of the exemption of liability.

Intermediaries, especially hosting service providers, often use AI to detect and react to illegal content posted by their users. AI makes it possible to process large amounts of information quickly. Filters and other AI-tools can be used to detect the illegal content or to prevent the re-upload of content declared illegal. Machine learning models are also able to make a decision about the legality of the content.¹¹³⁶ The European Commission calls for the development and the innovation of filtering technologies in order to increase their efficiency and accuracy.¹¹³⁷ The Commission also encourages the use of filtering technologies to ensure that previously removed content is not re-uploaded.¹¹³⁸

However, AI has limitations. When AI is used, there is a real risk of blocking lawful content and unduly restricting freedom of expression. Those risks appear when the intermediary uses automated filters to detect illegal content and even more when it is used to detect equivalent content. Indeed, currently existing automated measures cannot take into account all the nuances such as the context, the irony, etc.¹¹³⁹ In this regard, “[w]here hosting service providers use automated means in respect of content that they store, effective and appropriate safeguards should be provided to ensure that decisions taken concerning that content, in particular decisions

¹¹³³ A. DE STREEL et al, “Online Platforms’ Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)”, o.c., p. 40.

¹¹³⁴ H. SCHULTE-NOLKE et al., “The legal framework for e-commerce in the Internal Market: State of play, remaining obstacles to the free movement of digital services and ways to improve the current situation (Study requested by the IMCO committee)”, o.c., p. 28.

¹¹³⁵ Commission Recommendation on Measures to Effectively Tackle Illegal Content Online, o.c., p. 6.

¹¹³⁶ A. DE STREEL et al, “Online Platforms’ Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)”, o.c., p. 43.

¹¹³⁷ European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms”, o.c., p. 13.

¹¹³⁸ Commission Recommendation on Measures to Effectively Tackle Illegal Content Online, o.c., p. 6.

¹¹³⁹ Council of Europe, “Recommendation CM/Rec (2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries”, o.c., p. 7.

to remove or disable access to content considered to be illegal content, are accurate and well-founded. Such safeguards should consist, in particular, of human oversight and verifications, where appropriate and, in any event, where a detailed assessment of the relevant context is required in order to determine whether or not the content is to be considered illegal content".¹¹⁴⁰

Although effective, these automated tools also have limitations in terms of accuracy and requires human verification. For this reason, when the identification of a content as illegal is made by an automated and autonomous system, the content provider must have the possibility to contest the decision taken by AI and to require that the decision be reassessed by a human. This so-called "human-in-the-loop" safeguard must be inherent to the use of AI in every decision-making process.¹¹⁴¹ The removal of the content should be vetted by a human capable of understanding nuances that AI cannot.¹¹⁴² It is argued that "[t]he main advantage of human moderators is that their review will always allow for a greater degree of context (such as local culture, traditions, politics) and common sense to be applied to the online content in question".¹¹⁴³

The DSA proposal states in its Article 17.5 that "online platforms shall ensure that the decisions are not solely taken on the basis of automated means".¹¹⁴⁴ However, a general right for human intervention shall be expressly provided for by the updated legal framework.

Most platforms already have complaint mechanisms in place so that their users can easily notify an illegal content but many complaint turn out to be off-topic or unsubstantiated. As a consequence, the platform is not able to react to the notification in an efficient way.¹¹⁴⁵ Therefore, the definition of a notification process, as set out in the DSA, is relevant to ensure that the notifications are valid and consistent enough to allow the provider to act upon it.

5.7. Overview of the Identified Gaps

On the basis of the conducted analysis the following main gaps, which have (or might have) an impact regarding AI should be highlighted.

Firstly, filters and other AI-tools are used by intermediaries to detect the illegal content or to prevent the re-upload of content declared illegal. However, the current state of AI technologies does not guarantee an infallible result. For that reason, the use of artificial intelligence by intermediaries must be subject to legal regulations establishing appropriate safeguards. These safeguards consist mainly of a right to human intervention and an obligation of information. The stakeholders must be made aware of a notification of a content, the actions taken by the intermediary following the notification, and their respective rights pertaining the procedure. Among their rights, they must be reminded of their right to appeal the decision to maintain/delete a content.

Secondly, voluntary monitoring is desirable to combat illegal content and is even encouraged by the Commission. However, intermediaries hold back their intervention out of fear of losing the benefit of the exemption. The updated regulatory framework must expressly state that the mere

¹¹⁴⁰ European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms", o.c., p. 13.

¹¹⁴¹ European Commission, "White Paper on Artificial Intelligence - A European approach to excellence and trust", o.c.

¹¹⁴² European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms", o.c., p. 12.

¹¹⁴³ A. DE STREEL et al, "Online Platforms' Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)", o.c., p. 44.

¹¹⁴⁴ Art. 17.5. DSA Proposal.

¹¹⁴⁵ A. DE STREEL et al, "Online Platforms' Moderation of Illegal Content Online Law, Practices and Options for Reform (Study requested by the IMCO committee)", o.c., p. 40.

fact that providers use AI-technologies does not automatically preclude the exemption of responsibility.

The DSA brings a certain number of answers to the identified gaps.

CHAPTER 5 – INSURANCES (WP 5)

1. Introduction

AI can also have an influence on insurances. This will be covered in this final part of the study. More specifically, the benefits and concerns of using AI in insurances are examined (part 2). We will then focus on policy proposals made by interest groups (part 3) as well as on the existing Belgian legal framework (part 4). Once this has been done, the shortcomings in the legal framework (part 5) as well as key takeaways specifically with regard to AI and insurances will be covered (part 6). This part will only focus on the aspects and problems specifically related to the use of AI in insurance, and supplements to that extent the analysis in the previous chapters.

2. AI in Insurance: Benefits and Concerns

As emphasised in recent policy documents and guidelines of the Organisation for Economic Co-operation and Development (OECD), the European Insurance and Occupational Pensions Authority (EIOPA) and the EU Commission, as well as in studies, AI might be beneficial to insureds/beneficiaries and third parties (part 2.1.). However, at the same time some concerns are raised. Although these concerns are not new and well known in insurance, with the development of AI it should be monitored whether and to what extent they might be accentuated by the use of AI (part 2.2.).

2.1. AI in Insurance: Benefits

The use of AI allows insurers to consider a wider array of personal and behavioural data (including data not communicated by the policyholder/insured), allowing them to set a more accurate and fair premium. In general AI could improve the efficiency of transactions and business processes in several ways:

- Robo-advice is used to provide advice and offerings calculated through algorithms.¹¹⁴⁶ Automated advice could assist persons which do not have access to financial advice to gain input in a more cost efficient way than a human advisor.¹¹⁴⁷
- AI might be useful for product development. Insurance firms consider that AI will enable them to better understand their customer's needs and characteristics and, therefore, allow them to develop more personalised products and services.
- Due to the phenomenon of the inverted production cycle and the fear of adverse selection, moral hazard and subsidy aversion, classifying risks according to their loss profile (segmentation) is a key feature of private insurance. This results in higher risk insureds generally paying a higher premium, compared to those perceived to be a lower risk. Traditional pricing is based on a limited number of easily identifiable factors, such as address, name, age, diagnosed diseases and the information material to the assessment of the risks is communicated by the policyholder/insured.
- AI might help to develop more granular risk assessments, better segmentation of risks and more accurate price setting. The use of AI will allow insurers to consider a wider array of personal and behavioural data and charge corresponding premiums.

¹¹⁴⁶ EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", 2019, p. 21 available at https://www.eiopa.europa.eu/content/big-data-analytics-motor-and-health-insurance_en; The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", 2020, p. 6 available at https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/ai_in_insurance_web_0.pdf.

¹¹⁴⁷ OECD, "The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector", 2020, p. 25 available at <https://www.oecd.org/finance/The-Impact-Big-Data-AI-Insurance-Sector.pdf>; EIOPA, "European Commission's Digital Finance Strategy consultation - EIOPA draft response", 2020, p. 3 available at https://www.eiopa.europa.eu/content/eiopa-response-european-commission-digital-finance-strategy-consultation_en.

- AI is useful to assist decision-making.¹¹⁴⁸
- AI might result into new risk factors that enable the development of new products, such as Usage-Based Insurance (UBI).¹¹⁴⁹ The current penetration of UBI in Europe is still low. From the 222 insurance firms that participated in EIOPA's thematic review, only 15% of the motor insurance firms and 4% of the health insurance firms currently offer some kind of UBI product. It is to be expected that this number will increase in the next years.
- AI can enhance claims management, as AI-processes can speed up claims payment significantly.
- AI can make fraud detection more efficient and more accurate. According to EIOPA, fraud detection is currently the most common use of big data analytics.¹¹⁵⁰

2.2. AI in Insurance: Concerns

However, using AI in insurance also raises various concerns and points of attention. Some of them are more 'operational-related' (parts 2.2.1 to 2.2.7.), while others are more 'impact-related' (parts 2.2.8 to 2.2.10). These concerns seem to arise in all types of insurance contracts. However, the consequences are expected to be more severe in the case of health insurance.

2.2.1. Data Quality

There are several concerns and challenges related to data quality.

- Traditional datasets (e.g. demographic data or car characteristics) are increasingly combined with new types of data (e.g. behavioural data) in order to perform more sophisticated and comprehensive analysis.¹¹⁵¹

Insurance companies use rating factors in their pricing models based on both internal data (e.g. data collected directly from the candidate policyholder) and externally derived from third sources. The use of AI enables insurance companies to increasingly use rating factors unrelated to the risk to be insured when setting insurance premiums. The Financial Conduct Authority (FCA) found evidence that prices were set based on where consumers shop, what other products they buy or a customer's buying and media habits.¹¹⁵²

- Moreover, AI is about finding correlations and not causation. However, not all correlations imply causation. If the output of a model is based on correlations, which are falsely assumed to be causations, then the decision-making process would be biased as well.¹¹⁵³
- Also crucial is that the quality of AI models depends on the input data. The effectiveness and reliability of an algorithm is dependent on the quality, accuracy and completeness of the available data, and can be hampered by possible errors. It is, therefore, crucial to ensure the data quality and the suitability of data for the intended AI-applications in insurance. This is even more relevant in cases where insurers rely on data from external data sources to enrich existing datasets or to develop AI applications. In EIOPA's thematic

¹¹⁴⁸ The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 7.

¹¹⁴⁹ EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c., p. 18; EIOPA, "European Commission's Digital Finance Strategy consultation – EIOPA draft response", o.c., p. 3.

¹¹⁵⁰ EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c., p. 16.

¹¹⁵¹ EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c., p. 8.

¹¹⁵² FCA, "General Insurance pricing practices Market Study", 2020 available at <https://www.fca.org.uk/publication/market-studies/ms18-1-3.pdf>; This conclusions has also been reached by EIOPA, see EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c., p. 8.

¹¹⁵³ EIOPA, "European Commission's Digital Finance Strategy consultation – EIOPA draft response", o.c.

review, some firms admitted that it is challenging to find purchased data from third parties with the same quality standards than those datasets that they use internally.¹¹⁵⁴

Insureds may be adversely impacted because of insurers making assumptions and decisions that are based on alternative data that is incomplete, inaccurate or irrelevant. In the Netherlands, for example, a Dutch insurance consumer witnessed a 30% premium rise for his home insurance contract, following a re-assessment based on the use of big data and AI-tools. Evidence showed that, in this case, the insurance company was relying on information that was demonstrably wrong.¹¹⁵⁵

2.2.2. Transparency and Explainability of AI

Transparency and explainability are key principles and important to building trust with insureds and other stakeholders.¹¹⁵⁶ The underlying algorithm of AI is not transparent in most cases, especially in deep machine learning and biases could be built in, unintentionally and intentionally, potentially leading to inappropriate advice/output.¹¹⁵⁷ In EIOPA's thematic review, some insurance companies acknowledged that if AI-tools such as machine-learning algorithms would be used for pricing and underwriting purposes, it would be very difficult to explain to costumers the outcome of such tools.¹¹⁵⁸

Moreover, transparency and explainability enable individuals to seek redress against decisions affecting them.¹¹⁵⁹ This includes also the assessment of infringements of anti-discrimination law. Therefore, insurers should strive to enhance the interpretability of their AI-systems, particularly if these have a significant impact on individuals.¹¹⁶⁰

2.2.3. Taking Into Account Consumer's Individual Price Sensitivity

The use of AI could enhance insurance companies' understanding of a consumer's individual price sensitivity and its likelihood to shop around or switch insurance contracts at the time of renewal. As a consequence, insurance companies may increasingly charge prices based on the optimum amount of margin they can earn from an individual consumer, rather than the risk and/or cost of the individual policyholder.¹¹⁶¹

The possibility of unfair outcomes for insureds resulting from this price discrimination schemes seems to be significant. In 2018, the UK Citizens Advice submitted a complaint to the UK's Competition and Markets Authority (CMA) following their research that showed that 1 in 3 customers in the UK could be paying up to 70% more for their home insurance contracts compare to new consumers that regularly switch insurers. The FCA confirmed these findings as it found widespread evidence of insureds paying a "loyalty penalty": longstanding insurance customers

¹¹⁵⁴ EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c., p. 43; EIOPA, "European Commission's Digital Finance Strategy consultation – EIOPA draft response", o.c.

¹¹⁵⁵ Consumentenbond, "Premies woonhuisverzekeringen stijgen door gebruik Big Data", 2018, available at <https://www.consumentenbond.nl/nieuws/2018/premies-woonhuisverzekeringen-stijgen-door-gebruik-big-data>, BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", 2020, p. 9 available at https://www.beuc.eu/publications/beuc-x-2020-039_beuc_position_paper_big_data_and_ai_in_insurances.pdf.

¹¹⁵⁶ The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 10.

¹¹⁵⁷ OECD, "The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector", o.c. p. 44.

¹¹⁵⁸ EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c., p. 44; see also The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 11.

¹¹⁵⁹ The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 10.

¹¹⁶⁰ The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 10.

¹¹⁶¹ BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", o.c., p. 6; EIOPA, "European Commission's Digital Finance Strategy consultation – EIOPA draft response", o.c.

often paid more on average compared to new customers of insurance firms.¹¹⁶² Similar evidence can be found in the United States and Ireland.¹¹⁶³ So far, there is no similar research or evidence in Belgium.

2.2.4. Absence of Human Intervention

An important element that is included in many guidelines is the concern about human intervention. The request for human oversight is intended to ensure that AI does not undermine human autonomy or causes other adverse effects. The AI HLEG Guidelines provide some context on human intervention. It refers to oversight in the form of governance mechanisms such as human-in-the-loop, human-on-the-loop or human-in-command.¹¹⁶⁴

2.2.5. Interoperability

The EIOPA encourages the European Commission to promote the operability of applications and portability of data between different platforms as this would improve the power of consumers to switch between providers and, therefore, create an appropriate framework for innovation in insurance.¹¹⁶⁵

2.2.6. Third-Party Services and Outsourcing

There is an emerging trend to set up co-operation models in which the insurance value chain is originated, managed and controlled by technological platforms or other third parties. This raises a number of potential risks that other firms outside the insurance regulatory perimeter take a predominant position with significant impact on insurance business, including insurance distribution.¹¹⁶⁶

If not properly implemented and managed, co-operation models with third parties can make it harder for insurance undertakings to exercise effective control, oversight and governance of consumer outcomes, but also for supervisors to have full oversight of the value chain. It could potentially also lead to concentration and operational risks that might not always be apparent. Moreover, the extensive use of third parties can give rise to a number of conduct and prudential issues.

Based on EIOPA's recent work on the fragmentation of the insurance value chain and new business models, some underlying risks for supervisors associated with the fragmentation of the insurance value chain include:

- increased bundling of services and provision of insurance (e.g. when insurance is included in the price at point of sale);
- oversight concerns due to longer and more complex insurance value chains;
- risks that critical activities are moving beyond the regulatory perimeter;
- shift in market powers and structure;
- concentration risk;

¹¹⁶² Citizens Advice, 2017, available at

<https://www.citizensadvice.org.uk/Global/CitizensAdvice/Consumer%20publications/Report%20-%20Insurance%20loyalty%20penalty.pdf>; FCA, "General Insurance pricing practices Market Study", 2020 available at <https://www.fca.org.uk/publication/market-studies/ms18-1-3.pdf>.

¹¹⁶³ BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", o.c., p. 7-8.

¹¹⁶⁴ OECD, "The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector", o.c. p. 22; High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI", o.c., p. 16.

¹¹⁶⁵ EIOPA, "European Commission's Digital Finance Strategy consultation – EIOPA draft response", o.c.

¹¹⁶⁶ EIOPA, "European Commission's Digital Finance Strategy consultation – EIOPA draft response", o.c.

- competition issues, including 'lock-in' effect;
- threat to the viability of traditional business models;
- strategic risk;
- ICT, cyber, operational resilience, outsourcing, legal, compliance and reputational risks and other operational risks (which might not be apparent);
- the need to develop supervisory skills set to understand and oversee the aforementioned developments and changes and to properly respond to them.

2.2.7. Pricing Competition and Adverse Selection

Increasing segmentation has the potential to cause a price competition in which the insurers with a smaller market share are eliminated and the remaining insurers face smaller profits or larger losses.¹¹⁶⁷ The price competition is likely to be the result of insurers following each other in their segmentation policy in order to avoid adverse selection and ending up with only the bad risks.

2.2.8. Availability, Access and Affordability of Insurance

Segmentation in insurance leading to uninsurability or to difficulties in obtaining affordable and accurate insurance coverage is not new and not typically technology or AI related. In particular in a competitive (EU) insurance market, the use of AI could strengthen segmentation, especially to the detriment of higher risks. Increasingly sophisticated profiling could reduce to an even greater extent the availability, access, cover (exclusions) and affordability of insurance.¹¹⁶⁸ For example, to facilitate a swift claims handling of natural disasters causing damage to agribusinesses, insurance companies have developed parametric insurance products. The basic concept of parametric solutions is rather simple: parametric insurance covers the probability of a predefined event happening (e.g. a major hurricane or earthquake), paying out according to a predefined scheme instead of a lengthy claims adjustment process. Since the payout is based on independently verifiable and unambiguous parameters, the predetermined payment is made quickly, simply and without lengthy adjustments.¹¹⁶⁹ However, parametric insurance, while ensuring a quicky payment to the insured, might involve the potential risk of a more vigorous risk assessment using AI tools leading to more exclusions.

So far, EIOPA did not find evidence that an increasing granularity of risk assessments is causing exclusions for high-risk consumers, but EIOPA expects the impact of AI to increase in the years to come.¹¹⁷⁰

Although actuaries do not fear an impairment of risk pooling and mutualisation of risks (the core of insurance), increasingly personalised insurance products and the impact of AI on the insurance market should be monitored closely.

2.2.9. Direct and Indirect Discrimination

The use of AI in insurance carries the risk of unjustified discrimination, especially indirect discrimination. Insurance companies are prohibited from pricing and claims handling based on certain by law protected factors, such as gender, age, race. AI could lead to the application of other factors, not traditionally protected by anti-discrimination laws. Moreover, those factors could

¹¹⁶⁷ Commissie voor Verzekeringen, *Rapport van de werkgroep segmentering*, p. 18.

¹¹⁶⁸ EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c., p. 29; BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", o.c., p. 16; The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 10; L. WORTHAM, "The economics of insurance classification: the sound of one invisible hand clapping", *Ohio State Law Journal* 1986, vol. 47, p. 878.

¹¹⁶⁹ See: <https://www.munichre.com/en/solutions/for-industry-clients/parametric-solutions.html>.

¹¹⁷⁰ EIOPA, "European Commission's Digital Finance Strategy consultation – EIOPA draft response", o.c. p. 3.

feasibly act as proxies for these traits or could closely be correlated with protected characteristics and lead to proxy discrimination or indirect discrimination. In telematics motor vehicle insurance in which driving habits are being monitored, for example, we can imagine a situation where less educated individuals work during the night and take roads in urban areas. In a scenario where both of these elements represent a statistically higher risk and these insureds will have to pay more for their insurance, the question could be raised whether this would imply an indirect discrimination of less educated individuals. Another example of potential discrimination is if certain areas inhabited predominantly by persons of a particular race and/or nationality are marked as risky, or if poorer people living in more urban areas make more use of urban roads and this driving habit represents a statistically higher risk.

2.2.10. Ethics, Fairness and Sustainability S-goal

Closely related but not the same is the concern about fairness. Fairness is associated with many different notions, such as freedom, dignity, autonomy, privacy, non-discrimination, equality. These values need to be interpreted in a cultural, political, economic context. It seems, therefore, impossible to provide a universal standard of fairness. Especially in insurance, ensuring fair decisions is particularly intricate and complex in comparison to other industries. This relates to the differences in interpretation between the actuarial concepts of fairness and discrimination on the one hand and the concepts in anti-discrimination law on the other hand.

At a general level, a procedural and a substantive dimension of fairness can be distinguished.¹¹⁷¹ The procedural dimension implies that consumers are treated fairly throughout the entire process. An important aspect of fair treatment is the ability for customers to contest and seek effective redress against decisions affecting them. The substantive dimension implies that decisions should be fair in the sense that they do not unfairly discriminate and disadvantage individuals or groups of individuals. Most guidelines, therefore, emphasise the absence or minimisation of unfair bias and discrimination of AI-driven decisions as a key element of fairness. Some guidelines also mention equal and just distribution of both benefits and costs as a feature of fair decisions.¹¹⁷²

Increasing individualisation of insurance, driven by AI and data analytics, may disadvantage certain groups, for instance by charging unaffordable premiums or being denied cover altogether. When it comes to the use of AI-systems, it is often not enough to eliminate sensitive attributes from the data to ensure non-discrimination ('fairness through unawareness'), as such attributes can easily be picked up in proxies that correlate with these attributes. More granular risk-based pricing could be seen as especially unfair if it is done on the basis of personal characteristics over which consumers have no control or related to socially protected groups. This has led to the emergence of the notion of 'behaviour-based fairness'. With this kind of fairness, insureds are considered having control over their behaviour. What mainly determines the cover are not the technical calculations made by the insurance company, but the insured's own behaviour. As a consequence, premiums are considered to be fair if responsible behaviour is rewarded correctly.¹¹⁷³

¹¹⁷¹ The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 12. See also High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI", o.c.

¹¹⁷² The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 12. See also High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI", o.c.

¹¹⁷³ G. MEYERS and I. VAN HOYWEGHEN, "Enacting actuarial fairness in insurance: from fair discrimination to behavior-based fairness", *Science as culture* 2017, p. 431; D. MINTY, "Behavioural fairness is a serious risk to the future of insurance" available at <https://ethicsandinsurance.info/2020/04/29/behavioural-fairness/>.

3. Policy Proposals Made by Interest Groups

In view of tackling the above mentioned concerns regarding the use of AI in insurance, (consumer) organisations have already launched policy proposals to:

- Ban unfair price optimisation practices when selling insurance products to consumers. Firms should be prohibited from setting prices based on consumers individual price sensitivity or their likelihood to switch insurance contracts.¹¹⁷⁴
- Organise public control over the use of AI-technology as the societal risks of discrimination in insurance is considered to be very high. Rules governing the use of algorithms are, therefore, needed. Supervisors may, for example, need powers to eliminate the use of certain data points that are unnecessary or could be potential sources of bias, and regularly audit algorithms in order to detect potentially unlawful discriminatory outcomes.¹¹⁷⁵
- Modify anti-discrimination law since some situations cannot be properly tackled using anti-discrimination laws, as they traditionally focus on discrimination based on a limited list of protected factors.

Stringent requirements and limitations should be imposed on the use of data for personalised risk assessment. In particular, the processing of data may not intrude on intimate areas of private life. Rating criteria chosen by insurance companies should have a legitimate objective and there must be a clear causal relationship between the data and the risk. There should also be stringent requirements in respect of transparency, non-discrimination and the protection of third parties. In EIOPA's thematic review, some insurance companies highlight the strict transparency requirements of the GDPR and the fact that they are compliant with these requirements.¹¹⁷⁶

- Increase transparency about the types of personal data considered by insurers when selling policies to consumers and about how algorithmic decision that affect them are made. In particular, firms will need to be more transparent about the data points they take into consideration, as well as about the role of algorithmic decision-making in setting the premiums and the rationale behind the functioning and results of such systems.¹¹⁷⁷ Some guidelines also emphasise that individuals should be aware of the fact that they are interacting with an AI-system such as a chatbot. Some guidelines also advice counterfactual explanations (e.g. "you were denied insurance because ...").¹¹⁷⁸

EIOPA emphasises that explainability requirements may differ depending on the use. For example, fraud prevention techniques may arguably need to be less transparent vis-à-vis consumers in order to avoid jeopardising the ability of insurance undertakings to fight against fraudsters.¹¹⁷⁹ In relation to this, some have explored the idea of "explainable AI", which encourages the notion that AI also needs to be able to respond to questions on "why" it has reached certain decisions.¹¹⁸⁰

¹¹⁷⁴ BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", o.c., p. 8.

¹¹⁷⁵ BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", o.c., p. 30.

¹¹⁷⁶ EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c., p. 44.

¹¹⁷⁷ BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", o.c., p. 12-13; The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 11.

¹¹⁷⁸ The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 11-12.

¹¹⁷⁹ EIOPA, "European Commission's Digital Finance Strategy consultation – EIOPA draft response", o.c., p. 52.

¹¹⁸⁰ OECD, "The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector", o.c. p. 26; The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 11.

- Monitor the use of AI and set out metrics to be used to measure affordability and exclusion. The Dutch Insurance Association has developed a 'solidarity monitor' to assess the development of the spread of insurance premiums and individual insurability over time in motor vehicle insurance, household insurance, liability insurance and death insurance.¹¹⁸¹ Supervisors should closely monitor the prices between traditional insurance policies and policies that rely on personalised risk assessment to assess the impact of big data and AI-technologies. The difference between individual prices charged on the basis of personalised and non-personalised risk assessments should not exceed certain percentages.¹¹⁸²
- Impose limits on the individualisation of insurance, for instance by limiting the allowed ratio between the highest and lowest premium.¹¹⁸³ Consumers should continue to be able to access insurance policies that do not rely on intrusive data processing practices or behavioural analytics.¹¹⁸⁴
- Empower supervisors to carefully monitor the reliability of algorithms, including the accuracy and the relevance of the data used.¹¹⁸⁵

4. Current Belgian Legal Framework

In this part, the multi-layered (legal) framework will briefly be pointed out (part 4.1.). Subsequently, the current Belgian legal framework regarding 'operational-related' (part 4.2.) as well as 'impact-related concerns (part 4.3.) will be analysed.

4.1. General Point of Attention: 'Multi-layered' Belgian law

Belgian law must be compatible with the EU (EEA) legal framework on insurance. The key features of this legal framework can be summarised as follows:

- insurance companies and insurance distributors operate in an EEA internal insurance market, based on the right of establishment and the right of free provision of services (see Treaty of the Functioning of the European Union-TFEU);
- the taking up and pursuit of insurance activities and insurance distribution is already quite extensively regulated, while national rules related to non-harmonised aspects have to meet the requirements of the general good test as developed by the Court of Justice of the EU;
- the key principle of the operational and financial regulation is 'home country control';
- the prohibition of *a priori* and *a posteriori* systematic control of tariffs, premiums, insurance conditions and documents used in the contractual relation between the insurer and the insured (with the exception of compulsory non-life insurance contracts and tariffication factors in life insurance);

¹¹⁸¹ The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 14; Verbond van Verzekeraars, "Solidariteitsmonitor. Drie jaar later, 2020", 2020, available at <https://www.verzekeraars.nl/media/7948/solidariteitsmonitor-2020.pdf>.

¹¹⁸² So far there is no evidence that the use of AI is increasing the standard deviation (the spread between the lower and the higher premiums), see EIOPA, "Big Data Analytics in Motor and Health Insurance: A Thematic Review", o.c. p. 18.

¹¹⁸³ The Geneva Association, "Promoting Responsible Artificial Intelligence in Insurance", o.c., p. 13.

¹¹⁸⁴ BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", o.c., p. 16.

¹¹⁸⁵ BEUC, "The Use of Big Data and Artificial Intelligence in Insurance", o.c., p. 14; OECD, "The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector", o.c. p. 25.

- insurance companies have the freedom to set rates (freedom of tariffication) as interpreted by the CJE (e.g. Case DKV/Test Achats of 7 March 2013), and which is not an absolute freedom;
- the competition rules stated in the TFEU fully apply to the insurance sector. Since the EC Commission Regulation on Block exemption was not renewed in 2017, insurers and insurance associations have to conduct a self-assessment;
- Article 7 of the Rome I Regulation¹¹⁸⁶ provides specific conflict of laws rules to determine the national law applicable to the insurance contract;
- consumer law applies to insurance contracts concluded with consumers (policyholder).

4.2. Current Belgian Law Regarding ‘Operational-Related’ Concerns

In this part, we will first discuss compliance monitoring and supervision of AI-Technologies in the insurance sector (part 4.2.1.) as well as briefly focus on the GDPR (part 4.2.2.).

4.2.1. Compliance Monitoring and Supervision of AI-Technologies in Insurance

There are currently no specific rules in Belgium on the supervision of the design and the use of AI-technologies by insurance companies and insurance distributors. However, the general (EU-based) supervision framework applies to:

- insurance companies: Act of 13 March 2016 on the status and supervision of insurance or reinsurance undertakings (Supervision Act¹¹⁸⁷) and the conduct of sales rules (Insurance Act¹¹⁸⁸);
- insurance distributors (Part 6 Insurance Act)

Regarding insurance companies, the monitoring and supervision of AI falls under the governance rules supervised by the National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA).¹¹⁸⁹

In EIOPA’s thematic review, many insurance companies mention the Solvency II’s governance requirements (audit, actuarial, compliance and risk-management functions) as providing several lines of defence to address potential issues arising from AI.¹¹⁹⁰ They can use their “three lines of defence” to respond to the concerns related to AI-technologies. The risk, actuarial and the compliance department (second line of defence) could take on this role under the supervision of the internal audit function (third line of defence).

The outsourcing by insurance companies is regulated in the Supervisory Act (implementing the Solvency II rules). The outsourcing can be for services rendered to insureds (e.g. call centres, etc.) or administrative work (e.g. bookkeeping, claims settlement, investment management, etc.) and

¹¹⁸⁶ Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008.

¹¹⁸⁷ Wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen.

¹¹⁸⁸ Part 2-3 of Wet van 4 april 2014 betreffende de verzekeringen.

¹¹⁸⁹ The NBB’s Overarching circular on governance (version update May 2020) stresses the need of properly working IT systems and the importance of cybersecurity (available at https://www.nbb.be/doc/cp/eng/2020/20200505_nbb_2016_31_governance_clean.pdf, p. 71). See for the regulation on IT infrastructure: <https://www.nbb.be/en/financial-oversight/prudential-supervision/areas-responsibility/insurance-or-reinsurance-18>. See also for EU insurance companies and insurance companies of third countries: Circulaire CBFA 2009 17 1 (7 April 2009) Financiële diensten via internet: prudentiële vereisten and Bijlage bij Circulaire CBFA 2009 17 1 (7 April 2009) Gezonde praktijken inzake het beheer van internetbeveiligingsrisico’s, CBFA - Kredietinstellingen - Circulaires en mededelingen - Financiële diensten via het Internet: prudentiële vereisten (fsmab.be) and https://www.fsmab.be/sites/default/files/public/sitecore/media%20library/Files/fsmabfiles/circ/nl/2009/cbfa_2009_17-1.pdf.

¹¹⁹⁰ EIOPA, “Big Data Analytics in Motor and Health Insurance: A Thematic Review”, o.c. p. 42, 49.

specialist functions (e.g. IT, internal audit and data management, etc.).¹¹⁹¹ Moreover, insurance contract law (Part 4 Insurance Act) and conduct of business rules (Part 2, 3 and 6 Insurance Act) impose obligations on the insurance companies and distributors regarding information and archiving, irrespective of the tools or data used to reach the (policy) decision. The FSMA is the competent supervisory authority.

4.2.2. General Data Protection Regulation

Insurance companies and insurance distributors are subject to the GDPR, the imposed DPIA¹¹⁹² and the accountability principle. With regard to the application of the GDPR in an insurance context, there remain substantial legal uncertainty and questions. Most of them are related to the interpretation of the concepts of the GDPR and must be dealt with in general at EU level (see infra part 5.1.1).

4.3. Current Belgian Law Regarding ‘Impact-Related’ Concerns

With regard to the abovementioned concerns related to the ‘impact of AI’, Belgian law already provides a significant legal framework to address those issues. The advantage of this legal framework is the fact that it is technologically neutral. In the following paragraphs, we will focus on insurance contract law (part 4.3.1.), conduct of business rules (part 4.3.2.), general anti-discrimination laws (part 4.3.3.) and consumer laws that are applicable to insurance contracts (part 4.3.4.).

4.3.1. Insurance Contract Law

The Belgian insurance contract law already provides for several elements that may be relevant.

Most relevant are:

- a total prohibition on the communication and the use of genetic information (Article 58 and 61 Insurance Act).
- It also includes rules aiming at reintroducing redistributive solidarity, with a view to enhance and guarantee the access to an adequate and affordable insurance coverage, and fairness in particular with regard to:
 - o certain health insurance contracts (employment related or not employment related (Article 201-211 Insurance Act);
 - o certain outstanding balance insurance contracts (Article 212-226 Insurance Act; RD 10 April 2014);
 - o tariffication bureau in motor vehicle liability insurance (Article 9bis-9quinquies MVL Act 21 November 1989)
 - o mandatory coverage of natural disasters and tariffication bureau Natuurrampen in household insurance (simple risks/*eenvoudige risico's*)

¹¹⁹¹ See for the regulation, <https://www.nbb.be/en/financial-oversight/prudential-supervision/areas-responsibility/insurance-or-reinsurance-15>.

¹¹⁹² Art. 35 GDPR; BEUC, “The Use of Big Data and Artificial Intelligence in Insurance”, o.c.; WP 29, “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679” (WP 248 rev.01), 4 April 2017, p. 14 available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236; K. VRANCKAERT et al, “Ethische principes en (niet-) bestaande juridische regels voor AI. Een praktische gids”, o.c., p. 47-48, 50 and 80 available at <https://data-en-maatschappij.ai/publicaties/ethische-principes-en-niet-bestaande-juridische-regels-voor-ai>.

- The “right to be forgotten” is provided for certain outstanding balance insurance contracts concerning cancer and certain chronic diseases (Art. 61/1-61/3 Insurance Act and RD 26 Mai 2019).
- The Act of 10 December 2020¹¹⁹³ inserts the Articles 46/1 until 46/3 in the Insurance Act. It applies to individual life insurance contracts and health insurance contracts as defined in Article 201, §1 Insurance Act. The aim is to restrict the use of health data and lifestyle data collected through devices connected to the internet for risk pricing and/or defining the coverage.¹¹⁹⁴ The underlying ratio is the fear of hyper individualisation of risks jeopardising the mutualisation and the solidarity principle that underpins the insurance model,¹¹⁹⁵ in particular at the expense of persons of socially weaker groups who cannot afford to buy healthy food and exercise several times a week.¹¹⁹⁶

The rules provide that:

- o during the conclusion of the insurance contracts referred to in Article 46/1, the refusal of the insured to purchase or use a device connected to the internet that collects personal data concerning his lifestyle or health may not lead to a refusal to conclude a contract nor to a higher premium. It follows that the potential insured may not be punished for his refusal to purchase or use such a device (Article 46/2 Insurance Act);¹¹⁹⁷
- o no segmentation for acceptance, tarification and/or determination of coverage may be applied on the basis of the agreement of the insured to use such a device connected to the internet that collects personal data concerning his lifestyle or health or to share this data, nor on the basis of the use of such information by the insurer. Hence, an insured may not be treated favourably because he voluntarily wants to use such a device or share the data with his insurer (Article 46/3 Insurance Act).¹¹⁹⁸

4.3.2. Conduct of Business Rules

Regarding certain specific insurance contracts commonly concluded by consumers (policyholder) (Article 43 Insurance Act), Belgian law already provides for:

¹¹⁹³ Act of 10 December 2020 amending the Act of 4 April 2014 on Insurances (Wet van 10 december 2020 tot wijziging van de wet van 4 april 2014 betreffende de verzekeringen), MB 15 januari 2021.

¹¹⁹⁴ Wetsvoorstel tot wijziging van de wet van 4 april 2014 betreffende de verzekeringen, teneinde in verband met de ziekteverzekering en de levensverzekering beperkingen op te leggen aangaande het gebruik van de gegevens die door met het internet verbonden apparaten zijn verzameld, *Parl. St. Kamer* 2019-20, no. 55 0263/001, p. 3.

¹¹⁹⁵ Wetsvoorstel tot wijziging van de wet van 4 april 2014 betreffende de verzekeringen, teneinde in verband met de ziekteverzekering en de levensverzekering beperkingen op te leggen aangaande het gebruik van de gegevens die door met het internet verbonden apparaten zijn verzameld, *Parl. St. Kamer* 2019-20, no. 55 0263/001, p. 6; Verslag van de eerste lezing over het wetsvoorstel tot wijziging van de wet van 4 april 2014 betreffende de verzekeringen, teneinde in verband met de ziekteverzekering en de levensverzekering beperkingen op te leggen aangaande het gebruik van de gegevens die door met het internet verbonden apparaten worden verzameld, *Parl. St. Kamer* 2019-20, no. 55 0263/005, p. 4; Verslag van de tweede lezing over het wetsvoorstel tot wijziging van de wet van 4 april 2014 betreffende de verzekeringen, teneinde in verband met de ziekteverzekering en de levensverzekering beperkingen op te leggen aangaande het gebruik van de gegevens die door met het internet verbonden apparaten worden verzameld, *Parl. St. Kamer* 2019-20, no. 55 0263/009, p. 6.

¹¹⁹⁶ Verslag van de tweede lezing over het wetsvoorstel tot wijziging van de wet van 4 april 2014 betreffende de verzekeringen, teneinde in verband met de ziekteverzekering en de levensverzekering beperkingen op te leggen aangaande het gebruik van de gegevens die door met het internet verbonden apparaten worden verzameld, *Parl. St. Kamer* 2019-20, no. 55 0263/009, p. 6.

¹¹⁹⁷ J-M. BINON and N. SCHMITZ, “Développements récents dans les assurances de personnes”, in C. PARIS, J-M. BINON, V. CALLEWAERT, T. DUBUISSON, S. GILSON, F. LAMBINET, N. SCHMITZ and Z. TRUSGNACH (eds.), *Actualités en droit des assurances*, Waver, Anthemis, 2020, p. 282.

¹¹⁹⁸ J-M. BINON and N. SCHMITZ, “Développements récents dans les assurances de personnes”, o.c., p. 282.

- a general rule prohibiting segmentation unless objectively justified. It is stated that “any segmentation in terms of acceptance, pricing and/or coverage must be objectively justified by a legitimate aim and the means of achieving that aim must be appropriate and necessary” (Article 44 Insurance Act);
- a legal obligation of the insurance company to honour the following legal safeguards:
 - (1) the publication of the segmentation criteria it uses for each type of insurance contract on its website. The insurer must also provide guidance on the division and the segmentation criteria used (Article 45 Insurance Act);
 - (2) providing information on the segmentation criteria (i) in the insurance quote; (ii) when amending the insurance contract in the event of aggravation of the risk or of cancellation of the contract; and (iii) in the case of refusal of insurance coverage (Article 46 Insurance Act).

Part 6 of the Insurance Act already specifies, amongst other things, that insurance distributors must:

- act in accordance with the duty of care (Article 279 §1, Article 284 §1 - §2 and §4, Article 296 §2) meaning that they (i) must act honestly, fairly and professionally in accordance with the best interests of their customers, (ii) must determine the demands and needs of the customer and (iii) can only propose a contract/product consistent with the customer’s insurance demands and needs.
- provide a personalised recommendation explaining why a particular product would best meet the customer’s demands and needs, if the insurance distributor provides advice (Article 284 §1 - §4, Article 296 §3)
- maintain, operate and review a process for the approval of each insurance product, or significant adaptations of an existing insurance product, before it is marketed or distributed to customers. Amongst other things, insurance distributors must ensure that the intended distribution strategy is consistent with the identified target market (Article 288).

4.3.3. General Anti-Discrimination Laws

The three general anti-discrimination laws prohibiting discrimination in horizontal, contractual, relations do apply to all insurance contracts and impose a number of criminal and civil sanctions. The legal instruments are the General anti-Discrimination Act,¹¹⁹⁹ the Gender Equality Act¹²⁰⁰ and the Anti-Racism Act.¹²⁰¹ Together they apply to 19 factors. However, only very little (published) case law exists on the application of these laws in insurance.

4.3.4. Consumer Law Applicable to Insurance Contracts Concluded with Consumers

Although reference is also made to the part of this study dealing with consumer protection, it would be interesting to monitor whether websites or platforms comparing insurance terms and conditions and premiums increases competitive pressures for insurance companies and ensure

¹¹⁹⁹ Act of 10 May 2007 combating certain forms of discrimination (Wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie). See also, EU Commission, Guidelines on the application of Council Directive 2004/113/EC to insurance, in the light of the judgment of the Court of Justice of the European Union in Case C-236/09 (*Test-Achats*), OJ C 13 December 2012, p. 11.

¹²⁰⁰ Act of 10 May 2007 combating certain forms of discrimination.

¹²⁰¹ Act of 30 July 1981 on the criminalisation of certain acts motivated by racism or xenophobia (Wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden). See also Guidelines of the EU Commission on the interpretation of the *Test-Achats* case.

that the pricing practices are fair towards consumers and refrain them from pricing based on consumers individual price sensitivity or their likelihood to switch insurance contracts.

5. Shortcomings/Gaps of the Current Legal Framework

As pointed out above, legislative initiatives to tackle shortcomings or gaps in the current legal framework must be compatible with the EU legal framework on the European internal market of insurance activities and insurance distribution (see part 4.1). Moreover and of utter importance is the fact that the boundaries and specificities of private insurance must be safeguarded. Private insurance is not social insurance and it must be avoided that legislation would lead to insurers leaving the market. In the following parts, shortcomings regarding operational-related concerns (part 5.1.) as well as impact-related concerns (part 5.2.) are analysed.

5.1. Shortcomings Regarding ‘Operational Related’ Concerns

5.1.1. General Data Protection Regulation

In general, the application of the GDPR and its implementation in Belgium by the Act of 30 July 2018¹²⁰² in an insurance context causes difficulties and interpretation problems.

More specifically, a first important problem is the uncertainty as to the legal basis insurance companies/distributors can rely when processing personal data of the (potential) policyholder, insured and/or third parties in the course of their activities. This is especially true for the processing of special categories of personal data, among which health data (in the broad sense including lifestyle data). Insurance companies/distributors need to process health data not only in personal insurance (e.g. health insurance, life insurance), but also in damage insurance (e.g. in third-party liability insurance in which insurers/distributors need to process health data of the victim). Following Article 9(1) GDPR, the processing of this kind of personal data is actually forbidden unless one of the ten exceptions provided by Article 9(2) applies. Some of these exceptions are directly applicable, such as explicit consent of the data subject (Article 9(2)a) and necessity for the establishment of legal claims (Article 9(2)f). Others require some action of Member States, such as when the processing is necessary for reasons of substantial public interest (Article 9(2)g) and or when it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (Article 9(2)h).

So far, there is no specific legal ground insurance companies can rely on for the processing of special categories of personal data in Belgium. Therefore, they can only rely on explicit consent of the data subject when processing special categories of personal data in the course of their activities (e.g. underwriting, claims handling).

Also when processing data relating to criminal offences and convictions for underwriting purposes (e.g. in telematics motor vehicle insurance retrieving data concerning driving behaviour), it seems that explicit consent is the only legal basis insurance companies can rely on following Belgian law. Following article 10 GDPR, besides having to rely on a legal basis as foreseen by article 6(1) GDPR, the processing of these data may be carried out only under the control of an official authority, or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Article 10 Act of 30 July 2018 states that personal data relating to criminal convictions and offences can only be processed in the following cases¹²⁰³: (1) by natural persons or by legal persons under private or public law insofar as this is

¹²⁰² Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, MB 5 September 2018.

¹²⁰³ Article 10 Act of 30 July 2018.

necessary for the management of their own disputes (e.g. when handling claims or when assessing fraud committed by the insured); (2) by lawyers or other legal advisers to the extent required by the defense of their clients' interests (e.g. claims handled in the context of legal expenses insurance); (3) by other persons, if the processing is necessary for reasons of important public interest for the performance of tasks of general interest that have been established by or pursuant to a law, decree, ordinance or European Union law (e.g. processing in the context of money laundering); (4) insofar as the processing is necessary for scientific, historical or statistical research or with a view to archiving; (5) if the data subject has given explicit written permission for the processing of those personal data for one or more specific purposes and the processing remains limited to those purposes (e.g. in the context of the duty to disclosure of the policyholder); or (6) if the processing relates to the personal data that the data subject apparently disclosed on his own initiative for one or more specific purposes and the processing remains limited to those purposes.¹²⁰⁴

However, the application of explicit consent in an insurance context remains problematic. In particular, the question is raised whether consent can be freely given, as the personal data are necessary for the insurance company to fulfil its contractual obligations. Refusal by the (potential) insured to share its personal data might leave the insurance company with no other choice than to refuse to conclude a contract or to terminate the agreement.¹²⁰⁵ Moreover, questions arise regarding as to how insurers can obtain consent from a data subject that did not conclude a contract with the insurance company (e.g. insured other than the policyholder in collective insurance, a third party in a liability insurance, experts, ...). For these reasons, the Belgian Data Protection Authority and the Belgian 'Commissie voor Verzekeringen' advised the legislator to provide a legal basis that allows for the processing of special categories of personal data in the context of an insurance contract within certain boundaries.¹²⁰⁶ However, there remains uncertainty as on which legal provision of the GDPR this legal basis should be based, for which processing activities and for which kind of insurance contracts such a legal basis should be provided.

Moreover, the same questions arise with regards to the processing of (special categories of) personal data by insurance intermediaries. When purchasing an insurance product, insurance intermediaries are often involved to facilitate the process and to assist the potential policyholder with completing a (medical) questionnaire. Hence, while assisting the potential policyholder to conclude the insurance contract, insurance intermediaries also process personal data including

¹²⁰⁴ C-A. VAN OLDENEEL, 'Protection des données: le GDPR complété par deux nouvelles lois – Données à caractère pénal' (2018) Vol. 3 Bull. Ass., 405-406.

¹²⁰⁵ See Commissie voor Verzekeringen, Advies DOC C/2019/1 over de verwerking van medische gegevens in het kader van EU Verordening 2016/679 Algemene Verordening Gegevensbescherming, 16 juli 2019; Insurance Europe, Position paper: Insurance Europe's contribution to the Article 29 Working Party consultation on draft guidelines on consent, 2018, p. 2 available at

<https://www.insuranceeurope.eu/sites/default/files/attachments/Contribution%20to%20the%20Article%2029%20Working%20Party%20consultation%20on%20draft%20guidelines%20on%20consent.pdf>; Gegevensbeschermingsautoriteit, Beslissing ten gronde 24/2020 van 14 mei 2020, DOS-2019-02902, 17; Insurance Europe, "Position paper: Insurance Europe views on EC report on the review of the GDPR", 2020, p. 11, available at

https://www.insuranceeurope.eu/sites/default/files/attachments/Views%20on%20the%20EC%20report%20on%20the%20review%20of%20the%20GDPR_0.pdf.

¹²⁰⁶ Gegevensbeschermingsautoriteit, Beslissing ten gronde 24/2020 van 14 mei 2020, DOS-2019-02902, 17; Commissie voor Verzekeringen, Advies DOC C/2019/1 over de verwerking van medische gegevens in het kader van EU Verordening 2016/679 Algemene Verordening Gegevensbescherming, 16 July 2019.

special categories of personal data. It remains uncertain whether insurance intermediaries have a legal basis to rely on when processing personal data in the course of their activities.¹²⁰⁷

Particular problems on the application of the GDPR also rise in the context of AI and profiling without human involvement in insurance. The GDPR specifically addresses profiling and defines it as: “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.¹²⁰⁸

The GDPR distinguishes between two forms of profiling. First, “general profiling and automated decision making”, to which the rules on legal grounds of processing (Article 6 and 9), data protection principles (Article 5) and the rights of data subjects apply. Second, “solely automated individual decision-making, including profiling”, to which the strict requirements of Article 22 GDPR apply. Solely automated individual decision-making means applying technology in a decision-making process without meaningful human involvement.¹²⁰⁹

AI-technologies make it easier for insurers to create profiles and to make automated decisions. For the purpose of this study, we assume that these technologies imply the absence of human involvement in the decision-making process, and therefore fall under the second form. The insurance company cannot circumvent the requirements of Article 22 GDPR by establishing meaningless human involvement. For example, if the insurer routinely applies automatically generated profiles to potential policyholders without any prior and meaningful assessment by a human who has any actual influence on the result, the decision will still be based solely on automated processing including profiling.¹²¹⁰ The human intervention cannot be merely symbolic and should always be carried out by someone who has the authority and competence to actively review and change the decision rather than being blindly steered by the process.¹²¹¹ This person should be able to take all relevant factors into account prior to the formalisation of the result of the automated decision-making process as a decision.¹²¹² On the other hand, if the algorithm is just a support tool and the decision is only considered a recommendation and can be adapted by a human at any time, Article 22 GDPR will not apply. In this case, the general rules of the GDPR will apply.

Again, the question arises whether insurance companies using AI-technologies have a legal basis to rely on. For solely automated processing, including profiling, with regular personal data Article 22(2) GDPR provides three potential legal grounds, namely if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate

¹²⁰⁷ Insurance Europe, Position paper: Response tot he EC stocktaking exercise on application of GDPR, 2019, p. 8, available at https://www.insuranceeurope.eu/sites/default/files/attachments/Response%20to%20EC%20stocktaking%20exercise%20on%20application%20of%20GDPR_0.pdf; Commissie voor Verzekeringen, Advies DOC C/2019/1 over de verwerking van medische gegevens in het kader van EU Verordening 2016/679 Algemene Verordening Gegevensbescherming, 16 July 2019.

¹²⁰⁸ Article 4(4) GDPR.

¹²⁰⁹ Article 29 Working Party, “Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679”, 17/EN WP251rev.01, 2018, p. 8; E. KAMENJASEVIC, “Profiling in the financial sector under the GDPR (Part I)”, CiTiP Blog, p. 2 available at <https://www.law.kuleuven.be/citip/blog/profiling-in-the-financial-sector-under-the-gdpr-part-i/>.

¹²¹⁰ Article 29 Working Party, “Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679”, o.c., p. 21.

¹²¹¹ Article 29 Working Party, “Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679”, o.c., p. 21.

¹²¹² Article 29 Working Party, “Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679”, o.c., p. 21.

interests; or (c) is based on the data subject's explicit consent. In Belgium, so far, there is no legal provision allowing insurance companies to apply solely automated individual decision-making, including profiling.¹²¹³ Hence, the only potential legal grounds insurance companies can rely on are necessity for entering into, or the performance of, a contract and explicit consent. In recent years, insurance companies are using automated individual decision-making in claims-handling and in order to detect fraudulent activities in all kinds of insurance contracts.¹²¹⁴ The question arises whether insurance companies have a legal basis to rely on for the processing of data for these purposes and, if not, whether such a legal ground should be created in Belgian law.

For special categories of personal data, there are only two potential legal bases provided for by Article 22(3) GDPR, namely explicit consent and necessity for substantial public interest. As explained before, the application of necessity for substantial public interest as a legal basis requires some action of the Member States. So far, this is not the case in Belgium. As a result, insurance companies can only rely on explicit consent if they want to apply solely automated individual decision-making involving special categories of personal data. As highlighted above, the application of consent as a legal basis remains problematic in an insurance context. As a consequence, insurance companies operating on the Belgian territory cannot possibly apply solely automated individual decision-making, including profiling, especially involving special categories of personal data.

A preliminary policy question to be answered is whether a legislative action is needed to allow/facilitate insurance companies to make decisions based on solely automated decision-making, including profiling? If so, for which processing purposes/insurance contracts? Several studies emphasise the importance of human involvement when taking decisions to avoid adverse effects, especially when the decisions might have a severe impact on people's lives.¹²¹⁵ However, prohibiting the use of solely automated decision-making, including profiling, on the basis of consent of the policyholder or any other legal basis would imply the prohibition to use AI-technologies and machine learning in insurance and, therefore, might hinder the design of innovative insurance products.

A second important concern relates to the fact that the principles dealing with the processing of personal data stipulated in Article 5 GDPR as well as the data subject's rights contained in chapter III GDPR have to be respected. In particular with respect to solely automated individual decision-making, including profiling, Article 22 GDPR requires data controllers to implement suitable measures. In this regard, legal uncertainty and interpretation problems also arise in practice. Of particular importance in insurance and even more pressing when it comes to AI are the application of the principles of accuracy (also issue of correlation and causation), transparency and data minimisation. These issues must be dealt with at the level of the EU legal framework. However, it can be argued that the Belgian rules concerning the segmentation criteria (Articles 42-46) and the

¹²¹³ Belgian law implements article 22 GDPR in article 35 of the Act of 30 July 2018 which can be translated as follows: "Any decision based only on automated processing, including profiling, which produces adverse legal effects for the data subject or significantly affects him/her, is permitted if a National law, decree, ordinance, European Union law or an international agreement provides appropriate safeguards for the rights and freedoms of the data subject, and at least the right to obtain human intervention by the controller. Any profiling which discriminates against natural persons on the basis of the particular categories in personal data referred to in Article 34 shall be prohibited". Accordingly, the Belgian law seems to refer just to future or sectorial laws permitting automated decision-making, see G. MALGIERI, "Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations", *Computer Law & Security Review* 35 2019, 12.

¹²¹⁴ Insurance Europe, Comments on profiling, 2017, 3; J. AMANKWAH AND C. VAN SCHOUBROECK, "Fraud detection in motor insurance: privacy and data protection concerns under EU law", not yet published.

¹²¹⁵ OECD, "The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector", o.c. p. 22; High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI", o.c., p. 16.

transparency thereof to which certain consumer insurance contracts are subject already meet some of the requirements of the GDPR (e.g. transparency, data minimisation).

Finally, the current legal safety net cast by the GDPR can only be considered as a baseline. Data controllers and processors will need to do more to meet the standards of the human-centred approach recommended by the European Commission report on trustworthy artificial intelligence.

5.1.2. Data Portability

As discussed in the previous chapters of this study, there are no absolute answers yet to questions related to data portability on a European level. For example, there is no definition of “ownership” at the EU level.¹²¹⁶ Moreover, several difficulties arise due to the particularities of data, namely the fact that data is limitless and non-rivalrous: someone else can use the data without harm to the use of the original data.¹²¹⁷ This must also be regulated at the EU level.

5.1.3. Control of AI-Technologies/Algorithms

The (mis)use of AI/algorithms by insurance companies and distributors can result in several consequences such as:

- breaching legal rules, such as insurance, consumer and data protection rules;
- insurance companies and distributors and their supervisory authorities neglecting to or not flagging, controlling or not being able to explain the decisions or breaches;¹²¹⁸
- a severe and unfair impact on an insured/beneficiary/victims or customer (access to insurance, fraud ...);
- segmentation based on correlation rather than causation;
- the question who can/should be held liable if an AI-tool/technique, in particular without human involvement, is taking decisions resulting in breaches of the law.¹²¹⁹

It has also been emphasised that an AI governance and supervision framework is key for the further introduction and use of AI.¹²²⁰ Depending on the general AI governance and supervision framework, and given the technicalities of insurance, additional or deviating supervision and rules/guidelines for the design and the use of AI-technologies in insurance might be necessary, as well as on if/how the independent functions in the insurance company should deal with this matter. With regard to the insurance sector, the following issues should be considered:

¹²¹⁶ V. JANEČEK, “Ownership of personal data in the Internet of Things”, *Computer law & Security Review* 2018, p. 1041.

¹²¹⁷ EC Joint Research Centre, “The economics of ownership, access and trade in digital data”, JRC Digital Economy Working Paper 2017-01, p. 13; Bird & Bird, “Big Data & Issues & Opportunities: Data Ownership”, 2019, p. 1 available at <https://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-opportunities-data-ownership> accessed 24 July 2020.

¹²¹⁸ This problem is often referred to as the “black-box problem”; See for example: T. CALDERS and A. VAN DE VIJVER, “Vrij gesteld 171.”, *T.F.R.* 2020, p. 614; EIOPA, “European Commission’s Digital Finance Strategy Consultation – EIOPA’s Draft Response”, o.c.; European Commission, “White Paper on Artificial Intelligence - A European approach to excellence and trust”, o.c., p. 12, 23-24; K. VRANCKAERT et al, “Ethische principes en (niet-) bestaande juridische regels voor AI. Een praktische gids”, o.c., p. 54 and 57; High-level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, o.c., p. 13.

¹²¹⁹ EIOPA, “European Commission’s Digital Finance Strategy Consultation – EIOPA’s Draft Response”, o.c., p. 3 and 52; High-level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, o.c., p. 19-20; K. VRANCKAERT, J. DE BRUYNE, T. GILS, E. WAUTERS, B. BÉNICHOU and P. VALCKE, “Ethische principes en (niet-) bestaande juridische regels voor AI. Een praktische gids”, o.c., p. 106-108.

¹²²⁰ EIOPA, “European Commission’s Digital Finance Strategy Consultation – EIOPA’s Draft Response”, o.c., p. 1, 3, 13, 14, 49-52; European Commission, “White Paper on Artificial Intelligence - A European approach to excellence and trust”, o.c., p. 12, 23 and 24; European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the European Union”, p. 11 available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0591&from=EN>; High-level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, o.c., p. 16 and 23.

- Which supervision rules for the implementation and functioning of AI do we need for insurance companies/intermediaries?
 - Which *a priori* controls (e.g. pre-approval,¹²²¹ certification,¹²²² an AI Impact Assessment,¹²²³ ...) are needed for the launch of an AI-system? Are they compatible with the European prohibition of *a posteriori* systemic control of tariffs, insurance conditions and contractual documents?
 - Which *ex post* controls (e.g. data retention requirements, periodic reporting requirements, AI Impact Assessment,¹²²⁴ audit requirements,¹²²⁵ ...) are required to monitor the design, use, functioning and development of the AI-technologies?
- Which (supervisory) authority can act as a supervisor (e.g. the NBB/FSMA, the Data Protection Authority, a new multidisciplinary supervisor, ...)?
- How can “double supervision” be avoided?
- How can supervisors efficiently and effectively monitor the AI-technologies used by insurance companies and distributors (e.g. risk-based supervision, cooperation between different supervisors, ...)?¹²²⁶
- Which governance framework (e.g. policies and procedures, training requirements,¹²²⁷ designated AI officer,¹²²⁸ ...) should be imposed?

In this regard, an inspiring example can be found in the anti-money laundering legal framework. Insurance companies that are subject to the Act of 18 September 2017 on the prevention of money laundering and the financing of terrorism (AML/CFT Act)¹²²⁹ must:

- Internally validate their AML/CFT screening tools/algorithms prior to launching the screening tools/algorithms;¹²³⁰
- Submit an annual report, questionnaire and risk assessment to their supervisor¹²³¹ (including amongst other things information about the screening tools/algorithms and the screening results);¹²³²
- Archive certain important documents for 10 years;¹²³³

¹²²¹ For example, a process similar to the approval process for critical outsourcing?. See Art. 92 of the Supervision Act.

¹²²² High-level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, o.c., p. 23.

¹²²³ K. VRANCKAERT et al, “Ethische principes en (niet-) bestaande juridische regels voor AI. Een praktische gids”, o.c., p. 65 and 80.

¹²²⁴ K. VRANCKAERT et al, “Ethische principes en (niet-) bestaande juridische regels voor AI. Een praktische gids”, o.c., p. 65 and 80.

¹²²⁵ High-level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, o.c., p. 20.

¹²²⁶ BEUC, “The Use of Big Data and Artificial Intelligence in Insurance”, o.c., p. 5.

¹²²⁷ High-level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, o.c., p. 16 and 23.

¹²²⁸ K. VRANCKAERT et al, “Ethische principes en (niet-) bestaande juridische regels voor AI. Een praktische gids”, o.c., p. 113; High-level Expert Group on Artificial Intelligence, “Ethics Guidelines for Trustworthy AI”, o.c., p. 23.

¹²²⁹ Belgian insurance companies, EU insurance companies and insurance companies of a third country, which are authorized to carry out in Belgium the life insurance activities mentioned in Annex II Supervisory Act.

¹²³⁰ Art. 17 of the Regulation of the National Bank of Belgium regarding the prevention of money laundering and the financing of terrorism; NBB’s comments and recommendations regarding ongoing due diligence and detection of atypical facts and transactions, section 1.3.2. available at <https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/customer-and-transaction-d-15>.

¹²³¹ For insurance companies subject to the AML Act: the NBB. For insurance intermediaries subject to the AML Act: the FSMA.

¹²³² Art. 3, 3° and 7 of the Regulation of the National Bank of Belgium regarding the prevention of money laundering and the financing of terrorism; NBB’s comments and recommendations regarding the reporting by financial institutions available at <https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/supervision-nbb/reporting-0?language=de>.

¹²³³ Art. 60 AML/CFT Act.

- Have a procedure in place for the screening tools/algorithms they use and on the analysis of the alerts that the screening tools/algorithms generate;¹²³⁴
- Appoint an anti-money laundering compliance officer (AMLCO) who must, amongst other things, perform a (final) review of a “suspicious activity report” resulting from an alert of an AML/CFT screening tool/algorithm;¹²³⁵
- Periodically review the effectiveness of the AML/CFT tools/algorithms, in particular, the adequacy of the configuration of the tool/algorithm and address the deficiencies as soon as possible;¹²³⁶
- Train their staff on AML/CFT matters;¹²³⁷
- Take into consideration the legal requirements, comments and guidance regarding amongst other things the parameters of the AML/CFT screening tools/algorithms.¹²³⁸

5.1.4. Financial/Conduct of Business Supervision

AI-systems can have an undesired/unknown impact on the solvency of insurance companies. The OECD suggests supervisors to establish regulatory sandboxes and innovation hubs to spur innovation in the financial sector by establishing platforms to enable experiments with their technology and relaxing some of the regulatory requirements within the platform. The regulatory sandbox approach intentionally creates a space for insurance technology to be experimented in a different regulatory regime than the regular applicable regulatory requirements. This supports better understanding of when technologies are deemed successful and scalable and how they will be graduated into the regular regulatory framework if this is the case.¹²³⁹

In relation to this, EIOPA has published a SupTech Strategy in which the use of technology by supervisors could deliver innovative and efficient supervisory solutions that will support a more effective, flexible and responsive supervisory system.¹²⁴⁰

5.2. Shortcomings Regarding ‘Impact-Related’ Concerns

A preliminary and general policy question relates to what kind of ‘fairness’ and ‘solidarity’ our society needs to strive for. Closely related is the question how this fairness and solidarity should be realised, taking into account the specificity of private insurance. Although the impact of AI on accessibility, discrimination and fairness in insurance is not clear yet and anyway not specific to AI, the following modifications could be assessed in the broader perspective of the comparative law analysis. They relate to insurance contract law (part 5.2.1) as well as conduct of business rules (part 5.2.2.).

¹²³⁴ Art. 8, §2, 1° AML/CFT Act.

¹²³⁵ Art. 9, §2, 45, 46 and 49 AML/CFT Act.

¹²³⁶ NBB’s comments and recommendations regarding ongoing due diligence and detection of atypical facts and transactions, section 1.3.2. available at <https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/customer-and-transaction-d-15/>

¹²³⁷ Art. 8 §2 3° AML/CFT Act; NBB’s comments and recommendations regarding training and education of staff, available at <https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/organisation-and-internal-16>.

¹²³⁸ Art. 17 of the Regulation of the National Bank of Belgium regarding the prevention of money laundering and the financing of terrorism; NBB’s comments and recommendations regarding ongoing due diligence and detection of atypical facts and transactions, section 1.3.2. available at <https://www.nbb.be/en/financial-oversight/combating-money-laundering-and-financing-terrorism/customer-and-transaction-d-15>.

¹²³⁹ OECD, “The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector”, o.c., p. 22.

¹²⁴⁰ EIOPA, “Supervisory Technology Strategy”, 2020 available at https://www.eiopa.europa.eu/content/supervisory-technology-strategy_en.

5.2.1. Insurance Contract Law

Several questions arise with regard to insurance contract law. The most important ones being:

- Should other chronic diseases be included under “the right to be forgotten” in outstanding balance insurance contracts, and/or should the scope of this “right to be forgotten” be extended to health insurance contracts?¹²⁴¹
- Should the rules on the duty of disclosure of the policyholder (Article 58 Insurance Act) be modified? Does the obligation of spontaneous disclosure need to be repealed?
- Should the scope of the specific rules on (non employment related) health insurance (Articles 201-211 Insurance Act) be extended to all types of health and accidents insurance contracts?

There is also a need to clarify and reconsider the Act of 10 December 2020 prohibiting data collected by internet connected devices (Articles 46/1-46/3 Insurance Act).

There remains major uncertainty as to the precise scope and interpretation of Act of 10 December 2020¹²⁴² inserting the Articles 46/1 until 46/3 in the Insurance Act. In particular, it is not clear whether the use of data collected by internet connected devices applied and assessed by a doctor (e.g. fibricheck a medically validated app that monitors heart rate) fall under the scope of the prohibition.

The scope of this regulation is limited to individual life insurance contracts and certain health insurance contracts as defined in Article 201, §1 Insurance Act. Excluded from its scope are for example accidents insurance. Consequently, the question arises whether there is a risk of a violation of the prohibition on discrimination in the Articles 10 and 11 of the Belgian Constitution.

This new legislation also raises policy questions. Is an apparently total prohibition, for instance, appropriate? Persons with a “healthy” lifestyle cannot obtain a lower premium or better insurance conditions? Moreover, is the use of these devices as a preventive measure not beneficial for society in general, as they might lower the cost of healthcare?

It could also be beneficial to provide supervisors and/or public authorities the power to investigate whether certain types of personal data should not be used in risk assessments by insurers in case of evidence of consumer and data protection concerns or dangers of unfair discrimination.

5.2.2. Conduct of Business Rules

The most relevant question regarding the conduct of business rules is whether the rules on the information and the provision prohibiting the use of segmentation criteria unless objectively justified (Art. 42-46 Insurance Act) should be extended to other insurance contracts? For instance, should the scope of these provisions be extended to all health and accident insurance contracts concluded with consumers, to all consumer insurance contracts or to all insurance contracts? Moreover, there is a need to clarify and reconsider the scope of the newly adopted rules regarding segmentation with personal data regarding health and lifestyle collected by internet connected devices (Art. 46/1-46/3 Insurance Act) (part 5.2.1)

Furthermore, insurance distributors should pay specific attention to the duty of care (Art. 279, Art. 284 and Art. 296 Insurance Act), the duty to advise (Art. 284 and Art. 296 Insurance Act) and the rules regarding product development (Art. 288 Insurance Act) when using and/or developing AI

¹²⁴¹ See General Policy Note of the Minister of Economy (in charge for insurance), 4 November 2020, Parl. Ch. Doc 55, 1580/013, p. 14.

¹²⁴² Act of 10 December 2020 amending the Act of 4 April 2014 on Insurances (Wet van 10 december 2020 tot wijziging van de wet van 4 april 2014 betreffende de verzekeringen), MB 15 januari 2021.

tools supporting their activities. The risk exists that AI algorithms/tools (unknowingly) breach the aforementioned rules (e.g. by offering a product to the customer that is not consistent with the customer's demands and needs.). It is advisable to insert a provision requiring insurance distributors to be able to explain why a certain decision/outcome is in line with the above obligations (i.e. to avoid liability).

6. Overview of the Identified Gaps With regard to AI and Insurances

There are several specific gaps related to AI and insurance which may need further examination. These are on the one hand 'operational-related' gaps (part 6.1.) and on the other hand 'impact-related' gaps (part 6.2.).

6.1. 'Operational-Related' Gaps

Several questions arise with regard to the application of the GDPR such as:

- What is the (appropriate) legal ground for processing personal data of the (potential) policyholder, insured and/or third parties, in particular for special categories of personal data, among which health data in the broad sense including lifestyle data? The legal ground of explicit consent of the data subject? Other legal ground(s)?
- To what extent is the use of AI and profiling allowed without human involvement in insurance? If so, on which legal ground (for the purposes of insurance underwriting, claims-handling and fraud detection) and how applying Article 22 GDPR?
- How guaranteeing the application of some fundamental principles in the GDPR among which the principles of accuracy (also issue of correlation and causation), transparency and data minimisation?

A fundamental issue relates to data ownership (i.e. who owns the data) and the regulation of data portability.

Several other gaps relate to the control of AI-technologies and algorithms, which will require additional research in the follow-up reports.

- Depending on the general AI governance and supervision framework and given the technicalities of insurance, for instance, additional or deviating supervision and rules/guidelines for the design and the use of AI-technologies in insurance might be necessary, as well as on if/how the independent functions in the insurance company should deal with this matter. Should this be regulated under the governance rules (principle of home country control) and/or as a conduct of business rule?
- What is the impact on the solvency of insurance companies and how to set up a more effective, flexible and responsive supervisory system?
- Should a provision be inserted in part 6 of the Insurance Act requiring insurance distributors to be able to explain why a certain decision/outcome is in line with the duty of care (Art. 279, Art. 284 and Art. 296 Insurance Act), the duty to advise (Art. 284 and Art. 296 Insurance Act) and the rules regarding product development (Art. 288 Insurance Act) when using and/or developing AI tools supporting their activities?

6.2. 'Impact-Related' Gaps

There are also several impact-related gaps. A preliminary policy question, for instance, is what kind of 'fairness' and 'solidarity' our society strives for? And how can this fairness and solidarity be realised, taking into account the specificity of private insurance?

The following modifications could be assessed in the broader perspective of the comparative law analysis.

- Should other chronic diseases be included under “the right to be forgotten” in outstanding balance insurance contracts, and/or should the scope of this “right to be forgotten” be extended to health insurance contracts?
- Should the rules on the duty of disclosure of the policyholder be modified (Article 58 Insurance Act)? Does the obligation of spontaneous disclosure need to be repealed?
- Should the scope of the specific rules on (non-employment related) health insurance be extended (Articles 201-2011 Insurance Act) to all types of health and accidents insurance contracts?
- Is there a need to reconsider the Act of 10 December 2020 prohibiting data collected by internet connected devices (Article 43/1-46/2 Insurance Act), and if so how?
- Should the rules on the information of the applied segmentation criteria and the provision prohibiting the use of segmentation criteria unless objectively justified (Art. 42-46 Insurance Act) be extended to other insurance contracts?
- Should the list of factors enlisted in the anti-discrimination laws be extended?

CHAPTER 6 – CONCLUSIONS

In this report, we analysed the legal framework under Belgian law with regard to intellectual property and trade secrets, consumer protection and competition law, as well as diverse fields of ICT law, including AI-safety and cybersecurity, data sharing, the eIDAS Regulation, e-Commerce and insurance legislation. We aimed to identify the regulatory gaps that are caused by the use of AI-systems. It became clear that the legal system has shown considerable resilience in the face of the increased use of AI-systems. However, the reliance on AI-systems does sometimes create issues in which the law requires clarification or where legal rules, despite the intention to remain technology-neutral, were not. When this is the case, legal convergence must follow technological convergence.

In this study, we have identified the abovementioned gaps and provided some suggestions to answer these questions. In order to resolve these questions and to come to recommendations, however, further research is needed and will be conducted. Therefore, in a follow-up to this study, we will conduct a comparative analysis of the approaches taken by Belgium's neighbouring countries – the Netherlands, France, Germany and the United Kingdom. This comparative research will be used for our recommendations, that will form the object of a third study in which we will attempt to provide normative recommendations.

Contributing authors (alphabetical): Jeffrey Amankwah, Jan De Bruyne, Alexandre de Streel, Thomas Gils, Daphné Hof, Hervé Jacquemin, Michael Lognoul, Victoria Ruelle, Nele Stroobants, Jozefien Vanherpe, Caroline Van Schoubroeck, Peggy Valcke & Koen Vranckaert








Study on Potential Policy Measures to Promote the Uptake and the Use of AI in Belgium in Specific Economic Domains

Part 2: Legal Comparative Analysis



FPS Economy, S.M.E.s, Self-employed and Energy

Rue du Progrès 50
1210 Brussels
Business number : 0314.595.348

-  0800 120 33 (free call)
-  facebook.com/SPFEco
-  [@SPFEconomie](https://twitter.com/SPFEconomie)
-  linkedin.com/company/fod-economie
-  instagram.com/spfecoo
-  youtube.com/user/SPFEconomie
-  <https://economie.fgov.be>

Publisher:
Séverine Waterbley
Chairman of the Board Committee
Rue du Progrès 50
1210 Brussels

Internet version

Disclaimer: this study has been executed by a contractor external to the FPS Economy, S.M.E.s, Self-employed and Energy. The opinions reflected in the study are the author's own and do not form any indication of the position of the FPS Economy or the Belgian State regarding the subject of the study. The FPS Economy cannot be held responsible for any inaccuracies as to the information contained in the study.

CHAPTER 1 – PRELIMINARY CONSIDERATIONS AND OUTLINE STUDY	13
CHAPTER 2 – INTELLECTUAL PROPERTY (WP 2).....	16
Questionnaire the Netherlands	16
1. Which authorities are competent for intellectual property?.....	16
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	16
3. Discussion of documents	16
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	16
3.1.1. If yes, briefly list these proposals.....	16
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	16
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	17
Questionnaire France	17
1. Which authorities are competent for intellectual property?.....	17
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	17
3. Discussion of documents	17
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	17
3.1.1. If yes, briefly list these proposals.....	17
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	19
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	19
3.2.1. Proposal 1 – CSPLA: efficiency and budgetary aspects.....	19
3.2.2. Proposal 2 – CSPLA: efficiency and budgetary aspects.....	20
3.2.3. Proposal 3 – INPI: efficiency and budgetary aspects.....	20
Questionnaire the United Kingdom.....	21
1. Which authorities are competent for intellectual property?.....	21
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	21
3. Discussion of documents	21
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	21
3.1.1. If yes, briefly list these proposals.....	21
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	23
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	23
3.2.1. Proposal 1 – MOPP: efficiency and budgetary aspects.....	23
3.2.2. Proposal 2 – Call for Views AI & IP: efficiency and budgetary aspects.....	24
Questionnaire Germany	24
1. Which authorities are competent for intellectual property?.....	24
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	24
3. Discussion of documents	25
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	25
3.1.1. If yes, briefly list these proposals.....	25
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	25
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	25
3.2.1. Proposal 1 – Text and data mining: efficiency and budgetary aspects.....	25
CHAPTER 3 – CONSUMER AND MARKET(WP 3)	27
WP 3.1. COMPETITION LAW	27
Questionnaire the Netherlands	27

1. Which authorities are competent for competition law?	27
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	27
3. Discussion of documents	27
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	27
3.1.1. If yes, briefly list these proposals.....	27
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	27
Questionnaire France	27
1. Which authorities are competent for competition law?	27
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	27
3. Discussion of documents	28
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	28
3.1.1. If yes, briefly list these proposals.....	28
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	28
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	28
3.2.1. Proposal 1 – Investigative powers: efficiency and budgetary aspects	28
3.2.2. Proposal 2 – Ensuring expertise: efficiency and budgetary aspects	28
3.2.3. Proposal 3 – Liability: efficiency and budgetary aspects.....	29
3.2.4. Proposal 4 – Anti-competitive behaviour: efficiency and budgetary aspects.....	29
Questionnaire the United Kingdom.....	30
1. Which authorities are competent for competition law?	30
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	30
3. Discussion of documents.....	30
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	30
3.1.1. If yes, briefly list these proposals.....	30
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	31
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	31
3.2.1. Proposal 1 – Collaboration: efficiency and budgetary aspects	31
3.2.2. Proposal 2 – Transparency: efficiency and budgetary aspects	31
3.2.3. Proposal 3 – Standards: efficiency and budgetary aspects.....	32
3.2.4. Proposal 4 – Broaden obligations: efficiency and budgetary aspects.....	33
3.2.5. Proposal 5 – Investigative powers: efficiency and budgetary aspects	33
3.2.6. Proposal 6 – Audits and monitoring: efficiency and budgetary aspects	34
3.2.7. Proposal 7 – Testing algorithms: efficiency and budgetary aspects	34
Questionnaire Germany	34
1. Which authorities are competent for competition law?	34
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	35
3. Discussion of documents	35
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	35
3.1.1. If yes, briefly list these proposals.....	35
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	35
WP 3.2. CONSUMER LAW	35
Questionnaire the Netherlands	35
1. Which authorities are competent for consumer law?	35
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	35
3. Discussion of documents	36

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	36
3.1.1. If yes, briefly list these proposals.....	36
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	36
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	36
3.2.1. Proposal 1 – Information obligations: efficiency and budgetary aspects.....	36
Questionnaire France	36
1. Which authorities are competent for consumer law?	36
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	37
3. Discussion of documents	37
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	37
3.1.1. If yes, briefly list these proposals.....	37
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	37
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	37
Questionnaire the United Kingdom	37
1. Which authorities are competent for consumer law?	37
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	37
3. Discussion of documents	38
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	38
3.1.1. If yes, briefly list these proposals.....	38
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	38
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	38
Questionnaire Germany	38
1. Which authorities are competent for consumer law?	38
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	38
3. Discussion of documents	38
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	38
3.1.1. If yes, briefly list these proposals.....	38
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	39
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	39
CHAPTER 4 – TELECOMMUNICATION AND INFORMATION SOCIETY (WP 4).....	40
WP 4.1. AI SAFETY AND CYBERSECURITY	40
Questionnaire the Netherlands	40
1. Which authorities are competent for safety and cybersecurity?	40
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	40
3. Discussion of documents	43
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	43
3.1.1. If yes, briefly list these proposals.....	43
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	49
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	49
3.2.1. Proposal 1 – Guidance to regulators regarding the application to their rules with regard to AI: efficiency and budgetary aspects.....	49

3.2.2. Proposal 2 – Setting up a standards committee for AI in the national standardisation organisation: efficiency and budgetary aspects.....	50
3.2.3. Proposal 3 – Setting up a Digital Trust Center: efficiency and budgetary aspects	50
3.2.4. Proposal 4 – Facilitating the testing of self-driving cars and other AI systems: efficiency and budgetary aspects	51
3.2.5. Proposal 5 – Investing in research projects: efficiency and budgetary aspects....	51
3.2.6. Proposal 6 – Awareness building through (secondary) education: efficiency and budgetary aspects	52
3.2.7. Proposal 7 – Principles for the use of artificial intelligence in the financial sector (and other sectors as well): efficiency and budgetary aspects.....	52
3.2.8. Proposal 8 – Supporting EU regulatory initiatives such as the Cybersecurity Act, the Radio Equipment Directive and European regulatory initiatives: efficiency and budgetary aspects	53
3.2.9. Proposal 9 – An act prohibiting the control of telecommunications infrastructure: efficiency and budgetary aspects	53
3.2.10. Proposal 10 – A Human Rights Impact Assessment: efficiency and budgetary aspects.....	54
Questionnaire France	54
1. Which authorities are competent for safety and cybersecurity?	54
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	55
3. Discussion of documents	60
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	60
3.1.1. If yes, briefly list these proposals.....	60
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	61
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	61
3.2.1. Proposal 1 – Creation of an Academic Centre on Artificial Intelligence: efficiency and budgetary aspects	61
3.2.2. Proposal 2 – Empowering the LNE to develop testing and certification methods for AI systems: efficiency and budgetary aspects	61
3.2.3. Proposal 3 – The creation of an AI foundation: efficiency and budgetary aspects	62
3.2.4. Proposal 4 – Specific sectoral platforms for AI: efficiency and budgetary aspects	62
3.2.5. Proposal 5 – Promoting specific design principles for autonomous vehicles: efficiency and budgetary aspects	63
3.2.6. Proposal 6 – Clarifying the traffic code for autonomous vehicles: efficiency and budgetary aspects	63
3.2.7. Proposal 7 – Developing a platform for the testing, qualification and certification of AI systems: efficiency and budgetary aspects.....	64
3.2.8. Proposal 8 – Developing a software platform for AI: efficiency and budgetary aspects.....	64
3.2.9. Proposal 9 – Developing a network of platforms for security and cybersecurity: efficiency and budgetary aspects	64
3.2.10. Proposal 10 – The creation of a one-stop shop for information relating to AI: efficiency and budgetary aspects	65
3.2.11. Proposal 11 – Facilitating dialogue between regulators: efficiency and budgetary aspects.....	65
3.2.12. Proposal 12 – Implementing sector-specific policies around major challenges: efficiency and budgetary aspects	66
3.2.13. Proposal 13 – The creation of a Joint Centre for Excellence at state level: efficiency and budgetary aspects	66
3.2.14. Proposal 14 – Appointing a body of experts for the auditing of algorithms: efficiency and budgetary aspects	67
3.2.15. Proposal 15 – Include ethics and law in education programs: efficiency and budgetary aspects.....	67

3.2.16. Proposal 16 – Reforming the Civil Code to allow for hardship: efficiency and budgetary aspects	68
3.2.17. Proposal 17 – Issuing guidance documents by regulators on how to apply their regulations and supervisory role to AI: efficiency and budgetary aspects	68
3.2.18. Proposal 18 – Funding research and initiatives in cybersecurity and the creation of a Cyber Campus: efficiency and budgetary aspects.....	69
3.2.19. Proposal 19 – Create a control cell for digital technologies: efficiency and budgetary aspects	69
Questionnaire the United Kingdom	70
1. Which authorities are competent for safety and cybersecurity?	70
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	71
3. Discussion of documents	75
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	75
3.1.1. If yes, briefly list these proposals.....	75
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	76
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	76
3.2.1. Proposal 1 – Setting up advisory bodies such as the AI Council, the CDEI and the Alan Turing Institute: efficiency and budgetary aspects	76
3.2.2. Proposal 2 – Setting up a separate Office for AI: efficiency and budgetary aspects	76
3.2.3. Proposal 3 – Guidance by independent regulators: efficiency and budgetary aspects.....	77
3.2.4. Proposal 4 – Guidelines on AI procurement: efficiency and budgetary aspects ..	77
3.2.5. Proposal 5 – Self-assessment tools: efficiency and budgetary aspects.....	78
3.2.6. Proposal 6 – Draft Online Safety Bill: efficiency and budgetary aspects.....	78
3.2.7. Proposal 7 – An Automated and Electric Vehicles Act: efficiency and budgetary aspects.....	79
Questionnaire Germany	79
1. Which authorities are competent for safety and cybersecurity	79
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	80
3. Discussion of documents	85
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	85
3.1.1. If yes, briefly list these proposals.....	85
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	85
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	85
3.2.1. Proposal 1 – Establishing Centres of Excellence on AI and develop Centres of Excellence: efficiency and budgetary aspects	85
3.2.2. Proposal 2 – A Standardisation Roadmap: efficiency and budgetary aspects	85
3.2.3. Proposal 3 – Establishment of a Data Ethics Commission: efficiency and budgetary aspects	86
3.2.4. Proposal 4 – Guidance on the use of artificial intelligence and the supervision of artificial intelligence: efficiency and budgetary aspects.....	87
3.2.5. Proposal 5 – Establishing a risk-based classification system for AI systems: efficiency and budgetary aspects	87
3.2.6. Proposal 6 – Sector-specific recommendations (e.g. automated driving): efficiency and budgetary aspects	88
3.2.7. Proposal 7 – Adapting the NIS Act in the same way as the IT-Security Act 2.0: efficiency and budgetary aspects	88
3.2.8. Proposal 8 – Adopting laws such as the Netzwerkdurchsetzungsgesetz: efficiency and budgetary aspects	89
WP 4.2. DATA ECONOMY	89

Questionnaire the Netherlands	89
1. Which authorities are competent for data economy?	89
2. Have the authorities under 1. published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	89
3. Discussion of documents	90
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	90
3.1.1. If yes, briefly list these proposals.....	90
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	90
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	90
Questionnaire France	91
1. Which authorities are competent for data economy?	91
2. Have the authorities under 1. published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	91
3. Discussion of documents	91
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	91
3.1.1. If yes, briefly list these proposals.....	91
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	91
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	92
3.2.1. Proposal 1- Access to data: efficiency and budgetary aspects	92
Questionnaire the United Kingdom	92
1. Which authorities are competent for data economy?	92
2. Have the authorities under 1. published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	93
3. Discussion of documents	93
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	93
3.1.1. If yes, briefly list these proposals.....	93
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	93
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	94
Questionnaire Germany	94
1. Which authorities are competent for data economy?	94
2. Have the authorities under 1. published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	95
3. Discussion of documents	95
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	95
3.1.1. If yes, briefly list these proposals.....	95
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	95
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	96
3.2.1. Proposal 1- Access to data: efficiency and budgetary aspects	96
WP 4.3. ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR ELECTRONIC TRANSACTIONS (EIDAS REGULATION)	97
WP 4.4. E-COMMERCE	97
Questionnaire the Netherlands	97
1. Which authorities are competent for e-commerce?	97
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	97
3. Discussion of documents	97
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	97

3.1.1. If yes, briefly list these proposals.....	97
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	97
Questionnaire France	97
1. Which authorities are competent for e-commerce.....	98
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	98
3. Discussion of documents	98
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	98
3.1.1. If yes, briefly list these proposals.....	98
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	99
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	99
3.2.1. Proposal 1 – Removal unlawful content: efficiency and budgetary aspects	99
Questionnaire the United Kingdom	100
1. Which authorities are competent for e-commerce?.....	100
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	100
3. Discussion of documents	100
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	100
3.1.1. If yes, briefly list these proposals.....	100
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	101
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	101
3.2.1. Proposal 1 – Responsibilities: efficiency and budgetary aspects.....	101
3.2.2. Proposal 2 – Technological solutions: efficiency and budgetary aspects	102
Questionnaire Germany	103
1. Which authorities are competent for e-commerce?.....	103
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	104
3. Discussion of documents	104
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	104
3.1.1. If yes, briefly list these proposals.....	104
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	104
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	104
3.2.1. Proposal 1 – Notification procedure: efficiency and budgetary aspects	104
3.2.2. Proposal 2 – Block/remove content: efficiency and budgetary aspects.....	105
CHAPTER 5 – INSURANCES (WP 5)	107
Questionnaire the Netherlands	107
1. Which authorities are competent for insurances?	107
2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?	107
3. Discussion of documents	108
3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?	108
3.1.1. If yes, briefly list these proposals.....	108
3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....	110
3.2. Discussion of relevant substantive proposals identified under 3.1.1.	110
3.2.1. Proposal 1 – Establishment of an InnovationHub and a Regulatory Sandbox: efficiency and budgetary aspects	110
3.2.2. Proposal 2 – Compliance-by-design and appropriate governance: efficiency and budgetary aspects.....	111

- 3.2.3. Proposal 3 – Use specific criteria and evaluation methods for model selection: efficiency and budgetary aspects111
- 3.2.4. Proposal 4 – Definition of data quality standards and controls: efficiency and budgetary aspects112
- 3.2.5. Proposal 5 – AI Policy and Communication: efficiency and budgetary aspects .113
- 3.2.6. Proposal 6 – Ensure control and accountability: efficiency and budgetary aspects115
- 3.2.7. Proposal 7 – Implementation of ethical and fairness standards, procedures and controls (e.g. “human-in-the-loop”) in AI tools/techniques, with a special attention for (unintentional) biases, discrimination and social acceptance: efficiency and budgetary aspects.....116
- 3.2.8. Proposal 8 – Training and expertise requirements: efficiency and budgetary aspects).....117
- 3.2.9. Proposal 9 – Explainability requirements: efficiency and budgetary aspects118
- 3.2.10. Proposal 10 – Risk and impact assessments: efficiency and budgetary aspects)119
- 3.2.11. Proposal 11 – Establish validation procedures: efficiency and budgetary aspects)119
- 3.2.12. Proposal 12 – Outsourcing requirements: efficiency and budgetary aspects ..120
- 3.2.13. Proposal 13 – Legal basis for the processing of health data for insurance purposes: efficiency and budgetary aspects.....121
- Questionnaire France122
 - 1. Which authorities are competent for insurances?122
 - 2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?122
 - 3. Discussion of documents123
 - 3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?123
 - 3.1.1. If yes, briefly list these proposals.....123
 - 3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....128
 - 3.2. Discussion of relevant substantive proposals identified under 3.1.1.128
 - 3.2.1. Proposal 1 – Establishment of a multidisciplinary Fintech Innovation Unit: efficiency and budgetary aspects128
 - 3.2.2. Proposal 2 – Definition of appropriate governance of algorithms: efficiency and budgetary aspects129
 - 3.2.3. Proposal 3 - Data quality requirements and verification of data use: efficiency and budgetary aspects129
 - 3.2.4. Proposal 4 – Explainability requirements and methods: efficiency and budgetary aspects.....130
 - 3.2.5. Proposal 5 – Outsourcing requirements, including an ex-ante risk assessment: efficiency and budgetary aspects131
 - 3.2.6. Proposal 6 – Mutualisation and standardisation: efficiency and budgetary aspects131
 - 3.2.7. Proposal 7 – Risk assessment methodologies: efficiency and budgetary aspects131
 - 3.2.8. Proposal 8 – Govern human intervention: efficiency and budgetary aspects132
 - 3.2.9. Proposal 9 – Audit methodologies: efficiency and budgetary aspects133
- Questionnaire the United Kingdom133
 - 1. Which authorities are competent for insurances?133
 - 2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?133
 - 3. Discussion of documents134
 - 3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?134
 - 3.1.1. If yes, briefly list these proposals.....134
 - 3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....137

- 3.2. Discussion of relevant substantive proposals identified under 3.1.1.137
 - 3.2.1. Proposal 1 – Undertake data discrimination audits: efficiency and budgetary aspects.....137
 - 3.2.2. Proposal 2 – Review third party data and software suppliers: efficiency and budgetary aspects138
 - 3.2.3. Proposal 3 – Make privacy notices more accessible: efficiency and budgetary aspects.....138
 - 3.2.4. Proposal 4 – Reconsider the types of data that should not be used in risk assessments: efficiency and budgetary aspects.....139
 - 3.2.5. Proposal 5 – Innovation Hub: efficiency and budgetary aspects: efficiency and budgetary aspects139
 - 3.2.6. Proposal 6 – Regulatory sandbox: efficiency and budgetary aspects140
 - 3.2.7. Proposal 7 – Government intervention to avoid uninsurability: efficiency and budgetary aspects141
 - 3.2.8. Proposal 8 – Data storage standards: efficiency and budgetary aspects142
 - 3.2.9. Proposal 9 – Establish clear lines of accountability: efficiency and budgetary aspects.....143
 - 3.2.10. Proposal 10 – Fair pricing framework: efficiency and budgetary aspects143
 - 3.2.11. Proposal 11 – Signposting service: efficiency and budgetary aspects144
 - 3.2.12. Proposal 12 – Require firms to offer a renewal price that is no higher than the equivalent new business price for the customer through the same sales channel: efficiency and budgetary aspects144
 - 3.2.13. Proposal 13 – Legal basis for the processing of health data in private health insurance: efficiency and budgetary aspects145
- Questionnaire Germany146
 - 1. Which authorities are competent for insurances?146
 - 2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?146
 - 3. Discussion of documents147
 - 3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?147
 - 3.1.1. If yes, briefly list these proposals.....147
 - 3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated.....151
 - 3.2. Discussion of relevant substantive proposals identified under 3.1.1.151
 - 3.2.1. Proposal 1 – Addressing providers that have not been regulated to date and making sure that the current legal framework is applicable to them; adapting outsourcing systems: efficiency and budgetary aspects151
 - 3.2.2. Proposal 2 – Re-evaluate the concept of systemic importance: efficiency and budgetary aspects152
 - 3.2.3. Proposal 3 – Test scenario an no black box explanation: efficiency and budgetary aspects.....153
 - 3.2.4. Proposal 4 – Traffic light system and public availability of data protection impact assessments: efficiency and budgetary aspects.....154
 - 3.2.5. Proposal 5 – Adequate monitoring and transparency mechanisms to tackle discrimination: efficiency and budgetary aspects.....154
 - 3.2.6. Proposal 6 – Only use data that is actually relevant for risk assessment: efficiency and budgetary aspects155
 - 3.2.7. Proposal 7 – Responsibility: efficiency and budgetary aspects.....156
 - 3.2.8. Proposal 8 – Provide alternative products: efficiency and budgetary aspects ...156
 - 3.2.9. Proposal 9 – Hub-and-spoke concept: efficiency and budgetary aspects157
 - 3.2.10. Proposal 10 – Providing processes and criteria to ensure data quality: efficiency and budgetary aspects157
 - 3.2.11. Proposal 11 – Cooperation with financial supervisors and data protection authorities: efficiency and budgetary aspects.....158
 - 3.2.12. Proposal 12 – Creating a consumer-centred data portal: efficiency and budgetary aspects158
 - 3.2.13. Proposal 13 – Utilising technical options for using Big data and AI with anonymised data: efficiency and budgetary aspects159

3.2.14. Proposal 14 – Specific legal basis for automated individual decision-making, including profiling, in the context of providing services pursuant to an insurance contract: efficiency and budgetary aspects159

3.2.15. Proposal 15 – Stringent requirements and limitations on the use of data for personalised risk assessment: efficiency and budgetary aspects160

CHAPTER 6 – CONCLUSIONS161

CHAPTER 1 – PRELIMINARY CONSIDERATIONS AND OUTLINE STUDY

Artificial intelligence (AI) and robots are becoming increasingly important in our daily lives.¹ AI-systems are already used for a variety of purposes and deployed in many sectors. Examples are self-driving vehicles, surgical robots, chatbots or virtual assistants. It goes even further. AI-systems are increasingly being used for fraud detection, diagnosis of diseases (cf. IBM's WATSON),² marketing purposes (cf. personalised targeting). It is also deployed in sports to reduce injuries or make tactical decisions, and may even be relied upon in the legal profession. For instance, LawGeex developed an algorithm to review contracts. In an experiment, human lawyers took an average of 92 minutes to complete the task achieving an accuracy level of 85 percent. The software only took 26 seconds to review the contracts and achieved an accuracy level of 94 percent.³ Even more striking, Google Brain developed an AI-system (AutoML) that has created its own "child".⁴ In sum, we "are in the midst of a robotics revolution".⁵

Before proceeding with the study, a proper definition of the concept of AI is required. Although there is currently not a universally accepted technical or legal definition, a distinction is often made between weak, strong and super AI. Artificial narrow intelligence (ANI) or weak AI refers to systems that can perform a specific or few tasks very well, in some cases even better than humans. They operate within a predefined environment (e.g. facial recognition, recommendation systems or self-driving cars). Artificial general intelligence (AGI) or strong AI refers to machines that exhibit human intelligence. AGI aims to perform any intellectual task that a human being is able to do. General AI refers to a system that is intelligent in all domains just like humans. Artificial superintelligence (ASI) – 'singularity' – is the point at which AI-systems will outsmart humans. It refers to any intellect that greatly exceeds the cognitive performance of humans in virtually all domains of interest (p. 5-6).⁶ Nowadays, all AI application are (still) weak.⁷

A distinction is often made between a knowledge-based approach (top-down) on the one hand and a data-based approach on the other hand (bottom-up). The former implies that an expert in the field tries to pour his/her knowledge into a model (e.g. a set of rules, patterns or logical statements). This model is subsequently implemented as a series of instructions – and thus as an algorithm – in the machine to obtain its goal. Such systems aim to capture the knowledge of human experts (e.g. doctors) to support autonomous decision-making. The data-driven approach emerged because of the large amount of available data. Systems are presented with many examples of input and the corresponding output. This process of deducing patterns and learning from examples/experience is called machine learning (ML).⁸ Machine learning is the scientific study of algorithms of computer systems that learn through experience. ML algorithms build a model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to do so. The system itself finds or recognises patterns in order to provide correct answers.⁹ For instance, AI-systems can be shown thousands of images of cats and dogs to

¹ R. LEENES et al., "Regulatory challenges of robotics: some guidelines", *Law, Innovation and Technology* 2017, vol. 9, no. 2, p. 2; G. HALLEVY, "Criminal Liability of Artificial Intelligence Entities - From Science Fiction to Legal Social Control", *Akron Intellectual Property Journal* 2010, vol. 4, no. 2, p. 172.

² P. MARKS, "Dr House goes digital as IBM's Watson diagnoses rare diseases", *New Scientist*, 18 October 2016.

³ C. JEFFREY, "Machine-learning algorithm beats 20 lawyers in NDA legal analysis", *Techspot*, 31 October 2018.

⁴ A. SULLEYMAN, "Google AI creates its own 'child' AI that's more advanced than systems built by humans", *Independent*, 5 December 2017.

⁵ R. CALO, "Robots in American Law", University of Washington School of Law Research Paper no. 2016-04, p. 3.

⁶ European Commission, "AI Watch Historical Evolution of Artificial Intelligence", November 2020, p. 5-6.

https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120469/jrc120469_historical_evolution_of_ai-v1.1.pdf.

⁷ R. DEVILLÉ, N. SERGEYSSELS and C. MIDDAG, "Basic Concepts of AI for Legal Scholars", in J. DE BRUYNE and C. VANLEENHOVE, *Artificial Intelligence and the Law*, Antwerp, Intersentia, 2021, p. 1-21; S.J. RUSSELL and P. NORVIG, *Artificial intelligence: a modern approach*, Pearson Education Limited, 2016, 1132 p.

⁸ R. DEVILLÉ, N. SERGEYSSELS and C. MIDDAG, *o.c.*, p. 1-21. Also see: E. MANNENS, "Wat je moet weten over AI", in J. DE BRUYNE and N. BOUTECA, *Artificiële intelligentie en maatschappij*, Gompel & Svacina, 2021, p. 17-49.

⁹ European Commission, "AI Watch Historical Evolution of Artificial Intelligence", November 2020, p. 5-6.

learn the distinctions (cf. supervised learning). After a while, the system will be able to make a distinction between dogs and cats.

The European Commission (EC) defines AI as systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based acting in the virtual world (e.g. voice assistants, image analysis software or speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).¹⁰ The High Level Expert Group on AI – also known as the AI HLEG – expands this definition.¹¹ AI-systems are software (possibly embedded in hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI-systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.¹² Artificial intelligence is also defined in the recent Proposal of a Regulation on AI. It refers to software that is developed with one or more of the techniques and approaches listed in Annex I (e.g. machine learning approaches, logic and knowledge-based approaches and statistical approaches) and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with (Article 3(1)). We will rely on this working definition of AI.

The rise of AI-systems is no surprise considering their many benefits. They can be more accurate and efficient because they process information faster than humans.¹³ Consequently, they may perform many tasks ‘better’ than their human counterparts.¹⁴ Companies from various economic sectors already rely on AI-applications to decrease costs, generate revenues, increase product quality and improve their competitiveness.¹⁵ AI-systems and robots can also have advantages for the specific sector in which they are to be used. For instance, traffic will become safer with autonomous vehicles. The number of accidents should decrease as computers are generally much better drivers than humans. More generally, transport will become more time-efficient with autonomous car technology. Self-driving cars will also enable people currently facing restrictions in operating a vehicle – such as the elderly, minors or disabled people – to fully and independently participate in traffic.¹⁶ At the same time, however, several challenges exist as well. Think of AI-systems that discriminate against women in a job application¹⁷ or identify black persons on a picture as gorillas (cf. bias).¹⁸ Other ethical questions include the human-machine relationship, and especially which role humans may still play in an AI-era. Another ethical issue relates to the choice that a self-driving car has to make when a collision may occur, for instance between hitting an old man and two toddlers (cf. trolley dilemma¹⁹). The increased use of AI-systems also affects the labour market as many professions are likely to disappear in the long term, at least change

¹⁰ European Commission, “Communication on Artificial Intelligence for Europe”, 25 April 2018, COM(2018) 237 final, p. 1.

¹¹ Following the launch of its AI Strategy in 2018, the European Commission appointed a group of 52 experts to advise for its implementation. The group members were selected following an open selection process and comprised representatives from academia, civil society and industry.

¹² High-Level Expert Group on Artificial Intelligence, “A definition of AI: Main capabilities and scientific disciplines”, 8 April 2019, p. 6.

¹³ S.G. TZAFESTAS, *Roboethics: A Navigating Overview*, Athens, Springer, 2015, p. 147.

¹⁴ H.M. DEITEL and B. DEITEL, *Computers and Data Processing: International Edition*, Orlando, Academic Press, 2014, p. 434. See in this regard the experiment with supercomputer WATSON and the identification of lung cancer cases (I. STEADMAN, “IBM’s Watson is better at diagnosing cancer than human doctors”, *Wired*, 11 February 2013).

¹⁵ S.H. IVANOV, “Robonomics - Principles, Benefits, Challenges, Solutions”, *Yearbook of Varna University of Management* 2017, vol. 10, p. 283-285.

¹⁶ See for example: J.R. ZOHAN, “When Robots Attack: How Should the Law Handle Self Driving Cars That Cause Damages?”, *University of Illinois Journal of Law, Technology and Policy* 2015, vol. 2, p. 471.

¹⁷ J. DASTIN, “Amazon scraps secret AI recruiting tool that showed bias against women”, *Reuters*, 10 October 2018.

¹⁸ J. VINCENT, “Google ‘fixed’ its racist algorithm by removing gorillas from its image-labeling tech”, *The Verge*, 12 January 2018.

¹⁹ This trolley dilemma has been criticised. It is too simplistic and does not really represent a real dilemma.

significantly. Just think of taxi drivers when vehicles become autonomous.²⁰ Some even predict that AI-systems could challenge/threaten humanity in the long term.²¹

More importantly, the commercialisation of AI will pose several challenges from a legal and regulatory point of view as well as it affects nearly all legal domains.²² In a first part of this study (cf. gap analysis), we examined the impact of AI on several legal domains that are relevant for the Federal Public Service Economy. In this second part of the study, we conducted a legal comparative analysis of the situation in four jurisdictions: France, the Netherlands, the United Kingdom and Germany. We completed a similar questionnaire for each of these countries for all Work Packages, namely intellectual property (chapter 2), consumer and market (chapter 3), telecommunications and information society (chapter 4) and insurances (chapter 5). We examined which authorities are competent, whether AI-related policy documents have been issued and which information can be relevant/useful for Belgian authorities. Based on this analysis, we have drawn a separate Excel sheet with a summarising table/chart. The idea is to give the FPS a general and clear overview of the specific AI-related actions taken in the different countries. Additional information can be found in the different questionnaires, which are included below. A summary is provided in the last part (chapter 6).

²⁰ See for more information: M. WEBB, "The Impact of Artificial Intelligence on the Labor Market", 6 November 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3482150; C.B. FREY and M.A. OSBORNE, "The future of employment: How susceptible are jobs to computerisation?", *Technological Forecasting and Social Change* 2017, vol. 114, 254-280.

²¹ See: N. BOSTROM, *Superintelligence: Paths, Dangers, Strategies*, Oxford, Oxford University Press, 2014, p. 328.

²² R. LEENES et al., o.c., p. 2. See in general: M. EBERS and S. NAVAS (eds.), *Algorithms and Law*, Cambridge, Cambridge University Press, 2020, 319 p.; A. DE STREEL and H. JACQUEMI, *L'intelligence artificielle et le droit*, CRIDS, Larcier, 2018, 482 p.; J. DE BRUYNE and C. VANLEENHOVE, *Artificial Intelligence and the Law*, Antwerp, Intersentia, 2021, 520 p.

CHAPTER 2 – INTELLECTUAL PROPERTY (WP 2)

Questionnaire the Netherlands

1. Which authorities are competent for intellectual property?

- Benelux Office for IP – BOIP
- Octrooicentrum Nederland
- Responsible ministries: Ministry of Economic affairs and Climate / Ministry of Justice and Security

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

- The Ministry of Economic Affairs and Climate has published three relevant documents
 - o [“Strategisch Actieplan voor Artificiële Intelligentie”](#), published in October 2019
 - o [“Beleidsnota in verband met Mededeling Actieplan Intellectuele Eigendom”](#), November 2020
 - o [“Beleidsnota: Modernisering Rijsoctrooiwet 1995”](#), 8 December 2020

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

N/A

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

- “Strategisch Actieplan voor Artificiële Intelligentie”:
 - o The Action plan recognises the challenges AI-systems may bring for the current Dutch intellectual property framework. The actions it proposes, are:
 - The Netherlands will continue monitoring developments in IP law and AI, in line with initiatives taken in a European or international context.
 - Implementation of the TDM-exceptions, stemming from the CDSM-directive (literal transposition, no modifications).
- “Beleidsnota in verband met Mededeling Actieplan Intellectuele Eigendom”:
 - o This document is a response to the communication of the European Commission of its action plan on intellectual property. In relation to the topic of the study, is the following excerpt (p.5): “The government follows the Commission's view that the digital revolution forces to reflect on the question of how and what should be protected. The rapid development of AI raises questions (and possibly uncertainties) about IP protection for AI itself and for creations developed by or with the help of AI. For the time being, the government shares the Commission's opinion that AI systems should not be treated as authors or inventors and will provide input to the follow-up process”.

- “Beleidsnota: Modernisering Rijksoctrooiwet 1995”:
 - o This policy note lists a range of policy initiatives in order to make the Dutch patent system more attractive for SME's. It contains interesting proposals, but they are not directly relevant for the purpose of this study.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

N/A

Questionnaire France

1. Which authorities are competent for intellectual property?

- INPI - *Institut national de la propriété industrielle*
- BDPI - *Bureau de la propriété intellectuelle*
- CSLPA - *Conseil supérieur de la propriété littéraire et artistique*
- HADOPI - *Haute Autorité pour la Diffusion des Œuvres et la Protection des droits d'auteur sur Internet*

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

- CSPLA published two relevant reports:
 - o A first report titled “[Rapport Mission Intelligence artificielle et Culture](#)”, published on 27 January 2020, written by A. BENSAMOUN and J. FARCHY.
 - o A second report titled “[Rapport de mission transposition des exceptions de fouille de textes et de données: enjeux et propositions](#)”, published on 15 December 2020, written by A. BENSAMOUN and Y. BOUQUEREL.

Furthermore, the CSPLA is in the [process of preparing](#) a third (set of) report(s) on database protection, in which they will analyse the current French regime of (sui generis) database protection. The first related report should be published in the course of June 2021.

- HADOPI also published a relevant report, titled “[L'intelligence artificielle: les premières applications dans le secteur culturel et les enjeux de régulation](#)”, published in September 2019.
- Finally, INPI updated its patent [examination guidelines](#) in October 2019, whereby it included a part on artificial intelligence.

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

- CSPLA
 - o Rapport Mission Intelligence artificielle et Culture (“CSPLA 1”)
 - As a preliminary remark, it should be pointed out that this report is an academic report which includes some policy suggestions but that none of these suggestions have actually been included in any kind of legislative

proposal. In that sense, the report also explicitly stipulates that this is a political/legislative choice in the end and that an international or European solution is preferable.

- With regard to IP protection for data, the report suggests the establishment of some type of collective management societies for data, who could be responsible for licensing data for e.g. text-and data mining on behalf of the initial rightsholders.
 - With regard to the (attribution of) ownership of AI-generated output, it suggests four possible solutions (p. 36-41 and 45-47): the developer of the AI-system, the user of the AI-system, establishing a regime similar to the UK regime for computer-generated works (in which the rights are awarded to the person who made the arrangements necessary for the creation of the work) or no copyright protection (in favour of alternative systems like contractual solutions, technical measures, trade secrets, unfair trade practices or public domain). For each of these categories of proposals, the report briefly lists advantages and disadvantages, while it can also be understood that the authors of the report prefer to attribute the rights to the developer of the AI-system.
 - With regard to sui generis/ related right protection for AI-assisted/-generated output, the report lists three possibilities (p.41-45) . First, it suggests to establish a regime similar to the current French regime for collective works, in which there would be a presumption of authorship to the benefit of the person under whose name AI-generated works are published. Second, it suggests to establish a regime similar to the regime for posthumous works, meaning that the person who publishes the AI-generated work obtains the rights to it. Third, it suggests to establish a regime similar to the sui generis database protection. This would entail that the rights are attributed to the person who can demonstrate a substantial financial, material or human investment. The report adds that such sui generis rights could be limited to commercial exploitation, leaving research or private use purposes out of scope.
 - With regard to the infringement of intellectual property rights, the report (p.50-58) raises the question whether the right to communication to the public and the reproduction right (under reference to the Pelham-case, C-476/17) will indeed be infringed by AI-systems and continues with explaining the limited scope of the exceptions for private use, research purposes and text- and data mining (“TDM”).
- Rapport de mission transposition des exceptions de fouille de textes et de données: enjeux et propositions (“CSPLA 2”)
- In this report, the CSPLA considers the new TDM-exceptions which need to be implemented in French law.
 - In summary, the report (p. 87-92) advises to abolish the current French TDM-exceptions and replace them with the TDM-exceptions as set out in art. 3 and 4 CDSM-directive (as they would be irreconcilable).
 - With regard to the textual implementation, the report sets out how the articles should be implemented in French law, including some French peculiarities (not relevant for Belgium). Interestingly, earlier in the report, a variety of issues in relation to the transposition of the two exceptions are addressed, including e.g. ways of defining the beneficiaries of the scientific research TDM-exception (art. 3 CDSM), whether the opt-out under the general TDM-exception (art. 4 CDSM) should be justified or in what manner

rightsholders should express such opt-out. However, these discussions are often limited to a list of options, whereby the authors indicate which option they would prefer but which is not reflected in the proposed text. This is probably due to the fact that they often suggest that such topics should be clarified not in formal law, but in a decree of the Council of State, while also indicating that the directive does not leave much appreciation margin to member states (p. 48). Moreover, the preferred options will, generally speaking, not lead to a significant expansion or (a further) limitation of the scope of application of the TDM exceptions. This renders it, nonetheless, difficult to assess to what extent the French legislator will indeed take into account the authors' preferences.

- INPI
 - o Patent examination guidelines – October 2019 ("INPI")
 - These guidelines provided additional guidance on the patentability of AI-technology, largely similar to the updated EPO guidance.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

- HADOPI
 - o L'intelligence artificielle: les premières applications dans le secteur culturel et les enjeux de régulation
 - In its rather briefly elaborated paper, HADOPI addresses four issues without indicating any specific French policy measures. It tackles the role AI can play in the distribution of cultural works (e.g. through recommendation algorithms), the role AI can play in online IP enforcement (e.g. through automatic recognition systems), how AI can be regulated (by referring to transparency/auditability requirements) and how AI can become a regulatory tool (by referring to its possible judiciary use cases or its role in online evidence searches).

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – CSPLA: efficiency and budgetary aspects

A. Which purposes were identified/established?

This purpose of this report is very similar to the purpose of the study at hand but with a focus on copyright, i.e.: what challenges arise under French copyright law in relation to AI-systems and is French copyright law fit for purpose. In response to the identified challenges, the report lists various policy proposals. None of these proposals, however, have an explicit purpose apart from providing possible legal solutions to the identified challenges/fill the legal gaps within the current copyright framework in order to provide legal certainty to the users/developers of AI-systems and ensure investment in the further development of AI-technology (p. 30-31).

B. How do the measures try to achieve their purpose?

By showing that French copyright law is, in principle, sufficiently flexible to incorporate AI-assisted/-generated output, albeit that it may be necessary to amend certain statutory provisions if certain political choices would be made (e.g. the creation of sui generis/ related right protection for AI-assisted/-generated output).

C. Where possible to assess, to what extent did these measures achieve their purpose?

N/A

D. Where possible to assess, what impact did the measures have on the government budget?

N/A

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. We have identified similar issues and gaps.

3.2.2. Proposal 2 – CSPLA: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of this report is to provide guidance on how to transpose and implement the TDM-exceptions into French copyright law. The authors also address a variety of additional issues in order to further clarify the scope of application of the two exceptions, expressing their preference for certain possibilities, but without reflecting them in the proposed textual implementation.

B. How do the measures try to achieve their purpose?

By proposing a textual implementation which respects the wording of the CDSM-directive, while also taking into account certain French peculiarities, taking into account the limited margin of appreciation for member states when implementing a harmonisation directive.

C. Where possible to assess, to what extent did these measures achieve their purpose?

N/A - as the TDM-exceptions stem from a European directive, this can only be evaluated on a European level.

D. Where possible to assess, what impact did the measures have on the government budget?

N/A

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. We have identified similar issues and gaps.

3.2.3. Proposal 3 – INPI: efficiency and budgetary aspects

A. Which purposes were identified/established?

Implicit purpose: Providing additional clarity to applicants for patents on AI-technology.

B. How do the measures try to achieve their purpose?

By providing additional examples of patentable AI-technology.

C. Where possible to assess, to what extent did these measures achieve their purpose?

N/A

D. Where possible to assess, what impact did the measures have on the government budget?

N/A

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. We have identified similar issues and gaps, but of limited relevance as Belgium only knows patent 'registration' proceedings (the Belgian Office for Intellectual Property does not carry out patentability examinations itself and does, hence, not publish 'guidelines for examination'). It does, however, sometimes publish 'communications', which it could also do with regard to the patentability of AI-systems.

Questionnaire the United Kingdom

1. Which authorities are competent for intellectual property?

- UK Intellectual Property Office – UKIPO
- Responsible department: Department for Business, Energy & Industrial Strategy

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

The UKIPO has published two relevant documents:

- It has updated various sections of its Manual of Patent Practice (examination guidelines) in October 2020, whereby it included various parts on artificial intelligence. This manual can be found [online](#).
- In March 2021, it published the government [response](#) to the call for views on artificial intelligence and intellectual property.

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

- Manual of patent practice– October 2020 (“MOPP”)
 - o The updates to the Manual of Patent Practice (sections 1.29.5; 1.39.3; 7.11.1; 13.10.1) provide additional guidance on the patentability of AI-technology (e.g. in relation to excluded subject matter and inventorship) by reflecting e.g. the decisions in the [UK DABUS-cases](#).
- Government response to the call for views on artificial intelligence and intellectual property – March 2021 (“Call for Views AI & IP”)
 - o With regard to IP-protection for AI-technology, the government lists the following actions:
 - Publish enhanced IPO guidelines on patent exclusion practice for AI inventions and engage AI interested sectors, including SMEs, and the patent attorney profession to enhance understanding of UK patent exclusion practice and AI inventions. The IPO will review its patent practice in preparation for the guidelines and establish any difference in outcome for AI patent applications filed at the IPO and the European Patent Office (EPO).
 - Work with stakeholders and international partners to establish the feasibility, costs and benefits of a deposit system for data used to train AI systems disclosed within patent applications.
 - Commission an economic study to enhance our understanding of the role the IP framework plays in incentivising investment in AI alongside other factors. This will draw together the international evidence.
 - Engage with other government departments to gather emerging data and understanding of the drivers of the AI sector in the UK context. This will

- provide an evidence base on which to judge whether there is a rationale for further intervention in the area.
- With regard to IP protection for data, the government lists the following action:
 - Review the ways in which copyright owners license their works for use with AI, and consult on measures to make this easier, including improved licensing or copyright exceptions, to support innovation and research.
 - With regard to copyright protection for AI-assisted/-generated output, the government lists the following actions:
 - Consult on whether to limit copyright in original works to human creations (including AI-assisted creations).
 - Consider whether action should be taken to reduce confusion between human and AI works, and the risk of false-attribution.
 - With regard to sui generis/ related right protection for AI-assisted/-generated output, the government list the following action.
 - Consult on whether or not to replace the existing protection for computer-generated works²³ with a related right, with scope and duration reflecting investment in such works.
 - With regard to patent protection for AI-assisted/-generated output, the government lists the following action:
 - Build on the suggestions made by respondents and consult later this year on a range of possible policy options, including legislative change, for protecting AI generated inventions which would otherwise not meet inventorship criteria. (Note that the UK government is explicitly considering adopting new laws which would render AI-generated inventions patentable as opposed to e.g. the stance taken by the EPO but also the UK courts.).
 - With regard to trademark/design protection for AI-assisted/-generated output, the government believes that the current legislation is fit for purpose and does not foresee any legislative changes in the near future. It does, however, promise to monitor the situation because as AI technology develops, there may be a more significant impact on trademark/design law.
 - With regard to the infringement of intellectual property rights in an AI-context, the government plans the following action:
 - Conduct research into artificial intelligence and IP enforcement, and the opportunities and challenges in this area. Research has been commissioned, to report in autumn 2021.
 - Finally, the government also considers taking some more general actions:
 - Engage with like-minded nations and multilateral organisations (including the World Intellectual Property Organisation and EPO) on issues raised in the Call for Views, to deepen understanding, foster co-operation and establish common ground. The aim of this international leadership will be to shape the global debate in order to develop policy approaches that give the opportunity for growth as part of a balanced world IP system.

²³ It should be pointed out that this UK regime of "computer-generated works" is quite an exceptional regime. Section 9(3) and 12 (7) Copyright, Designs and Patents Act 1988 (CDPA) and Section 2(4) of the Registered Designs Act stipulate, in summary, that with regard to computer-generated works/designs, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work/design are undertaken (while also providing that copyright will expire 50 years after the date of creation). However, the application of this regime is often deemed quite unclear, as confirmed in the Call for Views, while scholars also tend to agree that this regime conflicts with current European copyright standards. See e.g. J. ALLAN e.a., *Trends and Developments in Artificial Intelligence – Challenges to the Intellectual Property Rights Framework*, Luxembourg, Publications Office of the European Union, 2020, p.88 and footnote 444.

- Work with partners including the Office for AI and AI Council to further engage with and develop our understanding of the AI sector, including technology start-ups and researchers.
- Hold a UK-wide programme of university-led seminars, building on the content of this government response. The first phase will start with a joint seminar with The Alan Turing Institute in the spring of 2021.
- Continue to look for opportunities to integrate AI into operational delivery of intellectual property rights, as part of the IPO's Transformation programme. This will support the IPO's aim to deliver timely, reliable and quality services. It will build on the IPO's recently launched trademarks Pre-Apply service, which uses AI to support customers to make high-quality applications. The IPO will also use AI to validate its data and make it readily available for use by businesses.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

N/A

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – MOPP: efficiency and budgetary aspects

A. Which purposes were identified/established?

Implicit purpose: Providing additional clarity to applicants for patents on AI-technology.

B. How do the measures try to achieve their purpose?

By providing additional guidance in relation to the patentability of AI-technology.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Based on the views expressed by stakeholders in the course of the call for views on AI and IP by the UKIPO, the current UK approach to patent exclusions seems to be quite criticised. Respondents pointed out that they, for instance, think it is hard to predict the outcome of UK IPO decisions on patent exclusion and seem to prefer the more permissive patent exclusion approach of the EPO, which appears to be giving better outcomes for AI patent applications.

Taking into account that the call for views ran from 7 September to 30 November 2020, while some sections were updated in the course of October 2020, it is, however, difficult to understand to what extent such critique was also aimed at the updated sections, rendering an efficiency judgement impossible.

D. Where possible to assess, what impact did the measures have on the government budget?

N/A

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. We have identified similar issues and gaps, but of limited relevance as Belgium only knows patent 'registration' proceedings (the Belgian Office for Intellectual Property does not carry out patentability examinations itself and does, hence, not publish a 'manual for patent practice' or 'guidelines for examination'). It does, however, sometimes publish 'communications', which it could also do with regard to the patentability of AI-systems.

3.2.2. Proposal 2 – Call for Views AI & IP: efficiency and budgetary aspects

A. Which purposes were identified/established?

The UK government aims to ensure that any measures they will implement:

- Encourage innovation in AI technology and promote its use for the public good.
- Preserve the central role of intellectual property in promoting human creativity and innovation.
- Are based on the best available economic evidence.

B. How do the measures try to achieve their purpose?

When implementing the envisaged measures in this area, the IPO will:

- Collaborate with experts from business, technology and research to build our understanding of the AI sector and develop a robust evidence base.
- Advocate common approaches with like-minded nations, and take a lead on the international stage.
- Communicate and engage with developers and users of AI and owners and users of intellectual property to promote understanding in this area.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not possible at the moment, as the actions still have to be taken (e.g. organising the consultations etc.)

D. Where possible to assess, what impact did the measures have on the government budget?

Not mentioned.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. We have identified similar issues and gaps as the respondents to the call for views. Some of the governmental actions may therefore also be considered by Belgian/European policy makers.

Questionnaire Germany

1. Which authorities are competent for intellectual property?

- Deutsche Patent- und Markenamt (DPMA) – German Patent and Trademark Office
- Responsible ministry: Ministry of Justice and Consumer Protection
- The Federal government has also published AI-related documents

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

- DPMA:
 - o The DPMA has an [online dossier](#) on AI and IP

- Federal Government²⁴
 - o In 2018, the German Federal Government published its AI strategy: [LINK](#) (which was updated in 2020: [LINK](#))
 - o In 2021, the Government published its [Federal Data Strategy](#)

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

- Federal Government
 - o In the 2018 AI-strategy, the German government considers adapting the legal framework governing copyright in order to make it easier to use text and data mining (TDM) as a basis for machine learning both for commercial and non-commercial purposes, following the principle “the right to read is the right to mine” (p. 39). (The 2020 update does not mention text and data mining.)
 - o Federal data strategy
 - The data strategy refers to the fact that data may be protected through (sui generis) database protection and trade secrets protection, while the text and data mining-exceptions may also be relevant (p. 21). More specifically, and with regard to text and data mining, it refers to the transposition of art. 3 and 4 of the CDSM directive (p. 24 and 69).
 - Moreover, the strategy explicitly rejects the creation of some kind of ‘data property’. Oppositely, it argues that the existing legal framework should rather be reinforced and that a legal framework with regard to the access to non-personal data should be created. (The related envisaged measures do, however, all fall outside of intellectual property law and will therefore not be discussed. They rather fall under WP - Data Economy).
 - o As both documents relate to the same topic (text and data mining), they will be discussed jointly.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

- DPMA: the online AI & IP dossier has a general, informative nature and does not contain any policy measures.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Text and data mining: efficiency and budgetary aspects

A. Which purposes were identified/established?

No specific purposes are identified, apart from making it easier to text and data mine for machine learning purposes (commercially and non-commercially) while aiming to strike a fair balance between the interest of copyright holders and content users.

²⁴ As part of Germany's Presidency of the Council of the EU, the Federal Ministry of Justice and Consumer Protection hosted a high-level online conference on “Data Economy, AI and Intellectual Property” on 8 September 2020. Materials can be found here, but do not include policy proposals: <https://www.eu2020.de/eu2020-en/news/pressemittellungen/data-economy-ai-intellectual-property-bmjv-lambrecht/2381948>. The results of the conference form the basis of a political stocktaking of the current situation and help to define further steps in Germany, in the European Union and at an international level.

B. How do the measures try to achieve their purpose?

By transposing art. 3 and 4 of the CDSM-directive. Germany intends to transpose these provisions in a new Section 44a (the "general" TDM exception, art.4 CDSM-directive) and a revised Section 60d (TDM for scientific research, art.3 CDSM-directive) of the German Copyright Code.²⁵

C. Where possible to assess, to what extent did these measures achieve their purpose?

N/A – As the TDM-exceptions stem from a European directive, this can only be evaluated on a European level and after the moment of entering into force.

D. Where possible to assess, what impact did the measures have on the government budget?

N/A

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. We have identified similar issues and gaps.

²⁵ Germany enacted a TDM-exception for non-commercial purposes in 2018. This exception, however, had a narrower scope than the TDM-exception included in art. 3 CDSM-directive.

CHAPTER 3 – CONSUMER AND MARKET (WP 3)

WP 3.1. COMPETITION LAW

Questionnaire the Netherlands

1. Which authorities are competent for competition law?

- Autoriteit Consument en Markt (ACM)

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

- [Oversight of algorithms](#), 2020

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

No concrete proposal relevant for the use of AI systems in relation with competition law

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

No other proposal.

Questionnaire France

1. Which authorities are competent for competition law?

- Autorité de la concurrence

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

- [Algorithms and competition](#), 2019
- [Concurrence et commerce en ligne – Competition and e-commerce](#), 2020
- [Common Understanding](#) of G7 Competition Authorities on “Competition and the Digital Economy” Paris, 5th June, 2019

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

- [Proposal 1](#): Ensure or strengthen the investigative powers of competition authorities
- [Proposal 2](#): Ensure expertise in algorithms
- [Proposal 3](#): Attribute liability for infringements made by AI systems
- [Proposal 4](#): Ex-ante regulation of all algorithms in *abstracto*

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

No other relevant proposal.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Investigative powers: efficiency and budgetary aspects

A. Which purposes were identified/established?

Ensuring or strengthening the investigative powers of competition authorities against the use of algorithms by firms.

B. How do the measures try to achieve their purpose?

The authorities must have access to the necessary information including information on the role and the functioning of the algorithm (i.e. the objective, its implementation, its changes over time, the input data, the output, the decision-making process). In addition, the authority shall have the power to conduct inspections.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not implemented yet.

D. Where possible to assess, what impact did the measures have on the government budget?

No data.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Strengthening the investigative powers of the Belgian competition authority is beneficial. Although this will not directly solve the identified gaps, it will allow the competition authority to be more effective in identifying problems, better understand the logic behind them, and ultimately find an appropriate solution or impose adequate remedies.

3.2.2. Proposal 2 – Ensuring expertise: efficiency and budgetary aspects

A. Which purposes were identified/established?

Ensuring expertise in algorithms.

B. How do the measures try to achieve their purpose?

Improve the competition authority's control over the use of algorithms by firms by ensuring sufficient in-house knowledge and resources. This can be done through the cooperation with

international authorities but also with private actors such as the businesses themselves and academics, evidence-based market studies, and sector inquiries.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

Not implemented yet.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No data.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

Increasing the expertise of the Belgian competition authority and its staff with regard to algorithms constitutes an indirect way to address the gaps. Similar to the first proposal, it is interesting to train the members of the competition authority with regard to AI, its functioning and especially its risks. In this way, they will be able to better identify uses of algorithmic systems that could lead to anti-competitive practices and react accordingly.

3.2.3. Proposal 3 – Liability: efficiency and budgetary aspects

A. *Which purposes were identified/established?*

Attribute the liability for an anti-competitive behaviour adopted by AI-systems.

B. *How do the measures try to achieve their purpose?*

Improve the enforcement of competition law by ensuring that it is possible for authorities to hold an actor liable when a violation of competition law is committed by using algorithms.

The document proposes two possibilities for attributing liability. The first proposition is to treat the algorithmic behaviour as a decision made by an employee. In this case, the undertaking is liable except if it can prove that the algorithm was acting without any authorisation. In that case, it is hard to define the modalities of that liability. The second proposition is to engage the undertaking's liability simply for using the algorithm which colluded, even if the undertaking was not aware of that possibility of anticompetitive behaviour. That way, there is a course of action for the authority to sanction the undertaking and the undertaking will be induced to be cautious when using algorithms.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

Not enforced yet. A consensus should first be found about the attribution of liability and then it has to be implemented/introduced in the national legislation.

D. *Where possible to assess, what impact did the measures have on the government budget?*

None.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

The issue of the attribution of liability is not settled in the Belgian legislation. Discussions are currently ongoing with regard to the topic. The clear attribution of liability would avoid uncertainty and prevent impunity in case no one is liable for the consequences of the use of AI.

3.2.4. Proposal 4 – Anti-competitive behaviour: efficiency and budgetary aspects

A. *Which purposes were identified/established?*

Prevent the anti-competitive behaviour by algorithms that can be predicted from the outset of its creation.

B. How do the measures try to achieve their purpose?

By imposing an ex-ante regulation of all algorithms in abstracto and eventually ensure its respect by imposing that the algorithm passed a specific test before its integration in the undertaking's functioning. The goal is to make sure that the algorithm does not permit ab initio to reach an anti-competitive situation.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not enforced yet.

D. Where possible to assess, what impact did the measures have on the government budget?

The implementation of this proposal may require the creation of a certification (or label) and experts in charge of delivering that certification. This certification would attest that the algorithms passed the test before its commercialisation. This can be done by private companies. In that case, there is no impact on the government's budget. On the other hand, if the government wants to create a government agency to do it, it will generate the cost of the creation of this organisation and the remuneration of the staff.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

There is no obstacle to the implementation of such preliminary test in Belgium. It will then be necessary to set up this test and decide whether the competence to certify the algorithm will be entrusted to a private or public actor. In all cases, certification must be supervised to ensure that certifiers apply the same conditions of award.

Questionnaire the United Kingdom

1. Which authorities are competent for competition law?

- Competition and Markets Authority

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

- [Algorithms: How they can reduce competition and harm consumers](#), 2021
- [Pricing algorithms Economic working paper on the use of algorithms to facilitate collusion and personalised pricing](#), 2018
- [Common Understanding of G7 Competition Authorities on "Competition and the Digital Economy"](#) Paris, 5th June, 2019

3. Discussion of documents**3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?****3.1.1. If yes, briefly list these proposals**

- [Proposal 1](#): collaboration with other national and international regulators
- [Proposal 2](#): encouraging firms to be transparent about their algorithmic systems
- [Proposal 3](#): establishment of standards

- [Proposal 4](#): broaden the obligation set forth in the Commission Delegated Regulation 2017/589 to any firms using AI
- [Proposal 5](#): ensure the authorities' investigative powers
- [Proposal 6](#): impose audits, ongoing monitoring, algorithmic risk assessments
- [Proposal 7](#): Testing of the algorithms

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

The CMA Digital Markets Taskforce recommended an ex-ante regime applicable to the most powerful platform. The digital firms identified as having Strategic Market Status (SMS) would be subjected to additional obligations. Indeed, once the firm is identified as an SMS firm, this undertaking will be subject to a code of conduct, potential pro-competitive interventions, and particular rules regarding mergers.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Collaboration: efficiency and budgetary aspects

A. Which purposes were identified/established?

Collaboration with other national and international regulators.

B. How do the measures try to achieve their purpose?

Anti-competitive harm for consumers caused by the use of algorithms may be subject to different regulations and fall under the jurisdiction of various regulators. In order to prevent those risks, it is necessary to adopt an approach that combines those regulations (especially Data Protection Regulations). In the case of the UK, the competition authorities are the Information Commissioner's Office (ICO), the Financial Conduct Authority (FCA), Ofcom, and the Equalities and Human Rights Commission (EHRC)

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data.

D. Where possible to assess, what impact did the measures have on the government budget?

No data.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

For Belgium, the collaboration with other States already takes place within the European Commission.

3.2.2. Proposal 2 – Transparency: efficiency and budgetary aspects

A. Which purposes were identified/established?

Encouraging firms to be transparent about their algorithmic systems.

B. How do the measures try to achieve their purpose?

Firms should have an obligation to inform consumers about the use of algorithms and explain how the algorithm works and the decision-making process resulting in the output. This can be reached by focusing on the explainability of the AI system which will depend on the nature of the algorithm (decision tree, deep learning...)

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not enforced yet.

D. Where possible to assess, what impact did the measures have on the government budget?

None.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

This proposal consists in an obligation for firms using algorithms to be transparent about it. Not only should third people be aware that the undertaking is using AI technologies, but they should also be informed about how the AI system works, which data are used, what consequence does the use of AI have (decision, ranking...).

In fact, it is already foreseen in the Digital Service Act (DSA)²⁶. Indeed, this regulation, directly applicable in Belgian law, provides for several transparency obligations for platforms. These obligations concern, among other things, the use made by these platforms of artificial intelligence systems (for example used to make recommendations, to choose which information is shown or not to the Internet user (feed), to choose which advertisement is shown to the Internet user...).

Firstly, the DSA provides for an obligation for all intermediary service providers to establish transparency reports explaining any content moderation activities they have undertaken. The minimum content of the report is set out in Article 13 of the DSA. Other articles add other mentions that must be included in the transparency report, depending on the qualification of the service provider as a platform and the size of that platform²⁷. The larger the platform, the more information the transparency report must contain. Article 23 of the DSA imposes supplementary obligations concerning the transparency reports by online platforms. Article 24 DSA provides for transparency in the field of online advertising displayed by online platforms. Article 33 DSA imposes supplementary obligations for the transparency report of very large online platforms and article 30 DSA is about the online advertising on those very large platforms.

Secondly, platforms must also publish reports exposing the reaction they have when faced with content declared illegal or contrary to their terms and conditions (Article 23 DSA).

In the end, the European legislator already took the step to impose transparency obligations to online platforms. Those obligations will be part of Belgian law as soon as the Regulation on Digital Single Act will be adopted at the European level.

3.2.3. Proposal 3 – Standards: efficiency and budgetary aspects

A. Which purposes were identified/established?

Establishment of standards.

B. How do the measures try to achieve their purpose?

The creation of standards, guidance, good practice for the conception and the use of algorithms could be a way to prevent the occurrence of anti-competitive practices.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not implemented yet.

D. Where possible to assess, what impact did the measures have on the government budget?

None.

²⁶ EU Commission, Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act), 2020/0361 (COD), Proposal, 15 December 2020 (hereafter "DSA").

²⁷ The size of the platform is defined by the number of user of that platform.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

There is no obstacle for the implementation of that proposal in Belgium. Moreover, in Belgium as in many other countries, the adoption of such Soft law instrument is recommended and encouraged.

3.2.4. Proposal 4 – Broaden obligations: efficiency and budgetary aspects

A. Which purposes were identified/established?

Broaden the obligation set forth in the Commission Delegated Regulation 2017/589 to any firms using AI.

B. How do the measures try to achieve their purpose?

This regulation provides for obligations to investment firms engaged in algorithmic trading. Those obligation includes both technical and organisational obligations for those firms to prevent the risks related to the use of algorithms.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not implemented yet.

D. Where possible to assess, what impact did the measures have on the government budget?

None.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

In practice, it is fundamentally only transparency obligation which are already imposed by the UK regulation for investment firms. As it has been said for proposal 2, the DSA already plan to impose transparency obligations on intermediary service providers and online platforms. (See proposal 2)

3.2.5. Proposal 5 – Investigative powers: efficiency and budgetary aspects

A. Which purposes were identified/established?

Ensure the authorities' investigative powers.

B. How do the measures try to achieve their purpose?

There is a range of tools at the disposal of the authority to analyse the use of algorithms by the firm and its consequence on the market and consumers. However, it is fundamental that those authorities are able to obtain information related to the algorithms: data, documents, ...

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data.

D. Where possible to assess, what impact did the measures have on the government budget?

No data.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Increasing the investigative powers of the Belgian competition authority will allow the authority to work more effectively in order to tackle anti-competitive practices achieved by the use of algorithms.

3.2.6. Proposal 6 – Audits and monitoring: efficiency and budgetary aspects

A. Which purposes were identified/established?

Impose audits, ongoing monitoring, algorithmic risk assessments.

B. How do the measures try to achieve their purpose?

The rapid evolution of technologies and the unpredictability of the functioning of the algorithms calls for an update of the control regularly. Permanent or at least regular control can be achieved through audits, monitoring and risk assessments.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data.

D. Where possible to assess, what impact did the measures have on the government budget?

None.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

There is nothing preventing the Belgian legislator from creating an obligation for companies using AI-systems to submit to these controls. However, if the legislator does not do so, companies should still be encouraged to do so voluntarily.

3.2.7. Proposal 7 – Testing algorithms: efficiency and budgetary aspects

A. Which purposes were identified/established?

Testing of the algorithms.

B. How do the measures try to achieve their purpose?

Some of the rules incorporated in the algorithm or in its design could be considered anti-competitive. One possibility is to use regulatory sandboxes. It allows to test the algorithm in a safe and supervised environment and make sure that it works well before integrating it into the company's operations (recommended by the Digital Markets Taskforce and already used by the FCA and ICO)

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not enforced yet.

D. Where possible to assess, what impact did the measures have on the government budget?

No data.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

There is no obstacle to the implementation of such preliminary test in Belgium. We already stated that the test could result in the award of a certification or a label. UK proposal goes further when proposing a technique for carrying out the test itself. Indeed, the use of sandboxes could be a way to test algorithms in order to observe their functioning in a safe environment.

Questionnaire Germany

1. Which authorities are competent for competition law?

- Bundeskartellamt

- Commission 'Competition Law 4.0' established by the Federal Ministry for Economic Affairs and Energy

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

- [Algorithms and competition](#), 2019
- [Algorithms and Competition in a Digitalized World](#), 2020
- [Strategie Kunstliche Intelligenz der Bundesregierung](#), 2020
- [Stellungnahme der Bundesregierung der Bundesrepublik Deutschland zum Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen](#), 2020
- [Common Understanding of G7 Competition Authorities on “Competition and the Digital Economy”](#) Paris, 5th June, 2019
- [A New Competition Framework for the Digital Economy Report by the Commission ‘Competition Law 4.0’](#), 2019

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

Cf. proposal of France.

The German and the French competition authorities have worked together to produce the document "Algorithms and competition", which contains the proposals relevant to this study. The documents of the German competition authority alone do not make any additional proposals of interest to this study.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

Cf. part on France.

WP 3.2. CONSUMER LAW

Questionnaire the Netherlands

1. Which authorities are competent for consumer law?

- Autoriteit Consument en Markt ([ACM](#))

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

The ACM has published several documents that relate to AI. Some are relevant for consumer protection, and hence are listed below. In addition, other authorities in the Netherlands issued documents that are to some extent relevant for AI and consumer protection.

- ACM, [Study into oversight of algorithmic applications](#), 2020
- ACM, [Guidelines on the protection of the online consumer](#), 2020
- Netherlands Government, [Action plan on AI \(SAPAI\)](#), 2019

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

Yes, a proposal that responds to one of the identified gaps was issued in the Netherlands, within the document of the ACM: [Study into oversight of algorithmic applications](#) (p. 2).

Online traders should provide their consumers with complete information, notably on the fact that they use algorithms.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

No other relevant proposal.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Information obligations: efficiency and budgetary aspects

A. Which purposes were identified/established?

Ensure that online traders provide their consumers with complete information.

B. How do the measures try to achieve their purpose?

The guidelines state that online traders should inform their consumers about several elements, notably on the fact that they use algorithms (which can be AI systems).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data available.

D. Where possible to assess, what impact did the measures have on the government budget?

No data available. Yet, given the type of measure (soft law) and the addressees of the document (online traders), the budgetary impact seems very limited.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. It could prove useful to adopt the same type of measure in Belgium, so that consumers would be informed when they face algorithms (i.e. AI systems).

Questionnaire France

1. Which authorities are competent for consumer law?

- The Direction générale de la concurrence, de la consommation et de la répression des fraudes ([DG CCRF](#))

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

No.

However, several documents were issued by other authorities, in France, regarding AI. A few relate to some extent to consumer protection:

- French Government, [France Intelligence Artificielle – Synthesis report](#), 2017
- French Government, [Mission Villani – For a meaningful Artificial Intelligence](#), 2018

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

There is no concrete proposal relevant for the gaps identified regarding consumer protection in France.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

In the synthesis report '[France Intelligence Artificielle](#)', the French Government proposes to encourage an approach in which the interests of consumers and undertakings could be conciliated, notably regarding algorithmic transparency. In this regard, the French Government proposes to assess if it is possible to create a platform for exchanges between stakeholders (i.e. undertakings, consumers and public authorities), whether at EU level or at national level (p. 25, row 2, column 2).

In a similar fashion, the [Villani Report](#) proposes to 'open the black box' (i.e. explain decisions made by AI to average persons), and develop the auditing of AI (p. 115-118).

These could obviously be beneficial in terms of consumer protection, where consumers interact with AI systems.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

N/A.

Questionnaire the United Kingdom

1. Which authorities are competent for consumer law?

- Competition and Markets Authority ([CMA](#))

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes.

Yet, such documents do not directly relate to consumer protection, but rather to competition law (cf. CMA document listed below). However, other authorities in the UK issued a document that is to some extent relevant for AI and consumer protection.

- CMA, [Algorithms: how they can reduce competition and harm consumers](#), 2021
- ICO & Alan Turing Institute, [Explaining decisions made with AI](#), 2020

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

There is no concrete proposal relevant for the gaps identified in the study regarding consumer protection in United Kingdom.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

The ICO and the Alan Turing Institute issued detailed guidance on explaining decisions made with AI, for companies that develop, use, or otherwise exploit AI systems (parts 1-3). Such guidance might prove useful where consumers face AI made decisions.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

N/A.

Questionnaire Germany

1. Which authorities are competent for consumer law?

- The Directorate-General V ([Consumer Policy](#))

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

No.

However, several documents were issued by other authorities in Germany regarding AI. A few relate, to some extent, to consumer protection:

- German Federal Government, [Artificial Intelligence Strategy](#), 2018
- German Federal Government, [Artificial Intelligence Strategy](#), 2020
- Federal Commissioner for Data Protection and Freedom of Information, [Activity Report](#), 2019

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

There is no concrete proposal relevant for the gaps identified in the previous study regarding consumer protection in Germany.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

In its Activity Report of 2019, the Federal Commissioner for Data Protection and Freedom of Information states that the principle of explainability should be enshrined in law, when AI technology is implemented in many fields (p. 8, 14-19, 29-31). Here again, this policy measure could prove beneficial in terms of consumer protection, where consumers interact with AI systems.

Similarly, the German Government stated in its AI Strategy of 2018 that it will promote research regarding explainability and accountability of decision-making systems, and promote research and development for applications that protect consumers' interests and privacy (p. 16).

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

N/A.

CHAPTER 4 – TELECOMMUNICATION AND INFORMATION SOCIETY

WP 4.1. AI SAFETY AND CYBERSECURITY

Questionnaire the Netherlands

1. Which authorities are competent for safety and cybersecurity?

- For product safety: [the Netherlands Food and Consumer Product Safety Authority](#), (operating under the auspices of the Dutch Ministry of Agriculture, Nature and Food Quality)
- For consumer protection (and therefore for some security-related obligations): the [Authority for Consumers & Markets](#)
- For data protection: the [Autoriteit Persoonsgegevens](#) (AP)
- For cybersecurity in general:
 - o The [National cyber Security Centre](#), operating under the Dutch Ministry of Justice and Security.
 - o Incident reporting is to the Dutch [CSIRT](#), which operates under the Ministry of Economic Affairs and Climate.
 - o Critical infrastructures are overseen by the [National Coordinator on the Fight against Terrorism and Security](#), operating under the Ministry of Justice and Safety.
 - o In 2018, the Ministry of Economic Affairs and Climate Policy established the [Digital Trust Center](#), which has as its mission to inform businesses on how to implement cybersecurity in their business.
- For sectoral cybersecurity regimes:
 - o Telecoms: the [Telecoms Agency](#)
 - o Finance
 - [De Nederlandsche Bank](#)
 - [The Autoriteit Financiële Markten](#)

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

- General initiatives on digitisation
 - o The updated [Digitisation Strategy 2.0](#) names AI as one of the priorities for the coming ten years. Digital resilience is also named as a separate priority (p. 24). For this purpose, the focus lies mainly on awareness building and ensuring minimum requirements for safety through the Radio Equipment Directive and the EU Cybersecurity Act (both of which have now been adopted).
 - o The Government's digital agenda [NL Digibeter](#) 2020 has listed several proposals which may impact the safety of AI systems used by governments. Such proposals include a Human Rights Impact Assessment, to be developed in 2021, design principles to avoid discrimination by AI systems in 2020 and a hackathon to develop safer AI systems.
 - o Within the framework of the Knowledge and Innovation Covenant 2023, budget was made available for [research into data and intelligence](#). Proposals may range from 750,000 to 3,000,000 EUR.
- Artificial intelligence (AI) initiatives in general
 - o In the [2019 Strategic Action Plan for AI](#), the Dutch government identified three tracks on which the artificial intelligence policy of the Netherlands is built. These

- tracks are 1) capitalising on societal and economic opportunities, 2) ensure a suitable economic climate for economy and society and 3) strengthening the foundations. Security-related policies are found under 1) and 3). Under track 1), the Ministry of the Interior will experiment on AI, with a focus on ethics by design and algorithm transparency (p. 15 and further). For this purpose, the [National Police Lab AI](#) was established. Under track 3) the initiatives include: 1) research into the legal aspects of decision-making algorithms, facial recognition algorithms and European certification of AI systems in the administration of justice. Moreover, the [government](#) also intends to invest in research into responsible use of AI as well as the transparency/explainability of algorithms (p. 40 and 42). To ensure that AI is used in such a way that everyone can trust it, the Dutch Government has the NEN Standards Committee share best practices and develop frameworks for ethically responsible AI systems and has it contribute to the development of global AI Standards (p. 45). For this purpose, the NEN has its own [standardisation committee](#) on AI and Big Data. More specifically in the field of Cyber Security, [actions](#) include research on the impact of the use of AI on national security, as well as research that is being commissioned by the Cyber Security Council into the use of new technology – including AI – for cyber defence (p. 51).
- Several policy briefs have been published on the use of AI in government functions. These include a [policy brief](#) on algorithms used by the government regarding transparency, a letter on the use of AI in legal proceedings, as well as a policy brief on safeguards against the use of data analyses by the government. The latter document contains guidance on what governments should do with regard to AI and includes explainability requirements, information to the public, validation and audits, auditability, human-in-the-loop (especially required for profiling purposes).
 - Product Safety
 - No documents have been found from the NVWA regarding AI-based products.
 - Data Protection
 - On 17 February 2020, the *Autoriteit Persoonsgegevens* published a [position paper](#) on the supervision of algorithms and AI systems. In it, they clarify their role as supervisor over the GDPR implications of AI systems.
 - Cyber security (non-sectoral)
 - On 17 November 2018, the Netherlands adopted the Act on the Implementation of Directive 2016/1148 (the [Wet Beveiliging Netwerk- en Informatiesystemen](#)). The obligations listed in the Act run parallel to the obligations of the Belgian NIS Act. Implementing this Act, the [Decision on the Security of Network and Information Systems](#) was adopted on 30 October 2018; it lists the sectors to be appointed OES under the Dutch NIS Act.
 - In the [National Cyber Security Agenda](#) (published on 20 April 2018), the Dutch Government acknowledges that “key technologies such as big data, 5G, quantum computers and artificial intelligence ensures that the digital domain and the physical domain are becoming more closely interwoven”. It underlined seven general ambitions of the Netherlands regarding cybersecurity in general. These include that the Netherlands has adequate digital capabilities to detect, mitigate and respond to cyber threats, as well as that the Netherlands should be at the forefront of digitally secure hardware and software. The focus for the latter is mostly on international standardisation.
 - The NCSC’s [Cybersecurity Assessment Netherlands 2019](#) identifies AI as a point of attention in its section *Looking Ahead to 2021*. First, it mentions that AI can

- become an interesting target for malicious actors, as well as create unpredictable results. AI systems are also identified as a means that can be used to launch cyber-attacks and to defend against them. The NCSC's [Cyber Security Assessment Netherlands 2020](#) further underlines that the spread of autonomous systems will lead to increased risks for digital security, amongst others due to the increased proliferation of IoT devices and the increased possibility for cyber-attacks.
- The NCSC published its [National Cyber Security Research Agenda III](#) on 5 June 2018. It identifies the main research challenges for cybersecurity around five pillars: 1. Design, 2. Defence, 3. Attacks, 4. Governance and 5. Privacy. In all five pillars, AI takes a role. For example, in pillar 2, automated defence, anomaly detection and monitoring (e.g. using AI, machine learning or visualisation) are example topics. Pillar 3 will consist of research on attacks on new ICTs, including AI. Research will also be conducted in standards and certification, as well as intermediary liability. For the final pillar, privacy enhancing technologies and privacy by design deserve mentioning.
 - The Digital Trust Center has provided several tools and principles to enable businesses to identify and mitigate their cybersecurity risks. These tools include a [risk class identification tool](#), [five basic principles](#) for doing business in a digitally safe way, a basic [cyber resilience scan](#), etc.
 - The [Horizon Scan National Security 2020](#) identifies autonomy and cognition by IT systems (i.e., AI) as risks to be taken into account for national security.
 - The Ministry of Economic Affairs and Climate Policy and the Ministry of Justice and Security have published a [Roadmap for Digital Hard-and Software Security](#). It aims to provide a coordinated approach to contribute to the implementation of the Dutch Cybersecurity Agenda. It is based on five principles: i) a product life-cycle approach, ii) joint responsibility of the provider and user, iii) maintaining a balance of private and public values, iv) using a portfolio approach and v) maintaining room for a complementary approach. The proposed measures include ensuring standardisation (through collaboration with existing incentives), developing a monitoring mechanism with the public and private sector, launching a pilot for a range of sector-specific tests, cybersecurity research, active cooperation with the EU regarding liability, exploring possibilities for regulatory compliance, awareness campaigns and empowerment and national government procurement policies.
- Cybersecurity (sectoral)
- Telecoms
 - On 20 May 2020, the Dutch Parliament adopted an [Act](#) to counter unwanted control over telecoms companies. Any party that wishes to obtain a controlling participation in a Dutch telecommunications company (indicated in an [implementing decision](#)) must notify this to the Dutch Ministry of Economic Affairs and Climate. If the Ministry of Economic Affairs considers this intention to be a threat to the public interest, it may impose conditions to the participation or even forbid the transaction.
 - The Telecoms Agency's year plan, [Onwards to a safe and resilient digital infrastructure](#), mentions that, in order to ensure digital resilience throughout the Netherlands, AI creates additional risks for digital resilience within the Netherlands. The proposed policy response is limited to thematic studies in this regard. For 2021, the intended measures include collaborating with supervisory authorities on the meaning of AI, to explain AI in the use of digital identification, digital transactions and

- the use of 'alternative' trust services, continuing cooperation within European institutions.
- Before adopting its 2021 supervision plan, The Telecoms Agency commissioned a [study by Dialogic](#) on the current use of AI and expected developments, as well as the risks and what the Telecoms Agency can do with them. The cyber(in)security of AI systems was considered an explicit risk.
 - Finance
 - The Netherlands have also [implemented the](#) Payment Services Directive and the [MiFiD II Directive](#), thus also adopting their requirements on the safety of algorithmic trading systems and safeguarding against operational risks.
 - In 2019, the DNB published a [report](#) on six principles for the use of AI by financial institutions. These principles ('SAFEST') have within them at least one security component. For example, the requirement of soundness includes requirements regarding data quality and compliance-by-design.
 - In its [Supervisory Strategy 2021-2024](#), the DNB identified as one of the pillars of its supervision to anticipate on coming technologies, such as artificial intelligence. In it, they expressed the ambition to increase security. However, no concrete AI-specific proposals were formulated.
 - On 15 March 2018, the AFM published a [report](#) on the risks of robo-advice, in which it clarified the opportunities and risks of robo-advice and its role.
 - Mobility
 - The Netherlands amended the Road Traffic Act of 1994, making it possible to carry out experiments with self-driving cars after obtaining a permit.

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

A. *The Strategic Action Plan on AI*

As mentioned, the [Strategic Action Plan](#) for AI mentions three tracks; i) capitalising on societal and economic opportunities, 2) ensuring a suitable economic climate for economy and society and 3) strengthening the legal foundations. Security-related policies were found mostly under 1) and 3).

The first track lists the following intended actions (p. 14):

- A new Knowledge and Innovation Agenda, including research into design principles for AI in the legal domain.
- A digital source on AI; round tables on the public domain and the technologies applies.
- The Ministry of the Interior and Kingdom Relations, the Association of Netherlands Municipalities and others will experiment with AI, with a focus on ethics by design and algorithm transparency.
- Improving access to innovation funding.
- Handing information to SMEs on AI.

Actions that are already underway include the National Police Lab AI, conducting research in how AI can be used by police authorities. Another [project](#) includes a study on the system design principles for a new generation of intelligent systems within the legal domain.

The second track focuses mainly on increasing AI take-up in general and will therefore not be discussed under this heading on safety and security.

The policies under the third track (Strengthening the Legal Foundations) were already discussed above.

B. The Dutch Digitisation Strategy 2.0

As priorities, the [Dutch Digitisation Strategy 2.0](#) wishes to create clear frameworks that strengthen confidence in AI by safeguarding human autonomy and control (p. 16). Under the heading “Digital Government”, several initiatives are planned that relate to AI safety and security. These include issuing a policy letter on AI and public values, as well as assessing the potentials and risks of algorithm-based decisions within the context of safeguarding public values (p. 23).

Under the heading “Digital Resilience”, achievements at the time included deploying 95 million EUR in additional structural resources earmarked by the government for cyber security (p.24). Planned actions include (p. 25):

- Focusing on structure and adaptive risk management:
 - o Increasing awareness
 - o Improving control measures
 - o Practice and testing
 - o Control and intervention
- The Dutch Government intends to realise the Nationwide Coverage System, enabling the broader, more efficient and effective sharing of cyber security information between public and privacy sector parties.
- The DTC is supporting the establishment of new partnerships, such as the North Netherland cyber resilience centre (focused on the high tech industry). A total of 1 million EUR will be made available for new partnerships over the course of 2019.
- The Netherlands wishes to see the EU introduce minimum digital safety requirements for all internet devices through the Radio Equipment Directive. No specific intentions to adapt the existing implementation are known.
- The Netherlands is also committed to the active development and implementation of EU-wise cyber security certification systems for ICT products, services and processes as a part of the Cyber Security Act.

The following [initiatives](#) are also ongoing under the heading “for a safe digital society” (p.39-40)

- The Dutch Cyber Security Agenda has been launched, focusing on 7 lines of action (discussed below). Initiatives include the start of investments in capacity and expertise at bodies such as the NCC, security and intelligence services, investigation services and the Ministry of Defence; private-public partnerships on a range of projects; developing a cyber security risk model for businesses; etc. The focus of the Dutch Government will lie more on implementation.
- The Digital Trust Center (DTC) will provide entrepreneurs with up-to-date information and concrete advice on cybersecurity threats. Such information includes a Roadmap on Secure Digital Hard- and Software, a document outlining guidance on how to achieve more secure IoT products in general. For this purpose, 1 million EUR will be made available for new partnerships.
- The Netherlands would also advocate for the adoption of the Cybersecurity Act; it has now been adopted.

- The Ministry of Defence would also update its Cyber Strategy over the course of 2019.

Under the heading “Basic rights and ethics in the digital age”, the Digitisation Strategy 2.0 lists the following initiatives:

- The government has called on the Netherlands Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid) will issue recommendations on the threats and opportunities of artificial intelligence. No recommendations have been made as of yet.
- The Minister for Legal Protection was to issue a letter on the legal impact of developments in the field of algorithms and artificial intelligence in the autumn of 2018.

In an effort to bolster the Netherlands’ digital resilience, the following agreements have also been reached:

- The Cyber Security Alliance will test organisations’ core systems.
- The Ministry of Defence will be working with stakeholders to explore the options for a Cyber Innovation Hub where ministries, research institutions and business can collaborate on cyber security issues.
- In the class room, the Dutch Government will also present copies of a comic book called ‘Donald Duck explores the digital world’, aiming to educate children in secure online practices.

C. NL Digibeter

The [Digibeter](#) lists the following initiatives which deserve mentioning for the protection of public values when deploying AI systems (27-28):

- Early 2021, the government wishes to publish a Human Rights Impact Assessment for governments, in order to detect risks in digitisation projects.
- Design principles for AI systems which allow developers to prevent discrimination by AI systems.

The NL Digibeter also focuses on standardisation (p. 93-94). Guidance was published on Open Standards.²⁸ It is important to note that the government also will publish procurement requirements for cyber-secure equipment (p. 94-95). These have not yet been developed, however. So far, the only requirement is that every webpage by the government is secured.

D. The National Cybersecurity Agenda

In the Dutch Cybersecurity Agenda, the Dutch government has acknowledged that the rise of new technologies ensure that the digital domain and the physical domain are becoming more intertwined. Those same developments have led to an increase in the vulnerabilities in the digital domain. The Dutch government therefore clearly underlines the importance of cybersecurity in the years to come.

This has led to the adoption of seven objectives in the *Dutch Cybersecurity Agenda*:

1. The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats.
2. The Netherlands contributes to international peace and security in the digital domain.
3. The Netherlands is at the forefront of digitally secure hardware and software.
4. The Netherlands has resilient processes and a robust infrastructure.
5. The Netherlands has successful barriers against cybercrime.

²⁸ See: <https://beslisboom.forumstandaardisatie.nl/content/beslisboom-voor-de-pas-toe-leg-uit-lijst>.

6. The Netherlands leads the way in the field of cybersecurity knowledge development.
7. The Netherlands has an integrated and strong public-private approach to cybersecurity.

These goals have been analysed individually. Especially objectives 3, 4 and 6 appears to lie within the remit of the Ministry of Economic Affairs.

Objective 3 (ensure digitally secure hard- and software) has as its objective to take a cohesive set of measures to encourage and enhance the digital security of hardware and software in a balanced way, and for which various parties have a responsibility. The Netherlands will therefore continue to implement the Roadmap for Digitally Secure Hardware and Software, with the following objectives:

- The Netherlands will encourage standardisation and certification initiatives, as well as supervision and enforcement to prevent digital security risks in hardware and software.
- The Netherlands will work to improve the detection of digital security risks in hardware and software by testing digital products and making risks clear.
- The Netherlands will work on mitigating digital security risks through a liability regime, and by increasing awareness and by offering a perspective for action for citizens and businesses.
- The Netherlands will strive for the realisation of a set of basic principles to foster the digital security of hardware and software.

The measures proposed to achieve Objective 3 include:

- Encouraging the adoption of international standards, partnerships and framework. The Netherlands wants to proactively join relevant European and global standardisation and certification initiatives through the NEN standardisation platform. The Netherlands will also pursue multilateral cooperation on standardisation for the Internet of Things, amongst others through the Global Forum on Cyber Expertise.
- The government wishes to develop a monitoring system with information about the digital security of digital products, with specific attention to Internet of Things devices. The government will include international experiences.
- The government is currently discussion focus areas for liability with regard to digitally insecure hard- and software with stakeholders and academics. In addition, the Netherlands is an active participant in the Expert Group on Liability and New Technologies; the Netherlands also proposed an obligation to make security updates mandatory in all cases involving software supplied to a consumer.
- The government is also investigating whether minimum requirements can be set through the Radio Equipment Directive.

Objective 4 (Resilient digital processes and a robust infrastructure) imply that all relevant parties will be involved in the continuity and digital resilience of critical processes, increasing the resilience of the entire chain. The Netherlands also aim to improve the quality of open source software and the accelerated adoption of modern internet protocols and internet standards.

The measures proposed to achieve Objective 3 include:

- Setting agendas in Europe for modern internet protocols and standards.
- Using cybersecurity requirements when procuring ICT products and services.
- Exploring the development of a certification system for cybersecurity providers so that public authorities and private parties know who they can acquire secure services from.

Objective 6 (Cybersecurity Knowledge Development) identifies the urgent need to maintain and deepen high-quality knowledge development in the Netherlands. It is therefore important to improve research, but also to provide innovative solutions to businesses and that citizens and

businesses continue to develop their knowledge to protect themselves against digital threats. There is moreover a need to increase digital literacy.

The measures proposed to achieve Objective 6 include:

- Structural investments in fundamental and applied cybersecurity research.
- Listing digital skills, including media-literacy and cybersecurity as integral focus areas in the review of the primary and secondary education curriculum.
- Encouraging the business community and civil society organisations to further develop the digital skills of employees and citizens and to ensure the continuity and cohesion between various awareness campaigns to that effect.

E. National Cyber Security Research Agenda

This was discussed above.

F. The Digital Trust Center

This was discussed above.

G. Horizon Scan National Security 2020

This document did not contain any AI-specific proposals.

H. Roadmap for Digital Hard- and Software Security

The Roadmap for Digital Hard- and Software Security was adopted in April 2018. It proposes the following measures:

- Standards and certification:
 - o Ensuring adoption of the EU Cybersecurity Act.
 - o Promoting standardisation, inter alia by launching initiatives such as Partnering trust, the Secure Software Alliance and the Smart Industry Standardisation Platform. The Netherlands will also seek cooperation with existing actors in the field.
 - o The Netherlands aim to forge links with global standardisation and certification initiatives via the NEN standardisation platform, which can play an important role in streamlining Netherlands-based activities in the various international standardisation institutions.
 - o The Netherlands will invest in multilateral collaboration in the field of IoT standardisation.
- Monitoring the digital security of products: the Dutch government intends to cooperate with the private sector and other relevant stakeholders to develop a monitoring mechanism offering information on the digital security of products, with a specific focus on IoT products.
- Cleaning up infected user products.
- Testing for digital security.
- Cybersecurity research.
- Liability (cf. Cybersecurity Agenda).
 - o The Dutch Government supports European initiatives in this regard.
- Statutory requirements, through the Radio Equipment Directive.
- Awareness campaigns and empowerment.
- National government procurement policy.

Further information on the Roadmap for Digital Hard- and Software Security can be derived from letters by the Ministry of Economic Affairs and Climate to the Dutch Second Chamber (the Dutch equivalent of the Chamber of Representatives). For example, in a letter to Parliament from 14

December 2020, the Netherlands has connected its initiative to connect requirements in the RED Directive to the general review of the General Product Safety Directive, currently going on at the EU level. Moreover, the Netherlands continue to plead for mandatory certification with regard to the implementation of the Cybersecurity Act.

I. Act to counter unwanted control

This was already discussed above.

J. Telecoms Agency, Onwards to a secure and resilient digital infrastructure

In general, the research is focused on gaining knowledge on the impact of these new techniques, including AI (see above). It gives guidance on what the Telecoms Agency will do with regard to artificial intelligence, as mentioned above.

One such study to be mentioned in this regard is the study conducted by Dialogic on *Managing AI Use in Telecom Infrastructures* (see above). In it, it outlined a few general risks related to AI and the role that telecoms agencies can play within it, giving advice to the Telecoms Agency on what it can do as a supervisor.

K. Experimental Law on Self-Driving Vehicles

On 26 April 2018, the Second Chamber adopted the Experiments Act on Self-Driving Cars. It amended the Road Traffic Act of 1994, making it possible to carry out experiments with self-driving cars after obtaining a permit.

L. Autoriteit Persoonsgegevens, Supervision of Algorithms

On 17 February 2020, the Dutch Data Protection Authority published a [report](#) on the supervision of AI algorithms, clarifying what algorithms are, how they relate to data protection legislation and how the Authority will organize its supervision with a view to ensure that the use of AI complies with data protection principles. Interesting to note is that the report focuses not only on the impact that AI can have on privacy, but also on the impact that AI can have on other rights, such as non-discrimination, when discussing the DPIA requirement.

M. Standards commission Artificial Intelligence and Big Data in the NEN

It must be noted that the [NEN](#) has started a standards commission 'Artificial Intelligence and Big Data', that can develop standards in the field of big data and artificial intelligence. It is a member of the ISO commission SC 42 Artificial Intelligence and thus contributes to standards for AI systems.

N. Principles for the use of AI in the financial sector

In its 2019 report *General principles for the use of AI in the financial sector*, the Dutch National Bank adopted seven principles regarding the use of artificial intelligence in the financial sector. These principles (known as the 'SAFEST' principles) comprise of the following:

- Soundness
- Accountability
- Fairness
- Ethics
- Skills
- Transparency

The principle of *soundness* entails that AI applications in the financial sector should be reliable and accurate, behave predictably and operate within the boundaries of applicable rules and regulations, such as the GDPR, especially when systemic risks might arise. These measures should

also be proven by financial service providers. This principle is implemented through five general rules: (i) Ensure general compliance with regulatory obligations regarding AI applications, (ii) Mitigate financial (and other relevant) prudential risks in the development and use of AI applications; (iii) Pay special attention to the mitigation of model risk for material AI applications; (iv) safeguard and improve the quality of data used by AI applications and (v) remain in control of (the correct functioning of) procured and/or outsourced AI applications. These principles relate to safety requirements one may find in, for example, the AI Act Proposal and Regulation 2017/589. This principle therefore relates, essentially, to having a sound safety and security policy when using artificial intelligence in the financial sector.

In its 2020 report, [Change for Trust](#), the DNB also came to several conclusions that more security-related policies are needed. It found that improvements in the availability and the quality of data are necessary, not only for service provision, but also for security (p. 46). In extending the availability of data, financial stability and security must also be taken as important focus points. More safeguards should be implemented, also due to the enhanced risks of financial fraud. The DNB underlines the necessity of sector-wide cooperation to avoid coordination failure in implementing policies. Therefore, each party must report fraud detection and know-your-customer issues, to avoid that changes are missed in the system. A general conclusion is also that cooperation initiatives on cybersecurity, KYC requirements and transaction monitoring are necessary to ensure the effectiveness and efficiency of the combat against fraud and anti-money laundering measures. The DNB is positive towards such cooperation, insofar as governance, responsibilities and data protection are adequately implemented.

In its Vision on Supervision, the DNB extends its focus to supervision. The DNB intends to focus on mitigating operational risks and will address financial institutions on the quality of the data they use. The DNB also expressed the wish to start using AI themselves.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

The Digital Trust Center did not explicitly relate to the work packages, but remains relevant to cybersecurity by providing guidance to companies on how to implement cybersecurity. The planned procurement guidelines on cybersecurity were also not mentioned in the work package, but may contribute to higher cybersecurity by government regulators.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Guidance to regulators regarding the application to their rules with regard to AI: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of studies and reports such as the one published by the ACM, the AP, the Telecoms the DNB and the AFM (and mentioned above) serve a similar purpose: they intend to clarify the role of the regulators on how to act with regard to AI systems. This guidance is still mostly absent in Belgium, with the exception of any policy documents listed in the D1 report.

B. How do the measures try to achieve their purpose?

The above listed goal is pursued by conducting analyses and drafting reports, which are then publicly disseminated through a report and, potentially, workshops.

C. Where possible to assess, to what extent did these measures achieve their purpose?

It is difficult to assess whether the purposes have been achieved. Some mention is made in e.g. policy briefs on these reports being made, but there are no data so far on the take up of these policies. This is also likely due to the recent nature of these reports.

D. Where possible to assess, what impact did the measures have on the government budget?

This will depend on the FTEs used in drafting these reports. It is therefore hard to assess these measures' exact impact.

E. To what extent are the abovementioned measures relevant to the Belgian context and purposes, as well as the identified gaps?

As mentioned above, such guidance is rather limited at the Belgian level. Therefore, the use of such guidance by Belgian independent regulators can be useful. However, principles must not be adopted for the sake of creating principles; principles must be taken up and translated into organisation cultures or into law. In many of these fields, policy takes place mostly at the European level. It therefore makes sense to focus the discussion at this level and to focus on the implementation only at Belgian level.

3.2.2. Proposal 2 – Setting up a standards committee for AI in the national standardisation organisation: efficiency and budgetary aspects

A. Which purposes were identified/established?

The creation of a specific standardisation body helps achieve the purpose identified in both the SAPAI Report and the Digitisation Strategy to exchange best practices and develop frameworks for reliable and ethically responsible AI applications, as well as to contribute to the development of global AI standards.

B. How do the measures try to achieve their purpose?

By setting up a standardisation committee within its own standardisation organisation, the NEN participates in the development of standards for AI through the ISO. This helps the Dutch build the standards for artificial intelligence.

C. Where possible to assess, to what extent did these measures achieve their purpose?

It is difficult to ascertain the specific input that the NEN had on the proliferation of artificial intelligence standards.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. So far, the NBN has no specific standardisation committee on artificial intelligence. Belgium can

3.2.3. Proposal 3 – Setting up a Digital Trust Center: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose was to provide information to companies on how to implement cybersecurity.

B. How do the measures try to achieve their purpose?

The goal is to provide a single entity that develops tools and provides this guidance.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (if applicable)

Such initiatives are also possible to the Belgian Government. The Center for Cybersecurity Belgium already plays a similar role. Its role can be expanded upon to manage AI systems more effectively.

3.2.4. Proposal 4 – Facilitating the testing of self-driving cars and other AI systems: efficiency and budgetary aspects

A. Which purposes were identified/established?

Through facilitating the testing of self-driving cars, the Dutch Government attempts to provide an easier way into the deployment of AI for the purposes of security and safety.

B. How do the measures try to achieve their purpose?

By allowing testing, it is possible to deploy a new technology. By providing regulation, it is ensured that this is done safely.

C. Where possible to assess, to what extent did these measures achieve their purpose?

This is difficult to ascertain. It made testing possible, but no data is available on the extent of testing of self-driving cars in the Netherlands.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (if applicable)

By increasing the opportunities for testing, the Belgian authorities can also ensure that AI is deployed safely and securely. However, if Belgium wishes to do so, it will have to take into account the division between the federal government and the regional governments when it comes to mobility

3.2.5. Proposal 5 – Investing in research projects: efficiency and budgetary aspects

A. What purposes were identified?

Projects such as the National Police AI Lab, the Knowledge and Innovation Covenant, and other research plans mentioned in the documents above, serve to gain knowledge of the opportunities and risks of artificial intelligence. This not only relates to the possibility of technical applications of AI systems, but also to their technical, operational, legal and societal risks.

B. How do the measures try to achieve their purpose?

By conducting research in conjunction with public authorities and private stakeholders, the research attempts to ensure that parties gain knowledge of artificial intelligence. On the one hand, this implies that technical progress is made in the field of AI. On the other hand, it implies that knowledge of the risks of AI systems is also increased, allowing a more effective use in accordance with public values.

C. To what extent did these measures achieve their purpose?

The research has resulted in some studies, as mentioned above. Thus, there was an addition to the knowledge capital of the Netherlands regarding the use of AI. However, the practical effects of such knowledge gains are too fresh to properly assess their impact.

D. *If possible to assess, what impact did these measures have on the government budget?*

Exact numbers would require an overview of the Dutch government budget. This is difficult to assess, as the expenses would have to be isolated from the Dutch general government spending. However, some of the policy documents give indications as to the budgetary impact of some of these funds. For example, the [SAPAI Report](#) mentioned a recent call from the Netherlands Organisation for Scientific Research (NOW) worth 2.3 million EUR (p. 44 and 59). The ministry of Social Affairs and Employment are also investing 3 million EUR in research on the impact of AI on work and employment (p. 57). According to the SAPAI Report, the total government expenditure on AI projects in general is 45 million EUR a year (p.61).

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (if applicable)*

Nothing prevents Belgium from taking such initiatives itself. Coordination with regional entities may be required, as some research is a competence of the Communities. Initiatives are already underway, such as the Flemish Action Plan Artificial Intelligence and Digital4Wallonia.

3.2.6. Proposal 6 – Awareness building through (secondary) education: efficiency and budgetary aspects

A. *What purposes were identified?*

The purpose of training is to increase the digital literacy of citizens and thus to ensure that sound cybersecurity habits are adopted. After all, to ensure adequate cybersecurity – not only of AI systems, but in general – users must have the knowledge to make effective use of the digital means made available to them.

B. *How do the measures try to achieve their purpose?*

Through the use of education, the purpose is to achieve better knowledge among the general public in order to ensure that cybersecurity is improved everywhere.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

No information available.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No information available.

E. *Are the abovementioned findings relevant to the Belgian context and purposes, as well as to the relevant gaps?*

The gaps did not mention cybersecurity education, as this is not an AI-specific goal. The goal applies in general and thus also to AI. However, this will continue to be a necessary complement of any AI safety-related policy and AI-cybersecurity-related policy: to inform the users of what is to be done. Using the school system is an obvious means to the goal, as then, students learn about technology soon and take these habits into their adult lives. It must be noted under the Belgian context however, that this is not a field in which the FPS Economics can intervene, without at least cooperating with the Ministries of Education, which are at Community level.

3.2.7. Proposal 7 – Principles for the use of artificial intelligence in the financial sector (and other sectors as well): efficiency and budgetary aspects

A. *Which purposes were identified?*

In the report, it is mentioned that it is challenging to get a comprehensive overview of the AI-specific challenges that financial firms face. The principles intend to provide a framework to help financial firms to assess how responsible their use of AI is and to facilitate their own assessment

of the direction and desirability of future regulatory developments. This purpose appears to lie mainly in giving guidance to finance firms on how to deploy AI responsibly.

B. *How do the measures try to achieve that purpose?*

The goal of achieving more responsible AI use in the finance sector is pursued by disseminating best practices amongst financial firms.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

At the time of writing, there is no information available on any take-up of these guidelines by financial firms in the Netherlands.

D. *Where possible to assess, what impact did the measures have on the government budget?*

The budgetary impact will depend on the FTEs implied in the drafting of this document. No such information is available.

E. *Are the abovementioned findings relevant to the Belgian context and purposes, as to the gaps?*

Any type of standard must be developed; this can also take place through the use of non-binding soft law principles. However, take-up must be monitored in order to ensure that such principles result in any policy at the ground. The financial sector, given its scale, is usually better regulated at the EU level.

3.2.8. Proposal 8 – Supporting EU regulatory initiatives such as the Cybersecurity Act, the Radio Equipment Directive and European regulatory initiatives: efficiency and budgetary aspects

A. *What purpose is identified?*

The purpose identified is to ensure that the existing legal framework applicable to AI ensures adequate safety of AI systems.

B. *How do these measures try to achieve their purpose?*

By supporting the EU legislator in its activities.

C. *To what extent are the purposes achieved?*

No information available, aside from the adoption of some legal instruments such as the Cybersecurity Act. This act is too recent and has not been fully implemented yet, in the absence of a certification mechanism.

D. *If possible to assess, what is the impact of the measures on the government budget?*

No information available.

E. *Are the abovementioned measures relevant to the Belgian context and purposes and to the identified gaps?*

The abovementioned measures may influence the implementation of the fragmented legal framework for cybersecurity and therefore impact the Belgian policy goal of integrating this framework. At the same time, this does not alter the legal framework essentially; more convergence may be required. It may also soon be achieved through the EU, through initiatives such as the AI Act Proposal.

3.2.9. Proposal 9 – An act prohibiting the control of telecommunications infrastructure: efficiency and budgetary aspects

A. *What purpose is identified?*

The purpose is to ensure that foreign actors cannot undermine the security of the Netherlands.

B. How do these measures try to achieve their purpose?

The goal is achieved by subjecting such acquisitions to the control of a government agency. Its effectiveness is yet to be evaluated.

C. To what extent are the purposes achieved?

See under B.

D. If possible to assess, what is the impact of the measures on the government budget?

No information available.

E. Are the abovementioned measures relevant to the Belgian context and purposes and to the identified gaps?

This is a measure that the Belgian government can also take. It does not relate to any of the specified gaps, but may nonetheless contribute to security and safety of AI systems in Belgium.

3.2.10. Proposal 10 – A Human Rights Impact Assessment: efficiency and budgetary aspects

A. What purpose is identified?

The purpose is to ensure that AI systems comply with public values.

B. How do these measures try to achieve their purpose?

By introducing an AI impact assessment prior to deployment.

C. To what extent are the purposes achieved?

None yet (principles must be developed).

D. If possible to assess, what is the impact of the measures on the government budget?

No information available.

E. Are the abovementioned measures relevant to the Belgian context and purposes and to the identified gaps?

This is a measure that the Belgian government can also take. However, such an impact assessment may also come in the form of the certification required by the AI Act Proposal, once adopted. It may therefore be ill-advised to redouble the work of the EU legislator.

Questionnaire France

1. Which authorities are competent for safety and cybersecurity?

- Contract law
 - o The national legislator and the national government
- Tort Law
 - o The national legislator and the national government
- Product Safety
 - o *Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes* ([DGCCRF](#) - Ministère de l'Economie)
- Data Protection
 - o *Commission Nationale de l'Informatique et des Libertés* ([CNIL](#))

- Standardisation
 - o *Association Française de la Normalisation* ([AFNOR](#))
- Digitisation
 - o *Conseil national du numérique* ([CNUM](#))
- Cybersecurity (non-sectoral)
 - o *Agence nationale de la sécurité des systèmes d'information* ([ANSSI](#))
- Cybersecurity (Sectoral)
 - o Telecoms
 - *Autorité de Régulation des Communications Électroniques et des Postes* ([ARCEP](#))
 - o Finance
 - National bank : [Banque de France](#)
 - Prudential supervisory authority : *Autorité de contrôle prudentiel et de résolution* ([ACPR](#)), which is a body of the *Banque de France*
 - Association pour le Management des Risques et des Assurances de l'Entreprise ([AMRAE](#))
- Other
 - o The *Direction Interministérielle du Numérique* ([DINUM](#)) is responsible for the digital transformation of bodies of the State.

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

- Artificial intelligence initiatives in general
 - o From 20 January until 14 March 2017, 17 working groups were assembled at the French Government's request to propose political actions regarding AI in France. Fifty proposals were proposed in several areas. Their [final conclusions](#) and [summary report](#) can be found here. Some recommendations relate to AI safety and security and therefore merit attention for this work package. These include (per working group):
 - From the Working Group on Research: the creation of an Academic Center on Artificial Intelligence (Conclusions, p. 13).
 - From the Working Group on Technology Transfer: the development of methodologies for testing and certification by the LNE (Laboratoire National de Métrologie et d'Essais) (conclusions, p. 91-92 and 104; also see p. 106 *et seq.*), create an AI Foundation that can work around challenges of businesses regarding AI (Conclusions, p. 92 and 105), as well as to create specific platforms regarding specific sectors, including autonomous vehicles (Conclusions, p. 92 and 104).
 - From the Working Group on Autonomous Vehicles: promote a logic-based approach for the taking of decisions to ensure a greater reliability of the developed AI, to clarify the traffic code to ensure an unambiguous interpretation for autonomous vehicles.
 - From the Working Group on Finance: identifying regulatory challenges;
 - From the Working Group on Sovereignty:
 - Developing a platform for the testing, qualification and certification for AI systems (ConfIAnce); to develop an integrative software platform for AI systems; the development of reliable machine learning techniques; the development of a network of platforms for security and cybersecurity (SecureIA).

- From the Working Group on Social and Economic Impact: mind the complementarity between human and machine.
 - On 29 March 2018, the report by Mr. Cédric Villani, [For a Meaningful Artificial Intelligence](#), was published. AI safety- and security-related recommendations can be found in Part 1 (An Economic Policy Based on Data) and 5 (Ethical Considerations of AI).
 - Under Part 1, proposals include the creation of a one-stop shop for all matters on AI (p. 32), facilitating dialogue between the several regulators (p. 34). Yet another proposal includes choosing to focus on four strategic sectors, i.e. health, transport/mobility, environment and defence/security (p. 40). Data policies should be implemented according to each sector (p. 48). The State should lead by example. Therefore, proposals also include to appoint an Interministerial Coordinator, to create a Joint Centre of Excellence for AI at the State level (e.g. DINUM) (p. 54-55). To develop the safety and security of AI systems, public authorities should also focus on making standards more secure, reliable, useable and interoperable: for this purpose, the LNE's responsibilities could be expanded (p. 58).
 - Under Part 5, lots of attention goes to "opening the black box" (p. 114 et *sqq.*). Another point of attention is the presence of algorithmic bias, which may cause discrimination (p. 116-117). For these two, no concrete proposals were formulated. For developing the auditing of AI systems, the report proposes to appoint a body of experts with the requisite skills to do so (p. 117) The teaching of ethics should be included in all engineering courses and the teaching of technology should be made optional in a major/minor system, even for social sciences. This to ensure more mixed profiles. (p. 119-120-. Regarding the impact of predictive policing and LAWS, the report supports informing citizens of their rights (p. 123-124).
- Contract law and consumer protection
 - The [Loi no. 2020-1508 du 3 décembre 2020 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière](#) was given the mandate to implement the Digital Content Directive (2019/770) within a period of ten months. No such decision has been taken at the time of writing.
 - The [Ordonnance n° 2016-131 portant réforme du droit des contrats, du régime général et de la preuve des obligations](#) amended French contract law in many ways that affect the obligation of AI designers to develop and deploy AI systems that are safe to use. One such change includes the creation of a broader obligation of information during negotiations, which affects transparency by AI sellers. Parties cannot contract away this duty. Moreover, the new Article 1195 *Code Civil* allows parties the right to renegotiate the contract in the event of unforeseeable changes, which may affect AI systems' autonomous development (although, it must be noted, that the autonomous nature of AI systems makes unforeseeable events something to be foreseen in advance).
- Data protection
 - The [Loi n° 2016-131 du 7 octobre 2016 pour une République Numérique](#) not only increased the powers of the CNIL to enforce privacy rules (as per the GDPR), but it also mandated the CNIL to act as the main body for the reflection on ethical aspects of new technologies.
 - On 15 September 2017, the CNIL published its report [Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de](#)

[l'intelligence artificielle](#). Based on two principles, the principle of loyalty (i.e., that the service should be rendered in good faith, without attempting to achieve other ends to the user's detriment) and the principle of vigilance (i.e. that one should remain vigilant and not excessively give in to machine bias), the (p. 6 and 48-50), the CNIL has come to adopt six recommendations to governmental and other bodies, which include that AI systems must be made more comprehensible, the design of AI systems should be placed at the service of human liberty and a national audit platform should be built for the audit of algorithms (p. 6). A proposal to strengthen the principle of loyalty includes the proposition to create a "notation agency for algorithms" to make algorithms available and to provide for a space to signal malfunctions (p. 49). Based on these principles, the report provides for five design principles, underlining the importance of the intelligibility, transparency and human intervention for AI systems, all rules which also contribute to the safety of the AI system (p. 50-52). These principles result in policy recommendations. These recommendations are the following: i) all components of the AI system lifecycle (designers, professional users and citizen users) should be trained in ethics (e.g. as the part of their curriculum during their education), that ii) AI systems are made comprehensible by reinforcing existing rights and organising mediations with users, iii) the design of AI systems is to be placed at the service of human freedom, iv) a national platform must be founded for algorithm audits by competent experts, v) research into AI development must be prioritised in order to make France the leader in AI and vi) ethical positions within companies must be strengthened.

- On 19 December 2019, the CNIL published its report [Facial Recognition: for a debate living up to the challenges](#), in which the CNIL gave its guidance on the risks of the use of facial recognition technologies. Aside from giving guidance on the impact of facial recognition technology (including the risk for unprecedented surveillance), the CNIL proposes four requirements for the use of facial recognition: i) draw some red lines, even before experimental use, ii) put respect for people at the heart of the approach (and thus, ask consent and avoid accustoming people to intrusive surveillance), iii) adopt a genuinely experimental approach. The CNIL also clarified its own role.
- Product safety
 - No AI-specific proposals were adopted or published by the DGCCRF. This can be explained by the fact that, as per the Villani Report, the supervision of AI is left to e.g. the CNIL and the ANSSI. They likely have the experience and expertise required to deal with digital systems (including AI systems), but it must be noted that the focus of these institutions lies more with cybersecurity than with safety.
 - The [Décret no. 2018-211 du 28 mars 2018 relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques](#) provides a legal framework for the testing of autonomous vehicles on French roads. The driver must still retain the capacity to take control of the vehicle, so fully autonomous driving is not yet allowed.
- Standardisation
 - AFNOR also has its own standardisation committee on Artificial Intelligence.
 - AFNOR has also hosted several [webinars on Artificial Intelligence](#).
 - In April 2018, AFNOR published its own [White Paper on the Impact and Expectations for Standardisation in Artificial Intelligence](#). This report identified several challenges to the standardisation of AI systems, including a proper estimation of an AI system's robustness, auditability and certification of AI

systems, explicability of AI systems, continuous learning by AI systems validation of the robustness of artificial neurons. AFNOR comes to five recommendations: (i) the concepts and terminology used by several bodies should be harmonised, (ii) a normative strategy should be used for AI robustness (i.e., AI systems should be standardised), (iii) industrial manufacturers should establish standards for interoperability, (iv) questions of ethics and security should be taken into account when drafting standards and (vi) to allow competent bodies to do their work, we need more competence and qualifications related to AI.

- AI and security are mentioned as a specific topic in AFNOR's most recent [standardisation strategy](#).
- Cybersecurity
 - France has also transposed the NIS Directive. The national implementations can be found in the [Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique](#) (NIS Decree) and [three implementing decisions](#).
 - The French Government has adopted a [National Digital Security Strategy](#). It identifies five areas of focus for the cybersecurity in France:
 - 1. France will ensure the defence of its fundamental interests in cyberspace, will reinforce the digital security of its critical infrastructures and do its most to ensure that of its essential operators. Measures taken to this end include the creation of an Expert Panel for Digital Trust,, identifying technologies in which in-depth knowledge is required for cybersecurity and set goals in this regard. Also, active monitoring of the security of technologies will be ensured (p. 14-15). Cyberdefence reserves will also be reserved for operational purposes and France will continue to contribute to voluntary cooperation (p. 17).
 - 2. France will develop cyberspace use that is in line with its values and will protect the digital lines of its citizens. Proposals include that France will equip itself with a clear road map for digital identity delivered by the State (p. 22) and labelling secure platforms (p. 23).
 - 3. France will raise children's awareness of digital security and responsible cyberspace behaviours as of school age. Initial higher education and continuing education will include a section dedicated to digital security adapted to the sector under consideration (p. 26-27).
 - 4. France will develop an environment that is favourable to research and innovation and will make digital security a factor in competitiveness. It will support the development of the economy and the international promotion of its digital products and services, that will be marketed with a high level of ergonomics, trust and security. Initiatives include knowledge transfer to the private sector and integrating the requirements for cybersecurity in their public procurement process (p. 31-34).
 - 5. France will be the driving force behind European strategic autonomy. Initiatives to this end include establishing a road map and cooperating with multilateral organisations (p. 38-40).
 - Together with AMRAE, ANSSI published a [position paper](#) called *Controlling the Digital Risk*, in which they provide a roadmap for businesses on how to implement a cybersecurity strategy.
 - On 3 September 2020, the government has launched a relaunch plan to restore the economy after the COVID-19 pandemic. With a fund of 136 million EUR

- reserved especially for cybersecurity, the plan aims to strengthening the cybersecurity of administrations and any organisations serving citizens.
- As a part of France's post-pandemic relaunch strategy, the government has provided a [document](#) outlining two major offers: (i) increasing the level of cybersecurity by programs by ANSSI consisting of assistance and the funding of projects, as well as (ii) encouraging the creation of CSIRTs at the regional level. The French government has also created a fund of 136 million EUR to reinforce cybersecurity, a sum which is to be managed by ANSSI.
 - In another policy document, [Cybersecrurité: faire face à la menace](#), ANSSUI provides its program for cyber acceleration. The strategy – which liberates 1 billion EUR (of which 720 are public investments) for several initiatives – aims to reach several specific benchmarks regarding funding, employment, the founding of unicorns and the amount of parents in the field. Actions include developing solutions for cybersecurity, improving synergies between the relevant actors, supporting the adoption of cyber solutions, training, as well as the creation of a Cyber Campus in 2021.
 - ANSSI also published several scientific publications on machine learning, including the use of machine learning for security. An example can be found [here](#).
- Cybersecurity (sectoral)
- Electronic Communications
 - In the report [Réseaux du futur](#), the ARCEP published its notes on a reflection of the role of artificial intelligence in telecoms. It outlines the general risks and benefits of AI in telecoms. It identified several main challenges, including a strong need for standardisation and the need for explainability and reliability of the AI system.
 - Finance
 - In December 2018, the ACPR published the report [Artificial intelligence: challenges for the financial sector](#). The document outlines the opportunities and risks of using AI in the financial sector. Identified opportunities include attack detection, fraud detection and risk detection. However, the possibility for attack and the risks of low data quality are also acknowledged as risks. IT considers three lines of action for supervisory authorities, i.e. i) increasing their expertise in data analysis and the use of AI; ii) creating enhanced cooperation between supervisors, more specifically the ACPR and the CNIL and iii) supporting standardisation and normalisation initiatives, as well as other work, towards increased auditability and explainability of smart algorithms.
 - In June 2020, the ACPR published its discussion document [Governance of Artificial Intelligence in Finance](#). It identified four independent criteria for evaluating AI algorithms and tools in finance, i.e. appropriate data management, performance, stability and explainability of AI systems. The document thus gives guidance on how to implement AI systems in the finance sector.
 - ACPR and Banque de France published several studies on the implication of digitisation in the financial sector.
 - The most [recent Annual Reports](#) of the ACPR illustrate that the ACPR has continually been active with AI. In the 2018 Annual Report, the ACPR signalled that it wished to increase research in the use of “suptech” (supervisory technology). In its 2019 Annual Report, the ACPR indicated that, after its study on AI in the financial sector, it has set up “voluntary workshops” to conduct AI-related research projects

- Other
 - o In a [2016 report](#) to the State Secretary responsible for Digital Affairs, two authors gave five recommendations on how to regulate artificial intelligence. These recommendations were 1° Create a collaborative scientific platform for the development of software tools and testing methods for algorithms, 2° Create a specialised control cell for the control of the Digital Economy, under the auspices of the DGCCRF, 3° Communicate on the functioning of algorithms and identify the person responsible for its functioning where possible, 4° Identify new services in the fields of employment, health, finance and insurances and 5° Launch training programs for operators of public services involving algorithms. Especially recommendation 3° is relevant for AI safety, as the DGCCRF is the entity that is also responsible for product safety.

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

The proposals include:

- From the Conclusions of the *France IA* Working Groups:
 - o From the Working Group on Research
 - The creation of an Academic Center on Artificial Intelligence.
 - The development of methodologies for testing and certification by the LNE.
 - The creation of an AI Foundation.
 - The creation of specific platforms regarding specific sectors, including autonomous vehicles.
 - o From the Working Group on Autonomous Vehicles
 - Promote specific design principles.
 - Clarifying the traffic code to ensure an unambiguous interpretation for autonomous driving systems.
 - o From the Working Group on Finance
 - Identifying regulatory challenges.
 - o From the Working Group on Sovereignty
 - To develop a platform for the testing, qualification and certification for AI systems.
 - To develop integrating software platforms for AI systems.
 - To develop a network of platforms for security and cybersecurity.
 - o From the Working Group on Social and Economic Impact: look at the complementarity between human and machine.
- From the *Villani* report:
 - o The creation of a one-stop shop for all matters on AI.
 - o Facilitating dialogue between all regulators.
 - o Focusing on four strategic sectors, which each receive their own data policy.
 - o The appointment of a Interministerial coordinator for AI-based matters.
 - o The creation of a Joint Centre of Excellence for AI at the State level.
 - o Expanding the LNE's responsibilities for making standards more secure, reliable, useable and interoperable (also cf. Conclusions France IA).
 - o Appointing a body of experts for the auditing of algorithms.

- including ethics in technical education and allowing mixed major/minor programs between social fields (such as ethics and law) and technical fields (such as engineering).
- Reforming the Civil Code to allow for hardship.
- Publishing guidance on how to apply applicable laws to specific technologies, including data protection and financial regulation (cf. CNIL reports and ACPR reports).
- Create a Cyber Campus and support funding in relevant research.
- Create a control for digital technologies at the DGCCRF.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

The proposals listed above regarding the integration of cybersecurity in education and the supporting of funding in relevant research do not relate to any of the gaps identified in the D1 report. However, they remain relevant for cybersecurity purposes.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Creation of an Academic Centre on Artificial Intelligence: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purposes identified to support research in the field.

B. How do the measures try to achieve their purpose?

The Centre attempts to organise specialised seminars and acts as a meeting point for specialists from several sectors.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Some Belgian initiatives, such as AI4Belgium and the Flemish Knowledge Centre Data & Society already achieve this purpose for the Belgian context.

3.2.2. Proposal 2 – Empowering the LNE to develop testing and certification methods for AI systems: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of such an initiative is to provide the tools to allow all to explain and to warrant the safety of AI systems on the French markets.

B. How do the measures try to achieve their purpose?

By empowering a government agency to develop such certification methods.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, no information is available regarding the certification methods that have been developed under this initiative. Projects are underway, but no deliverables were found. Therefore, the impact on the achievement of these purposes and the impact on the budget cannot be assessed as yet.

D. Where possible to assess, what impact did the measures have on the government budget?

See above.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Certification methods can help make standards more accessible and useable and thus contribute greatly to the safety of AI systems. Belgium also has the institutions available, more specifically through the NBN. However, one must be aware that such standardisation initiatives are also best implemented at scale. Therefore, it may be recommended to focus on participation in multilateral fora and the EU. Examples include the implementation of the Cybersecurity Act and (once adopted) the AI Act Proposal. However, one can always create an example of out a niche application. It appears that France has a (minor) intention to set the tone in this conversation.

3.2.3. Proposal 3 – The creation of an AI foundation: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose is to create a place for professionals to exchange and disseminate knowledge on progress, opportunities,, and risks related to artificial intelligence.

B. How do the measures try to achieve their purpose?

The creation of an AI Foundation is yet another body where such knowledge can be built.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Knowledge does not explicitly relate to one of the gaps selected in the D1 report, but remains important for the safety and security of AI systems. One of the main problems of safety and security is ignorance of the people. Any initiatives in this regard are more than welcome. Such initiatives are also partly underway, such as the initiatives taken through Agoria, AI4Belgium, DigitalWallonia and the Flemish Knowledge Centre Data & Society.

3.2.4. Proposal 4 – Specific sectoral platforms for AI: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose identified is to promote experimentation and to provide tools for the development of the relevant systems. This also includes the secure development of such systems.

B. How do the measures try to achieve their purpose?

By setting up specific platforms, specific knowledge to those sectors can be integrated, allowing for a more in-depth knowledge in the field.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

The same answer can be given as is applicable for Proposal 4.

3.2.5. Proposal 5 – Promoting specific design principles for autonomous vehicles: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of specific design principles such as a logic-based approach rather than a machine learning-based approach serves to guarantee a better reliability of the developed AI systems.

B. How do the measures try to achieve their purpose?

By promoting a logic-based approach and not a machine learning-based approach to the development of autonomous vehicles.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available. However, it may be argued that the entire exclusion of one specific methodology may be an undue restriction. After all, only using a logic-based approach could result in designers having to program the entire driving behavior, which may be unduly difficult and may hamper take-up of the technology concerned.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

The use of a specific approach may be made part of a standard on autonomous vehicles. This may be adopted, although it must be noted that traffic and mobility are also regionalised (thus increasing the transaction costs of policy) and that some initiatives may be best left up to scale, given that self-driving vehicles will probably be deployed across national borders.

3.2.6. Proposal 6 – Clarifying the traffic code for autonomous vehicles: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose identified is to guarantee that the applicable regulations can adequately deal with any challenges.

B. How do the measures try to achieve their purpose?

By adopting a legislative measure.

C. Where possible to assess, to what extent did these measures achieve their purpose?

A clarification was made allowing cars that have delegated driving functions on the road, provided that the driver can always take over control of the vehicle. This allows the cars to be used, but still hampers some of the efficiency gains that can be achieved from autonomous vehicles (while ensuring traffic safety at this point).

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

The abovementioned proposal does not explicitly refer to one of the gaps that are identified, except providing for some regulations on a specific type of autonomous system. It does not solve the regulatory patchwork identified in the D1 report.

3.2.7. Proposal 7 – Developing a platform for the testing, qualification and certification of AI systems: efficiency and budgetary aspects

A. Which purposes were identified/established?

The goal is to facilitate AI systems' diffusion throughout the industry and to increase citizens' trust and acceptance of the AI systems involved.

B. How do the measures try to achieve their purpose?

A project was made to develop a testing and certification platform.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Nothing prevents the Belgian (regional and federal) authorities to take such initiatives themselves.

3.2.8. Proposal 8 – Developing a software platform for AI: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose is to avoid dependence on foreign AI systems and the loss of value. This not only serves economic purposes, but also may serve security purposes. After all, the use of foreign actors means that we may cede control over critical infrastructure to foreign actors who may not have our interests at heart.

B. How do the measures try to achieve their purpose?

By developing a project to develop an ecosystem.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

The same answer can be given as is applicable for Proposal 7.

3.2.9. Proposal 9 – Developing a network of platforms for security and cybersecurity: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose identified is to improve the complementarity of French sites, to accompany the growth of start-ups and of business and to improve SME access to beneficial technologies.

B. How do the measures try to achieve their purpose?

By creating a network of platforms for cybersecurity between territories, for researchers and businesses.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

As mentioned under the D1 report, access to cybersecurity-related information is difficult for SMEs, which often do not have the resources necessary to ensure high-level compliance. For them, any access is welcomed. However, just creating platforms could be insufficient; the added value must be made clear, so that Belgian business want to join these platforms and want to use them. This necessitates awareness building campaigns, which is likely where the added value of the Belgian government truly lies.

3.2.10. Proposal 10 – The creation of a one-stop shop for information relating to AI: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose identified is to support future purchasers of AI solutions with valuable information regarding AI systems, so that they can make informed choices.

B. How do the measures try to achieve their purpose?

By creating an advisory body.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

This is something that the Belgian government can also do to ensure that people have access to information regarding AI. Existing bodies can already be used, insofar as they have the knowledge on them. Examples include business federations such as Agoria.

3.2.11. Proposal 11 – Facilitating dialogue between regulators: efficiency and budgetary aspects

A. Which purposes were identified/established?

The goal is to ensure a coordinated response with regard to the regulatory compliance problems faced by AI designers, deployers and users.

B. How do the measures try to achieve their purpose?

The Villani report proposes such consultations. Available information indicates that some regulators are entering into consultations. Another aspect is that one regulator is given the responsibility to deal with such topics and to take the niche of 'AI expert'. Examples of the latter include the CNIL for the ethical challenges (cf. the Digital Republic Act) and the LNE for certification methods.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

Most information is limited to joint reports. This thus indicates a limited effectiveness.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No information available.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

By coordinating their points of view regarding the proliferation of AI, the many regulators in the patchwork of regulations applicable to AI safety and security ensure can ensure that the patchwork leads less to contradictory solutions. This can reduce compliance burden to a limited extent. It remains to be seen whether this will be enough. Belgium can do this as well, but will have to surmount, amongst other things, the divide between the federal government and the regions to do so.

3.2.12. Proposal 12 – Implementing sector-specific policies around major challenges: efficiency and budgetary aspects

A. *Which purposes were identified/established?*

The identified purposes relate to facilitating the transformation.

B. *How do the measures try to achieve their purpose?*

The Villani Report proposes sector-specific policies with principles around them.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

No information available.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No information available.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

In light of Belgium's limited resources, a sector-specific approach also seems best. Strategic choices must be made in this regard. One can either choose sectors which are ubiquitous (such as self-driving cars) or look at areas of AI in which Belgian businesses have a specific expertise, so that Belgium has its own niche. This can include security applications, such as e.g. anomaly detection or detection of hate speech, the expert of which is [an Antwerp-based company](#).

3.2.13. Proposal 13 – The creation of a Joint Centre for Excellence at state level: efficiency and budgetary aspects

A. *Which purposes were identified/established?*

The purpose is to centralise knowledge within one entity.

B. *How do the measures try to achieve their purpose?*

The Villani report proposes to set up one body, such as the DINUM.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Again, Belgium has the possibility to do this as well, but will have to take the regional divide into account.

3.2.14. Proposal 14 – Appointing a body of experts for the auditing of algorithms: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of this body is to ‘open the black box’ and to limit problems of algorithmic bias. It can also help contribute to the safety of AI systems.

B. How do the measures try to achieve their purpose?

The Villani report proposes to set up a body of experts (p. 117-118). This should be done by a governmental body, but auditing should also be possible for civil society.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information is available regarding the implementation of this proposal. Therefore, no information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

This is also an action that the Belgian government can undertake. It must be noted that, for this purpose, Belgium needs the appropriate experts in this field. Being a small country, the pool of experts may be limited. Also, this body of experts should be able to provide its expertise to all entities that need such knowledge, including, but not limited to the Data Protection Authority.

3.2.15. Proposal 15 – Include ethics and law in education programs: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purposes identified relate to the training of developers, deployers and users of AI systems to include ethics in the design stage of the AI system. These mixed profiles allow engineers to integrate ethics in the design stage and lawyers who can assist the engineers in their engineering process.

B. How do the measures try to achieve their purpose?

So far, the action is limited to a proposal in the Villani report.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Indirectly, this contributes to increasing access to cybersecurity-related information for companies in the long run. Some Belgian initiatives also point in that direction, such as the inclusion of STEM in the curricula for secondary education and modules such as Technology and Law at the KU Leuven. This is a responsibility for the Communities, who are competent for education.

3.2.16. Proposal 16 – Reforming the Civil Code to allow for hardship: efficiency and budgetary aspects

A. Which purposes were identified/established?

No explicit purpose was established with regard to AI. However, the policies can allow for some changes in liability when dealing with AI systems' functioning.

B. How do the measures try to achieve their purpose?

Allowing for hardship allows to alter liability in the event the risks change in an unforeseeable way.

C. Where possible to assess, to what extent did these measures achieve their purpose?

There are not enough cases on how this hardship clause would apply to an AI system. To see how this develops, more case law is required.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Belgium is currently filing the same proposal in its Bill for Book V of the new Belgian Civil Code. It is therefore covered. This can also impact the compliance with security obligations and how standardisation will develop.

3.2.17. Proposal 17 – Issuing guidance documents by regulators on how to apply their regulations and supervisory role to AI: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose is to ensure that regulators provide principles to their users, or to themselves, on how they must deal with AI while complying with their regulatory obligations.

B. How do the measures try to achieve their purpose?

The regulators concerned (including CNIL and ACPR) publish documents that provide guidance on how to comply with their regulations, or how to cope with Artificial Intelligence more generally.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The reports add to the knowledge that is available to the entities addressed. However, there is no information available regarding the take-up. Therefore, there is no information available on the effectiveness.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

The Belgian regulators can do the same to lighten the regulatory burden. Therefore, they are applicable to the Belgian context. They can also assist in creating convergence of the several regimes if done right (i.e., in coordination with each other rather than each speaking from their own silo).

3.2.18. Proposal 18 – Funding research and initiatives in cybersecurity and the creation of a Cyber Campus: efficiency and budgetary aspects

A. Which purposes were identified/established?

The general purpose is to achieve a higher degree of cybersecurity throughout French society by increasing investments in cybersecurity research, development and deployment.

B. How do the measures try to achieve their purpose?

The French relaunch strategy is currently funding several initiatives. One relates to the development of sovereign solutions for cybersecurity; 515 million EUR are earmarked, of which 290 million EUR are public investments. To increase links and synergies between the actors in the value chain through the Cyber Campus, 148 million EUR are earmarked, have of which consists of public funding. For the adoption of cyber solutions, 176 million EUR is earmarked, of which 156 million EUR are publicly funded.

C. Where possible to assess, to what extent did these measures achieve their purpose?

These measures are still to be implemented. Therefore, their effectiveness is currently unknown.

D. Where possible to assess, what impact did the measures have on the government budget?

See the estimates under B.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Belgium will likely have less resources as a country to fund these initiatives. Nonetheless, these can increase the capacity for cybersecurity and therefore ramp up knowledge, R&D and regulatory compliance.

3.2.19. Proposal 19 – Create a control cell for digital technologies: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of such a control cell is to centralise the control of digital technologies and thus to pool expertise to ensure a higher level of convergence and enforcement.

B. How do the measures try to achieve their purpose?

The report mentioned above made a proposal, which has not yet been followed up on.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information is available on the practical implementation.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available on the practical implementation.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Convergence is a topic that can be dealt with through creating one specialised agency that can assist the other agencies. However, in order to achieve this, inter-institutional dialogue must run

smoothly. It is unclear if that is the case for the Belgian federal entities. The fact that AI policy is divided between regional entities and federal entities makes this even more difficult.

Questionnaire the United Kingdom

1. Which authorities are competent for safety and cybersecurity?

- General
 - o The United Kingdom Government has founded a national institute for data science and artificial intelligence, the [Alan Turing Institute](#), with its headquarters at the British Library. They undertake research for data science and artificial intelligence.
 - o United Kingdom [Office for Artificial Intelligence](#), which is a part of the Department for Digital, Culture, Media & Sport and the Department for Business, Energy and Industrial Strategy.
 - o The United Kingdom has also founded a [Centre for Data Ethics and Innovation](#), which analyses and anticipates the opportunities and risks posed by data-driven technology and puts forward recommendations to address them.
- Contract Law
 - o Note that the UK is a common law country. Rules of contract law are partially based on common (judge-made) law and partially based on statutes and/or regulations, the latter of which are passed by the national legislator and government.
- Tort Law
 - o Note that the UK is a common law country. Rules of tort law are partially based on common (judge-made) law and partially based on statutes and/or regulations, the latter of which are passed by the national legislator and government.
- Product Safety
 - o [Office for Product Safety and Standards](#) (OPSS)
- Standardisation
 - o [Office for Product Safety and Standards](#) (OPSS)
 - o The British Standards Institution ([BSI](#)) is the national standards body of the United Kingdom.
- Data Protection
 - o The [Information Commissioner's Office](#) (ICO)
- Cybersecurity (non-sectoral)
 - o The [National Cyber Security Centre](#) is not a true regulator, but does provide technical and support through a Single Point of Contact, a Computer Security Incident Response Team and by being a technical authority on cybersecurity.
- Cybersecurity (sectoral)
 - o Electronic Communications
 - [Ofcom](#) is the independent electronic communications regulator in the United Kingdom.
 - o Finance
 - [Financial Conduct Authority](#) (FCA)
 - [Bank of England](#)

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

- General

- The UK's AI Council has published an [AI Roadmap](#). The document contains 16 recommendations to help the Government develop a UK National AI Strategy. These recommendations include cementing the Alan Turing Institute as a national institute (and to invest in R&D), to make diversity and inclusion a priority, to commit to achieving AI and data literacy for all, as well as to use AI to keep the country safe and secure. One priority is to ensure that good governance of AI systems is ensured (p. 13-15). Three tenets of such 'good governance' include clear transparency about algorithmic decision making, the right to give meaningful public input and the ability to enforce sanctions.
- In 2017, the UK Government unveiled its Industrial Strategy, [Building a Britain fit for the future](#). In it, the UK commits to set Grand Challenges to put the UK at the forefront of the industries of the future, AI being one of them. The approach is based around five foundations of productivity: Ideas, People, Infrastructure, Business Environment and Places. Measures include concluding the AI Sector Deal, the AI Office and the AI Council. The AI Office will work initially with six priority business sectors, including cybersecurity (p. 40). The ambition is to lead the world in safe and ethical use of data and artificial intelligence. 9 million GBP will be invested into a new Centre for Data Ethics and Innovation.
- In a report called [Growing the Artificial Intelligence Industry in the UK](#) by Prof. Dame Wendy Hall and Jérôme Presenti, the two authors include sixteen recommendations to increase the uptake of AI. Recommendations include the development of the AI Council (Rec. 13) as well as that the ICO and the Alan Turing Institute develop a framework for explaining processes, services and decisions delivered by AI, to further improve transparency and accountability.
- In 2018, the UK Government published its [AI Sector Deal](#), as part of its Industrial Strategy. The Sector Deal sets out actions to promote the adoption and use of AI in the UK. Amongst others, this deal leads to a new AI Council, an Office for AI and a Centre for Data Ethics and Innovation, all of which have been established (see above). One challenge which was identified is to lead the world in the safe and ethical use of data through a new Centre for Data Ethics and Innovation, and to strengthen the UK's cybersecurity capability. Key commitments include investments in R&D, as well as measures to ensure the take-up of AI. It also relates to the Alan Turing Institute and the ICO to work together to develop guidance to assist in explaining AI decisions. Standardisation is identified as an industry action.
- In February 2020, the Committee on Standards in Public Life has published the document [Artificial Intelligence and Public Standards: A Review by the Committee on Standards in Public Life](#). The report outlines how current principle for government action and procurement relate to AI. One of the main findings is that existing principles are largely sufficient. The report nonetheless comes with a series of recommendations. To national bodies and regulators, the report recommends the articulate a clear legal basis for AI, to develop guidance against algorithmic bias, as well as to set up a regulatory assurance body for AI systems. Governments should also use procurement rules and processes to ensure AI compliance with standards. The Government should also consider how an AI impact assessment requirement could be integrated into existing processes to evaluate the potential effects of AI on public standards; finally, governments should establish guidelines on the explanation of AI systems. To front-line providers, both public and private, the report recommends them to evaluate risks, to consciously tackle bias and

discrimination, to ensure clear allocation of responsibility, to monitor and evaluate their AI systems to ensure they operate as intended and to set oversight mechanisms. The document also provides guidance on how existing laws apply to AI systems. The report also contains several recommendations for the regulation of AI systems (p. 39 *et seq.*)

- The Centre for Data Ethics and Innovation is already active in providing guidance on topics that relate to AI and safety in general. Examples include:
 - A [blog](#) on the types of assurance in AI and the role of standards.
 - A [review](#) on online targeting, in which research is done on how targeting approaches can undermine or reinforce the concept of autonomy.
 - A [review](#) on bias in algorithmic decision making.
 - The [AI Barometer](#). The AI Barometer is an analysis of the most pressing opportunities, risks and governance challenges associated with AI and data use, initially across five key UK sectors (including Criminal Justice, Financial Services, Health & Social Care, Digital & Social Media and Energy & Utilities). The AI Barometer found that some of the challenges are easier to achieve than others. It also identifies the top common risks for these sectors.
 - The CDEI has also published a series of snapshot paper. Examples include a [snapshot paper](#) on deepfakes, as well as a snapshot paper on [facial recognition technology](#).
- The Central Digital Office has published guidance in the form of the [Data Ethics Framework](#) to allow public servants to understand ethical considerations and to address these within their projects.
- The Central Digital & Data Office and the Office for Artificial Intelligence have published an [Ethics, Transparency and Accountability Framework for Automated Decision-Making](#). The framework provides seven steps when implementing automated decision-making in a service. These include 1. Testing to avoid any unintended outcomes or consequences, 2. Delivery of fair services for all of our users and citizens, 3. Clarity on who is responsible, 4. Handling data safely and protecting citizens' interests, 5. Help users and citizens to understand how it impacts them, 6. Ensure compliance with the law and 7. Build something that is future-proof.
- [Scotland's AI strategy](#) includes some areas related to AI safety, such as the creation of a Scottish AI Playbook, as well as to accelerate the use of common digital and data standards across the public sector.
- The UK Government has also published its [Guidelines for AI Procurement](#), which provide a summary of standards and steps to be taken to ensure that AI systems are used by public services in a safe way. These steps include: 1. Include your procurement within a strategy for AI adoption 2. Make decisions in a diverse multidisciplinary team, 3. Conduct a data assessment first, 4. Assess the benefits and risks of AI deployment, 5. Engage effectively with the market from the outset, 6. Establish the right route to market and focus on the challenge rather than a specific solution, 7. Develop a plan for governance and information assurance, 8. Avoid Black Box Algorithms and vendor lock in, 9. Focus on the need to address technical and ethical limitations of AI deployment and 10. Assess the benefits and risks of AI deployment. As a means of support, the Office for AI also co-created the WEF's [AI Procurement in a Box](#) tool. Other useful guidance can be found in the form of the [Government Design](#) Principles and the Technology Code of Practice.

- The [Technology Code of Practice](#) provides a set of criteria to help guide government design, build and purchasing of technology. It requires, amongst others, that things must be secure, privacy is integral, and that open standards should be used where possible.
- Tort liability
 - The UK has adopted its [Automated and Electric Vehicles Act 2018](#), providing several rules on the management of risks caused by automated vehicles. For automated vehicles, the rules relate mainly to the liability for the management of the vehicle. The insurer is liable whenever an accident is caused by an automated vehicle when driving itself on a road, if it is insured; if not, the owner of the vehicle is liable for that damages.
- Product Safety
 - The OPSS is currently conducting research on the product safety risks of IoT devices and AI systems. AI thus formed a part of the UK Product Safety Review's [Call for Evidence](#) issued on March 2021.
 - The Alan Turing Institute published the [document](#) 'Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems'. The guide comprehensively provides several principles to aid in the design, deployment and use of AI systems to ensure that the AI system is sufficiently reliable, interpretable, etc. The report outlines an Ethical Platform to help any development team continuously reflect, act and justify their development choices. Reflections are done using the SUM Values (Respect, Connect, Care and Protect). Actions are guided by the FAST Track Principles (Fairness, Accountability, Sustainability, Transparency). These principles are analysed in-depth and practical tips are given on how to technically implement them. Such tools include a Stakeholder Impact Assessment (p. 26 *et seq.*). The Sustainability principle also relates to the security and safety of the AI system. Justification is done through a Process-Based Governance Framework.
 - The UK Statistics Authority has published [a tool](#) to allow research to review the ethics of their own projects.
- Standardisation
 - The BSI has published a [white paper](#), giving an overview of the standardisation landscape in artificial intelligence. The documents provide an overview of the existing standardisation framework at the time of publication.
- Data Protection
 - In September 2017, the ICO published [a report](#) on Big Data, artificial intelligence, machine learning and data protection. In it, the ICO gives an overview of the data protection implications of AI and machine learning projects. It provides guidance on which characteristics are specific to AI. All aspects of data protection are covered, including the obligations to ensure data minimisation, purpose limitation, accuracy, the rights of individuals, security, as well as accountability and governance, etc.
 - The ICO has published [guidance on AI and data protection](#). The guidance serves to explain how data protection laws relate to AI. The guidance includes how to conduct a DPIA, as well as what the security and data minimisation risks are. This includes explanations of current adversarial attacks and the explanation of AI.
 - The ICO is has published a blog series outlining an [AI Auditing Framework](#). The framework serves to support the work of investigation and assurance teams when assessing the compliance of data controllers using AI and to help guide

organisations on the management of data protection risks. Several components have already been published online; contributions include view on known security risks, AI explanations, human bias and discrimination, the right to human intervention, privacy attacks on AI, DPIAs and AI, etc. Draft guidance on the AI Auditing Framework can be found in this [report](#).

- Cybersecurity (non-sectoral)
 - o When the UK was still a Member State, it implemented the NIS Directive and the Critical Infrastructures Directive. The national implementation of the NIS Directive can be found in the [Network and Information Systems Regulations 2018](#). The NIS Regulations were [reviewed](#) in 2020. Following this review, the government is now considering amendments to the NIS Regulations.
 - o The UK's national [Cyber Security Strategy 2016-2021](#) indicates that the UK will spend 1.9 billion GBP in defending its systems and infrastructure, deterring the UK's adversaries and developing a whole-society capability, from the biggest companies to the individual citizen. The goals of the Strategy is to defend the UK, to deter any attacks and to develop their cyber security industry. Measures to achieve goals include the following: the Government will explore options for the development of 'secure-by-design' hard- and software, it will adopt cybersecurity technologies in their government (p. 36). A portion of the 165m GBP Defence and Cyber Innovation Fund will also be used to support innovative procurement in defense and security. Also, agreed international standards will be promoted that support access to the UK market (p. 56).
 - o The NCSC has published [guidance](#) on the use of intelligent security tools for cyber security.
- Cybersecurity (sectoral)
 - o Electronic Communications
 - Ofcom requested Cambridge Consultants to conduct research into the ways AI affects content moderation. The [report](#) provides a history of AI as well as some insights as to the impact of AI on content moderation. Human bias, lack of explainability and the need for adaptiveness in the light of evolving content are identified as issues that AI systems are affected by. Benefits are also analysed.
 - o Finance
 - The United Kingdom has implemented both the MiFiD II Directive and the PSD 2 Directive. The implementation of the former can be found in the [Financial Services and Markets Act 2000 Regulations 2017](#), as well as the [Financial Services and Markets Act 2000 Order 2017](#). The implementation of the latter is found in the form of the [Payment Services Regulations 2017](#).
 - The 2019 report [Machine learning in UK financial services](#) by the Bank of England briefly touches upon some aspects of security. First, it describes firms' risk perceptions regarding the use of machine learning. Second, it must be noted that UK financial firms are found to benefit from the deployment of machine learning, e.g. in order to combat anti-money laundering and countering the financing of terrorism. It also proposes safeguards to mitigate the risks associated with using AI for this purpose by inserting a human in the loop.
 - The [minutes](#) of the [meetings](#) of the Artificial Intelligence Public-Private Forum set up by the Bank of England contain some work on the security and safety of AI systems. Aspects that were discussed were, amongst

others, data quality, data strategy and economics, as well as data standards and regulation.

- Other
 - o The Government published an [Online Harms White Paper](#), outlining the harms that can be caused online and proposing a new regulatory framework to deal with these harms. These proposals include creating a new statutory duty of care to make companies take more responsibility for the safety of their users and tackle harm caused by content on their services, compliance of which will be overseen by a new independent regulator. This duty of care shall include having an effective and accessible complaints function. Complaints must always be treated fairly. However, general monitoring will not be compelled. All in all, the Online Harms White Paper contains proposals not too dissimilar to the current Digital Services Act Proposal. The Government followed up on this initiative with a report on transparency reporting in relation to online harms. The Online Harms White Paper was followed up on by the [Online Safety Bill](#) that was published on 12 May 2021.
 - o The ICO has published extensive [guidance](#) on how to explain AI systems aimed at DPOs and compliance teams.
 - o The Alan Turing Institute and the ICO are currently both working on the project [ExplAIn](#). Implementing the AI Sector Deal, this project serves to develop guidance to companies to achieve sufficient explainability of AI, required to allow the auditing of AI systems and thus an increased safety of AI systems. The project is currently ongoing. The [interim report](#) concluded that three key themes emerged from this research: 1. Context is key: the importance, purpose and expectations regarding explainability depend on several factors such as the impact of the decision, the ability to change it and the data used to inform it, 2. While unclear where the responsibility lies, there is a desire for a range of education and awareness raising activities to better engage and inform the public on the use, benefits and risks of AI in decision-making and 3. There are several challenges in explaining AI decisions, including cost, commercial sensitivities and a lack of internal organisation accountability.

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

Most proposals in the United Kingdom are centralised not towards developing new requirements or to developing new rules. They serve mainly to provide guidance on how to understand AI and how to adequately manage AI through soft-law instruments.

Notable instruments that relate to these gaps include the set-up of the Alan Turing Institute (a research institution), a separate Office for AI and the AI Council, as well as the Centre for Data Ethics and Innovation.

Other highly notable instruments relate to the Online Harms Bill, the Automated and Self-Driving Vehicles Act, as well as the report by the Alan Turing Institute in which it proposed its own principles and self-assessment. The procurement tools are also a notable inclusion. Co-regulatory initiatives such as the AI Sector Deal also deserve mention.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

The Automated and Electric Vehicles Act is a prototype of liability rules for AI systems, more specifically self-driving cars.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Setting up advisory bodies such as the AI Council, the CDEI and the Alan Turing Institute: efficiency and budgetary aspects

A. Which purposes were identified/established?

Purposes identified were to lead the world in the ethical use of data, as well as to advise regulators and companies on how to manage AI.

B. How do the measures try to achieve their purpose?

The abovementioned institutions gather knowledge and disseminate knowledge. They can provide input for policy makers regarding AI for Britain. These institutions are already up and running and have already issued several policy documents, which all form soft law instruments that help prepare for harder AI policy.

C. Where possible to assess, to what extent did these measures achieve their purpose?

One can refer to the reports and documents they have already published above. The real impact of these documents is yet to be felt and is very hard to quantify.

D. Where possible to assess, what impact did the measures have on the government budget?

From the follow-up on the AI Sector Deal, it can be derived that 9 million GBP was already spent on the Centre for Data Ethics and Innovation alone. However, this type of cooperation can be funded in many ways and at many levels that Belgium sees fit.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

By creating separate institutions, they can gather the necessary knowledge to fill in the gaps that were identified in the D1 report. The Alan Turing Institute's report on understanding the safety of AI successfully gives an understanding of both the safety and the security impact of AI systems. This can inform the legislator as to the actions that should be taken.

It must be noted that these initiatives are already present in Belgium in a very limited form. The Flemish Action Plan AI already includes a track on research and a Knowledge Centre on Data and Society. AI4Belgium can also provide this knowledge if required. They may be constrained by the limited resources that come with being a smaller country. However, we need to take into account the legislative initiatives that are already taking place at the EU level, where much of the study work, guidance work, etc. is already underway. The UK has the benefit of coherence and thus agility; I believe it should be the focus of the Belgian government to translate the EU's policy with the same assets.

3.2.2. Proposal 2 – Setting up a separate Office for AI: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of this initiative was to oversee implementation of the AI Strategy.

B. How do the measures try to achieve their purpose?

By creating a new independent regulator.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The UK AI Office is providing guidance. However, the exact impact is hard to assess.

D. Where possible to assess, what impact did the measures have on the government budget?

Not possible to assess.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

It must be noted that EU does not have a specific regulator for AI. This is because the risks of AI systems pervade everything; therefore, we recommend using the existing infrastructure. Any AI-specific body can best function as a centre of expertise.

3.2.3. Proposal 3 – Guidance by independent regulators: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of guidance given by e.g. the ICO and the Bank of England is to increase understanding of how to comply with regulatory obligations when managing AI.

B. How do the measures try to achieve their purpose?

Guidance is given in many separate ways, one more accessible than the other. These include reports, but also snapshot papers and easy-to-access blogs.

C. Where possible to assess, to what extent did these measures achieve their purpose?

It is hard to assess the actual impact of such unquantifiable measures. No data are available regarding the take-up of this guidance. However, compared to the guidance coming from regulators in the other analysed countries, the guidance provided by e.g. the ICO and the Alan Turing Institute (which, granted, is not a regulator) excels in terms of comprehensiveness, practicality and simplicity. Moreover, these guidance's do not forget the technical aspects. Therefore, where possible, regulators may take inspiration from the UK regulators' communication style in order to increase policy understanding, also regarding the safety and security of AI systems.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Nothing prevents Belgian regulators from providing guidance of this sort. Constraints may include limited resources and lack of coordination between regulators. If those issues occur, it should be made a priority to sort these out.

3.2.4. Proposal 4 – Guidelines on AI procurement: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of the Guidelines for Procurement was to ensure that public bodies could use AI ethically and safely.

B. How do the measures try to achieve their purpose?

The Government issues guidance to bodies on which questions to ask themselves when procuring AI systems.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Nothing prevents the Belgian government from doing the same for its procurement processes.

3.2.5. Proposal 5 – Self-assessment tools: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose was to offer researchers and easy-to-use framework to review the ethics of their own projects.

B. How do the measures try to achieve their purpose?

By providing information and guidance.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Nothing prevents Belgium from taking the same measures through its own authorities, provided it has the resources to do so.

3.2.6. Proposal 6 – Draft Online Safety Bill: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of the Online Safety Bill is to ensure that the risk of illegal content is better managed on the Internet.

B. How do the measures try to achieve their purpose?

Measures include creating new duties of care for social media providers and by giving new powers to Ofcom to enforce these.

C. Where possible to assess, to what extent did these measures achieve their purpose?

It is not possible to assess this, as the measures have not been adopted yet.

D. Where possible to assess, what impact did the measures have on the government budget?

It is not possible to assess this, as the measures have not been adopted yet.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

This is another area in which the safety of software is dealt with, rather than the safety of hardware. Initiatives are already underway at the EU level, i.e. the Digital Services Act. Belgium should contribute to the discussion at that level first.

3.2.7. Proposal 7 – An Automated and Electric Vehicles Act: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose is to ensure that the UK's infrastructure and insurance system is ready for the largest transport revolution in a century.

B. How do the measures try to achieve their purpose?

The chosen action is to impose liability rules and thus have the cheapest cost avoider take due care to ensure the safety of the use of the automated vehicle.

C. How do the measures try to achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

The focus should first and foremost be on the apt application of existing legal principles on liability by Belgian courts. Where possible, however, the Belgian government can propose similar legislative initiatives to achieve safety through private ordering.

Questionnaire Germany

1. Which authorities are competent for safety and cybersecurity

- General
 - o The national legislator and government, as well as the legislator and government of the *Länder*
 - o Germany has established a [Data Ethics Commission](#) under the auspices of the Ministry of Justice
- Contract law and consumer protection
 - o The national legislators and governments
- Tort law
 - o The national legislator and the national government
- Product Safety
 - o The national legislator and government for the Product Safety Law and the implementing decisions. The implementation is done by the *Länder's* governments.
- Standardisation
 - o In general: [Deutsche Institut für Normung e.V. \(DIN\)](#)
 - o For electrotechnical standards: the Deutschen Kommission Elektrotechnik ([DKE](#))
- Data Protection
 - o Data protection is primarily a competence of the *Länder*, which each have their own data protection law and data protection authority. There is also a [Federal Commissioner for Data Protection and Freedom of Information](#), which is

responsible for the implementation of the [Federal Data Protection Act](#). The data protection authorities of the *Länder* consist of:

- The State Commissioner for Data Protection and Freedom of Information of [Baden-Württemberg](#)
 - The [Bavarian](#) State Office for Data Protection Supervision
 - The [Berlin](#) Commissioner for Data Protection and Freedom of Information
 - The [Brandenburg](#) State Commissioner for Data Protection and the Right to Inspect Files
 - The [Bremen](#) State Commissioner for Data Protection
 - The [Hamburg](#) Commissioner for Data Protection and Freedom of Information
 - The [Hessian](#) Commissioner for Data Protection and Freedom of Information
 - The State Commissioner for Data Protection and Freedom of Information of [Mecklenburg-Western Pomerania](#)
 - The State Commissioner for Data Protection of [Lower Saxony](#)
 - The State Commissioner for Data Protection and Freedom of Information of [Rhineland-Palatinate](#)
 - The Independent Data Protection Centre [Saarland](#)
 - The [Saxony-Anhalt](#) State Commissioner for Data Protection
 - The Independent Centre for Data Protection [Schleswig-Holstein](#)
 - The [Thuringian](#) Commissioner for Data Protection and Freedom of Information
- Cybersecurity (non-sectoral)
 - The [Federal Office for Information Security](#)
 - Cybersecurity (sectoral)
 - Electronic Communications
 - The Federal Network Authority ([Bundesnetzagentur](#))
 - Finance
 - The *Bundesanstalt für Finanzdienstleistungsaufsicht* ([BaFin](#))
 - The [Deutsche Bundesbank](#)

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

- General
 - The [2018 Artificial Intelligence Strategy of the German Federal Government](#) listed several proposals that are relevant to AI safety and security. These include establishing a German observatory for artificial intelligence, as well as to invite data protection authorities and business associations for a round table and to invite them to develop joint guidelines for developing and using AI systems in a way that complies with data protection law. Increasing IT security and responsible AI (and thus safe AI) are identified as explicit priorities (p. 8-9). Germany wishes to promote hardware-software co-design, thus resulting in a systems approach (p. 15). To ensure explainability, the German government will support research and adapt the regulatory framework where necessary (p. 16). Research will also be promoted into civil security and the detection of manipulated and automatically generated content (p. 17). Regarding the adaptation of the legal framework (p. 37 *et seq.*), the German government advocates an ethics by design approach throughout all developmental stages. One proposal is to examine the

possibility to establish and/or expand government authorities or private initiatives for the auditing of algorithms. (p. 38). Another focus is also standardisation (p. 39-40).

- The [2020 update to the Artificial Intelligence Strategy](#) indicates that the investments in AI are increased from 3 to 5 billion EUR, used for research and development initiatives. Another proposal relevant to safety is to begin developing data quality assurance mechanisms, for instance through benchmark tests, reference data, establishing and curating training data pools and setting up test data sets. The next point of attention is also identified to be regulation in work settings. For the security, robustness and resilience of AI systems, the focus lies mostly on championing initiatives at the EU level.
- Amongst other recommendations, the [German Data Strategy](#) lists several priorities regarding the strengthening of data and information security. These include the taking of measures to improve IT- and cybersecurity in the Information Security Law 2.0, to evaluate the cybersecurity strategy, as well as to support IT security research by a successor to the current framework program. Moreover, the German government will coordinate an interdepartmental steering committee in dealing with the global standardisation bodies that develop standards for data processing and IT security.
- The [Digital Strategy 2025](#) outlines several priorities of the German federal ministry for economic affairs regarding digitisation and provides 10 “steps towards the future”. One such step is to strengthen data security and develop information autonomy. To this end, several measures have been planned, including exploring additional regulations such as product liability rules for IT flaws and security requirements for hardware and software. Companies which are not subject to statutory requirements must also improve their cybersecurity; assistance will be provided to this end. A study will also be conducted to identify the key digital capacities (p. 33-35). In order to improve Industry 4.0, an Action Plan for Standardisation will also be developed (p. 43). Finally, one plan that is floated is to create a specific regulatory agency for digital affairs, a Digital Agency (p. 55-57).
- the German federal Ministry of the Interior has set up a [Data Ethics Commission](#), a governmental body that provides recommendations for action and suggestions for possible legislation on data and AI systems. The Data Ethics Commission has been asked to provide its opinion on the legal limits to the use of algorithmic decision-making systems and the commercial use of data. The Data Ethics Commission published its [opinion](#) (executive summary [here](#)) on 22 January 2020. The principles in it relate in large part to data security and the safety of AI systems. For example, it recommends that measures be taken against indefensible uses of data and that privacy-friendly design. Regarding algorithmic systems, the Data Ethics Commission recommends a risk-adapted regulatory approach, the components of which are already listed. First, it proposes that the risk potential should be judged on a universally applicable criteria-based risk model. The regulatory instruments should include corrective and oversight mechanisms. A risk scale is also proposed. As regards regulatory instruments, the Data Ethics Commission recommends that a mandatory labelling scheme is created for critical AI systems and that operators should provide a minimum level of quality. The Data Ethics Commission also recommends that a national centre of competence is set up for algorithmic systems.
- Some states have already set up their own groups of experts. Examples include [Hamburg](#) and [Hessen](#).

- The German federal parliament published a highly expansive [study](#) on recommendations regarding artificial intelligence. Areas include AI and discrimination, AI and risk management, AI and mobility (thus relating to self-driving cars) and AI and information security. Several working groups have worked on these topics, each providing their recommendations. For discrimination, the focus must lie on education, research and transparency (p. 60). For AI and risk management, the focus must be on implementation of the European agenda, sector-specific regimes, practical guidance, a risk-based approach and primary supervision by the sectoral authorities (p. 64). Regarding AI and liability, the focus should be on maintaining the current liability regime (p. 75). Regarding security, recommendations include research on AI recommendations, to require social innovations, to identify use cases for AI, as well as establish standard processes for the deployment of AI, to increase transparency and risk classification, as well as to monitor AI decisions on their discriminatory nature on a regular basis, etc. (p. 198-199). Social scoring is not considered legitimate (p. 231).
- Product safety
 - On 16 June 2017, the German legislator adopted an [amendment](#) to the Road Traffic Act which allows motor vehicles with a highly or fully automated function (i.e., self-driving vehicles) to enter German traffic. However, the conditions include that the vehicle can be overridden or deactivated by the driver at any time, making fully autonomous driving impossible as of yet.
 - The Data Ethics Commission has also published a [report](#) on their ethical considerations regarding automated driving. The report contains 20 recommendations about how automated vehicles should be built and managed.
 - The Federal Government has also published an [action plan](#) on the report by the Ethics Commission on Automated and Connected Driving. In it, the Federal Government proposes to build on the amendment of the Road Traffic Act to adapt to technological changes, taking as a starting point the proposals made by the Ethics Commission on the data protection requirements. It is clarified that automated driving must not result in total surveillance and that stringent safety requirements are required. Work on standardisation and the development of an appropriate regulatory framework are additional priorities.
 - In conjunction with TÜV (a major certifier in Germany), the BSI published a [white paper](#) on recommendations on how to obtain auditable, secure and safe AI systems. The paper provides two general strategies to secure AI systems: 1. Create favorable boundary conditions for the given task: proper education of developers and users, sufficient information exchange between both parties, and 2. Invest in R&D to advance available technologies to eventually allow for secure and safe AI systems despite complex boundary conditions and, therefore, to improve scalability and generalisability.
- Standardisation
 - In a joint project with the Federal Ministry of Economic Affairs and Energy, DIN and DKE adopted a [roadmap](#) for standards in the field of AI. The aim was to develop a framework for action regarding standardisation. The document contains five basic recommendations (p. 4-5 and 24-25): 1. Implement data reference models for the interoperability of AI systems, 2. Create a horizontal AI basic security standard, 3. Design practical initial criticality checks of AI systems, 4. Initiate and implement the national implementation programme "Trusted AI" to strengthen the European quality infrastructure and 5. Analyze and evaluate use cases for standardisation needs.

- Data protection
 - On 3 April 2019, the federal and state data protection authorities adopted the [Hanbach Declaration on Artificial Intelligence](#). This Declaration provides for seven data protection requirements that all will comply with when reviewing AI systems: 1. AI must not turn human beings into objects, 2. AI may only be used for constitutionally legitimate purposes and may not abrogate the requirement of purpose limitation, 3. AI must be transparent, comprehensible and explainable, 4. AI must avoid discrimination, 5. The principle of data minimisation applies to AI, 6. AI needs responsibility and 7. AI requires technical and organisational standards.
 - In a [Position Paper on Algorithms](#), the Conference of Information Freedom Offices has issues its requirements for artificial intelligence use by public bodies. Recommendations include the following: i) before using algorithms and AI processes, public bodies must check to what extent this use is in accordance with fundamental rights and freedoms, ii) public bodies must have sufficient transparency about the algorithms used, iii) transparency requirements must be observed during programming, iv) logging as well as essential parameters are essential to make the process more secure, v) public bodies must take the necessary risk-adequate measures, vi) discriminatory effects must always be avoided and vii) if there are high risks, a previous impact assessment must take place.
 - In a [position paper](#), the *Datenschutzkonferenz* (the Conference of Data Protection Authorities of the German states) have outlined guidance on the recommended technical and organisation measures to ensure that AI projects comply with data protection principles.
- Cybersecurity (non-sectoral)
 - Germany had already adopted an IT-Security Law on 24 July 2015. The German [law on critical infrastructures](#) was adopted on 22 April 2016.
 - In March 2019, Germany's interior ministry proposed a new cybersecurity bill called [IT Security Act 2.0](#). The draft was passed on 16 December 2020. The act was adopted on 23 April 2021. The new law amends the laws on information security, the protection of the federal administration, critical infrastructures. The BSI gains the authorisation to exercise control and audit powers regarding the federal administration. The BSI will also be tasked with regulating consumers and the basis for a uniform security IT label will be introduced to make security functions, especially for products for consumers. The BSI will also be authorised to request information from providers of telecommunications services. This includes that the BSI will have the right to detect security gaps at the interfaces of information technology systems to public telecommunications networks and to use systems and processes for the analysis of malware and attack methods. and the BMI will oblige manufacturers to provide information about their products. Moreover, operators of critical infrastructures will be required to use systems with cyberattack detection.
 - The BSI published a report called [Secure, robust and transparent application of AI: Problems, measures and needs for action](#). The report provides some recommendations to increase IT security for AI systems: i) classical measures remain unchanged, ii) the whole lifecycle should be analysed systematically; adversarial training and adaptive attacks should be considered, iii) the metrics used to evaluate the quality of the AI model should take into account the risk potential of the respective application; iv) sufficient quality and quantity of training should be ensured by systematic tests and measures, v) access and

- queries should be logged in a suitable way, vi) the correct functionality of AI systems should be tested in regular intervals using the corresponding metrics, vii) the criticality with respect to the lack of transparency and explainability of the models should be assessed in the context of the respective use case.
- The BSI also published an [AI Cloud Service Compliance Criteria Catalogue](#), in which it provides specific criteria in order to ensure secure AI cloud services. These criteria are related to i) preliminary criteria for general cloud computing, ii) security and robustness, iii) performance and functionality, iv) reliability, v) data management, vi) explainability and vii) bias.
- Cybersecurity (Sectoral)
- Telecommunications
 - Germany amended the [Telemediengesetz](#) (by inserting two new Articles 15a and 15b) and [Article 113 of the Telekommunikationsgesetz](#) by an Act of 30 March 2021. Amongst others, it creates additional reporting obligations regarding the reporting of information on networks' users towards authorities.
 - The Bundesnetzagentur has published a [Background Paper on Artificial Intelligence](#), outlining a general overview of the characteristics of artificial intelligence.
 - Germany adopted the [Netzwerkdurchsetzungsgesetz](#), which requires some social media platforms to report on the handling of complaints and to respond swiftly to complaints regarding illegal content.
 - In a [study](#) of 2017, the Bundesnetzagentur gave an overview of the digitisation taking place in several network sectors and the challenges they face, standardisation and information security being some of them. A [study on AI](#) is currently in the works.
 - Finance
 - Germany implemented the Payment Services Directive through the [Gesetz zur Umsetzung der Zweiten Zahlungsdiensterichtlinie](#). The MiFID II Directive was implemented into German law through the [Zweites Gesetz zur Novellierung von Finanzmarktvorschriften auf Grund europäischer Rechtsakte](#).
 - BaFin has published reports on AI in the financial sector. One study, [Big Data meets Artificial Intelligence](#), provides an overview of the benefits, risks and implications of using Big Data and AI in the financial sector. The report identifies the technical prerequisites for the use of AI in the financial sector (and problems there, including data selection bias, overfitting and complexity) as well as an overview of the main risks to, amongst others, financial stability and information security. Another study, [Supervisory Requirements for IT in Insurance Undertakings](#), identifies supervisory requirements for IT in general for insurance undertakings, also taking into account information security.
 - In a policy discussion paper, [The Use of Artificial Intelligence and Machine Learning in the Financial Sector](#), the Bundesbank provides its recommendations regarding AI systems in the financial sectors. Recommendations include that i) before passing new regulations, supervisors should leverage the existing frameworks first, ii) the use of AI should be assessed on a case-by-case basis without prior approval, iii) the prudential mandate does not include ethical considerations regarding AI, iv) AI is not a regulated activity, v) not all AI labels actually use AI. Regarding the explainability of AI systems, the considerations are clear

that black box systems may be used if the risks remain under control and that explainable AI is a promising answer to the black box characteristic, but not without its downsides. The focus lies mainly on data quality and pre-processing, as well as rigorous validation procedures.

- The BaFin published a [circular](#) in 2017 outlining the minimum requirements regarding IT risk management for credit services and financial institutions.

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

We refer to the documents listed under 2

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

N/A.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Establishing Centres of Excellence on AI and develop Centres of Excellence: efficiency and budgetary aspects

A. Which purposes were identified/established?

The goals identified were to make Germany a leading centre for AI and securing Germany's competitive advantage, as well as to responsibly develop AI in Germany and to integrate AI in society.

B. How do the measures try to achieve their purpose?

By creating a network of institutions that gather knowledge, both in terms of the technical possibilities of AI policy as well as on the societal impact.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Such impact is difficult to quantify.

D. Where possible to assess, what impact did the measures have on the government budget?

We know that the German government has allocated 5 billion EUR in total on their AI strategy.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Such Centres of Excellence already exist to some degree, for example through the Flemish Action Plan AI, the first pillar of which focuses on research into the technical aspects of AI and the third track of which, the Knowledge Centre Data & Society, provides input on the societal aspects.

3.2.2. Proposal 2 – A Standardisation Roadmap: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose identified is to engage in a broad coordination of standardisation initiatives regarding AI at European and ultimately the international level. The goal is to describe at an early state a framework for action that will strengthen German industry and science in the international

competition for the best solutions and products in the field of artificial intelligence, and create innovation-friendly conditions for the technology of the future. Another identified purpose is to identify the need for standards and specifications, especially with regard to the security, reliability and robustness of AI systems, and to thus contribute to ensuring the quality of AI solutions.

B. *How do the measures try to achieve their purpose?*

A guidance document is released that identifies the standards that are already applicable to AI systems and where standardisation is still lacking. Thus, it is possible to direct standardisation efforts more effectively.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

Such impact is difficult to quantify. Given the rather unique position of this document, it is noteworthy that this guide provides an overview of the existing standards, creating a good guidance for standardisation organisations of all countries (not just Germany) to direct their standardisation efforts.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No information available.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

Such an initiative could be undertaken by NBN as well. However, for such a document to have a lasting impact, one must take into account the benefits of scale and available resources. It can reasonably be presumed that DIN and DKE have more resources than NBN would have, thus making it more feasible to draft and disseminate such a document by themselves. If this is not the case, it may be recommended to give priority to international efforts rather than such guidance documents.

3.2.3. Proposal 3 – Establishment of a Data Ethics Commission: efficiency and budgetary aspects

A. *Which purposes were identified/established?*

The mission of the Data Ethics Commission is to provide the national legislators with a framework on how to develop data policy and deal with algorithms. I.e., create a body of experts than can provide input to legislators to ensure better AI legislation.

B. *How do the measures try to achieve their purpose?*

By the creation of an advisory body.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

We can refer to the reports that have been published by the Ethics Commission, including their opinion and their report on the ethics implications on automated driving. These documents do provide guidance; however, their exact impact is not quantifiable.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No clear information available.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

Belgium may use the same to inform its own government on AI policy, provided it considers this necessary. Given the proliferation of initiatives at the EU level currently going on, Belgium (being a small country) may prefer to focus on taking a constructive position in these initiatives.

3.2.4. Proposal 4 – Guidance on the use of artificial intelligence and the supervision of artificial intelligence: efficiency and budgetary aspects

A. Which purposes were identified/established?

The studies conducted by e.g. BaFin, the Bundesbank, the BSI, the IFK, the DSK, etc. all serve to provide guidance to regulators or to put forward a common interpretation of how to deal with AI systems within the specific sector.

B. How do the measures try to achieve their purpose?

By providing studies within the field with recommendations, or specific declarations. In general, this is through the use of soft law instruments.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The impact of such initiatives is hard to quantify.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Such policy documents are present at the Belgian level and may be used to provide useful guidance to Belgian business, governments and citizens on how to manage AI.

3.2.5. Proposal 5 – Establishing a risk-based classification system for AI systems: efficiency and budgetary aspects

A. Which purposes were identified/established?

An identified purpose is to ensure the safety of AI systems.

B. How do the measures try to achieve their purpose?

Throughout e.g. the Artificial Intelligence strategy and the report on the Data Ethics Commission, several strategy documents propose a risk-based classification model. Some documents steer towards a sectoral approach, although the German AI Strategy also aims to create horizontal AI standard.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not possible.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

The proposed solutions steer towards the increased convergence between product safety and digital security laws, which is necessary to adapt both to digitisation and the proliferation of AI systems. That being said, the AI Act Proposal has now been published and is currently undergoing review. Therefore, any work that Belgium were to publish in this regard could be the redoubling of work. This means that Belgium likely should use its available knowledge resources to contribute to the development of the AI Act and to ensure its rapid adoption.

3.2.6. Proposal 6 – Sector-specific recommendations (e.g. automated driving): efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose of e.g. the Data Ethics Commission's report on the ethical considerations of automated driving is to increase the safety of automated driving in Germany.

B. How do the measures try to achieve their purpose?

By providing guidance on how to implement automated driving.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Such reports are possible. However, given their limited role, they can only serve as preparation for further policy on automotive security.

3.2.7. Proposal 7 – Adapting the NIS Act in the same way as the IT-Security Act 2.0: efficiency and budgetary aspects

A. Which purposes were identified/established?

The IT Security Act 2.0 had as its purpose to update cybersecurity protection to tomorrow's attacks.

B. How do the measures try to achieve their purpose?

By updating the NIS Act in such a way as to strengthen local institutions, to create a mandatory IT-security label, to require inventory data from telecommunications services in order to inform those affected about security gaps and attacks, as well as to strengthen the IT security administration to give orders regarding cybersecurity.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The Act was adopted too soon to make a proper assessment.

D. Where possible to assess, what impact did the measures have on the government budget?

See above under C.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Belgian cybersecurity laws may be lacking. When planning such a reform, however, it must be noted that initiatives at the European level, including the NIS 2 Directive and the implementation of the EU Cybersecurity Act are already underway. Belgium is not a large country and is therefore ill-placed to engage in initiatives with a cavalier attitude. Therefore, it appears more efficient for Belgium to engage in the initiatives for the European rules first and to diligently implement these rules once they have been adopted. Many of the rules in the IT-Security Act 2.0 can already be found there.

3.2.8. Proposal 8 – Adopting laws such as the *Netzwerkdurchsetzungsgesetz*: efficiency and budgetary aspects

A. Which purposes were identified/established?

The intended purpose of the *Netzwerkdurchsetzungsgesetz* was to increase the fight against illegal content and hate speech on the internet.

B. How do the measures try to achieve their purpose?

By enhancing regulatory obligations of online social media providers to respond to notices, on pain of fines.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

It must be noted that the Digital Services Act Proposal was published in December 2020. Any intended results in this field are therefore best achieved through negotiation and implementation of the DSA in order to avoid contradictory rules later on.

WP 4.2. DATA ECONOMY

Questionnaire the Netherlands

1. Which authorities are competent for data economy?

There is no specific authority competent for data economy in the Netherlands. However, the Netherlands data protection authority ([Autoriteit Persoonsgegevens](#)) is competent to some extent, where the processing of personal data takes place.

2. Have the authorities under 1. published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Several documents were issued in the Netherlands, regarding AI. A few relate to data economy:

- Netherlands Government, 2019, [Dutch Digitalisation Strategy 2.0](#)
- Netherlands Government, 2019, [Dutch Digitalisation Strategy – Dutch vision on data sharing between businesses](#)
- Netherlands Government, 2019, [Data Agenda Government](#)
- Netherlands Government, 2019, [Action plan on AI \(SAPAI\)](#)

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

There is no concrete proposal relevant for the gaps identified in task I, regarding data economy, in the Netherlands.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

Several proposals are worth listing:

- Netherlands Government, 2019, [Dutch Digitalisation Strategy – Dutch vision on data sharing between businesses](#):
 - o To facilitate B2B voluntary data sharing by offering financial and organisational support, under certain conditions, where there is a clear economic or public interest (p. 7 and 17-18).²⁹
 - o To impose sector specific compulsory B2B data sharing obligations, in specific cases, where market forces are not sufficient to ensure data sharing (p. 7 and 21).
 - o To regulate control of data technically and organisationally (e.g. through sets of agreements), to empower individuals and businesses (p. 8 and 21-23).
 - o To develop certification tools to be used to determine if data-sharing agreements comply with FAIR principles (findable, accessible, interoperable, reusable) (p. 26).³⁰
 - o To create a data-sharing coalition, which is to establish a generic set of data sharing agreements (p. 26).
- Netherlands Government, 2019, [Data Agenda Government](#):
 - o To provide a platform where all open government data can be found (p. 31).³¹
 - o To improve the quality, usability and findability of open government data (i.e. enhance government's data management) (p. 31-34).³²
- Netherlands Government, 2019, [Action plan on AI \(SAPAI\)](#):
 - o To organize sector dialogues on data sharing bottlenecks enhance supply of public data on that basis (p. 36).

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

N/A.

²⁹ See notably the iSHARE scheme (<https://www.ishareworks.org/en/cookies>).

³⁰ This proposal is also contained in: Netherlands Government, Action plan on AI, 2019, p. 35.

³¹ See data.overheid.nl and the Netherlands National Platform for Public Sector Information. This proposal is also contained in: Netherlands Government, Action plan on AI, 2019, p. 35.

³² See also Netherlands' Open Government Act.

Questionnaire France

1. Which authorities are competent for data economy?

There is no specific authority competent for data economy as such in France. However, the French data protection authority ([CNIL](#)) is competent to some extent, where the processing of personal data takes place.

2. Have the authorities under 1. published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Several documents were issued in France, regarding AI. A few relate to data economy:

- French and British joint working group on data economy, 2016, [the data revolution at the service of growth](#).
- French Government, 2017, [National Strategy for Artificial Intelligence – Artificial Intelligence: legal issues – contribution of the working group 3.2.B. to the working group 3.2 – Anticipating the economic and social impacts of artificial intelligence](#).
- French Government, 2017, [France Intelligence Artificielle – Synthesis report](#).
- French Government, 2018, [Mission Villani – For a meaningful Artificial Intelligence](#).
- French Conseil Supérieur de la Propriété Littéraire et Artistique, 2020, [Mission Intelligence Artificielle et Culture](#).

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

Yes, a proposal that responds to one of the identified gaps was issued in France:

- French Government, 2018, [Mission Villani – For a meaningful Artificial Intelligence](#):
 - o Organising access to data held by private entities for public interest purposes (p. 27-28).

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

In addition to the above, several other proposals are worth listing:

- French and British joint working group on data economy, 2016, [the data revolution at the service of growth](#)
 - o To provide reference data infrastructures, in order to enhance data sharing (p. 21).³³
 - o To develop the use of open and common APIs, in the data economy (p. 11).
 - o To invest in the creation of reference data registers (p. 11).
- French Government, 2017, [National Strategy for Artificial Intelligence – Artificial Intelligence: legal issues – contribution of the working group 3.2.B. to the working group 3.2 – Anticipating the economic and social impacts of artificial intelligence](#)

³³ This proposal is also contained in: French Government, France Intelligence Artificielle – Synthesis report, 2017, p. 23, row 6, columns 1-3. This is notably done through the joint project from France and Germany: GAIA-X (see <https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html>).

- To monitor the contractual clauses used by economic operators in data sharing agreements, in order to identify and develop best practices in data sharing schemes (p. 10).³⁴
- French Government, 2017, [France Intelligence Artificielle – Synthesis report](#)
 - To enhance access to public and parapublic data. (p. 29, row 5, columns 1-2).
- French Conseil Supérieur de la Propriété Littéraire et Artistique, 2020, [Mission Intelligence Artificielle et Culture](#)
 - To create a new right of portability for “use data” in the cultural sector, to correct the informational asymmetry between cultural sector players and in order to implement new services made possible by AI (p. 63).
 - To encourage the development of shared metadata bases in the cultural sector (p. 65).

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1- Access to data: efficiency and budgetary aspects

A. Which purposes were identified/established?

To organise (i.e. through legislation) access to private sector data for general interest purposes.

B. How do the measures try to achieve their purpose?

No data available (no legislative proposal was made on this matter following the Villani report).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data available (no legislative proposal was made on this matter following the Villani report).

D. Where possible to assess, what impact did the measures have on the government budget?

No data available (no legislative proposal was made on this matter following the Villani report).

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

As there was no legislative proposal on this matter in France, it is not possible to answer this question. In addition, the recently proposed Data Governance Act might, if adopted, solve the gap pointed at in task I of the study (i.e. lack of a binding legal framework for B2G data sharing).

Questionnaire the United Kingdom

1. Which authorities are competent for data economy?

- The [Centre for Data Ethics and Innovation](#). It is tasked to identify the measures that should be adopted to maximise the benefits of data and Artificial Intelligence (AI) for the United Kingdom.
- In addition, the [Office for Artificial Intelligence](#) oversees the implementation of the AI and Data Grand Challenge (which has a scope limited to prevention, early diagnosis and treatment of chronic diseases).
- Finally, the United Kingdom data protection authority ([ICO](#)) is competent to some extent, where the processing of personal data takes place.

³⁴ This proposal is also contained in: French Government, Mission Villani – For a meaningful Artificial Intelligence, 2018, p. 27.

2. Have the authorities under 1. published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Several documents were issued in the United Kingdom, regarding AI, by various authorities. A few relate to data economy

- UK Government, 2017, [UK Digital Strategy](#)
- UK Government, 2017, [Growing the artificial intelligence industry in the UK](#)
- UK Government, 2017, [Industrial Strategy](#)
- UK Government, 2018, [AI Sector Deal](#)
- UK Government, 2019, [AI Sector Deal – One Year On](#)
- [Centre for Data Ethics, 2019, 2 Year Strategy](#)
- [UK Government, 2020, National Data Strategy](#)
- [AI Council, 2021, AI Roadmap](#)
- UK Government, 2021 (forthcoming), [National AI Strategy](#)

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

There is no concrete proposal relevant for the gaps identified in task I, regarding data economy, in the United Kingdom.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

Several proposals are worth listing:

- UK Government, 2017, [UK Digital Strategy](#)
 - o To work with organisations (such as the Open Data Institute) to create an environment to share data, and allow access to it through APIs, across sectors (point 7 - unlocking the power of data in the UK economy and improving public confidence in its use).
 - o To create registers of core reference data (point 7 - unlocking the power of data in the UK economy and improving public confidence in its use).
 - o To share anonymised data for research purposes (point 7 - unlocking the power of data in the UK economy and improving public confidence in its use)
 - o To ensure that data can be shared within the public sector, through a revision of the Digital Economy Bill (point 7 - unlocking the power of data in the UK economy and improving public confidence in its use).³⁵
- UK Government, 2017, [Growing the artificial intelligence industry in the UK](#)
 - o To develop Data Trusts³⁶ to ensure that data exchanges are secure and mutually beneficial (p. 4 and 46).

³⁵ This proposal is also contained in: [UK Government, National Data Strategy, 2.4. Driving better delivery of policy and public services, 2020.](#)

³⁶ This means "a set of relationships underpinned by a repeatable framework, compliant with parties' obligations, to share data in a fair, safe and equitable way", according to UK Government, Growing the artificial intelligence industry in the UK, 2017, p. 46.

- To ensure that public funding for research explicitly includes publication of underlying data in machine-readable formats with clear rights information, and open where possible (p. 4 and 48-49).
- To ensure that the default rule, for published research, is the right to mine data (text and data mining) (p. 4 and 49).
- UK Government, 2018, [AI Sector Deal](#)
 - To publish more public data in open and reusable format that is suitable for machine learning (point on key commitments).³⁷
 - To establish a Geospatial Commission to improve access to geospatial data for businesses (point on key commitments).
 - To work with major (public and private) data holders to identify barriers to data sharing (point on key commitments).
- [UK Government, 2020, National Data Strategy](#)
 - To establish a cross sector Smart-Data³⁸ working group, in order to coordinate and accelerate existing Smart-Data initiatives in several sectors (e.g. communications, finance, etc.) (point 6.1., data availability for the economy and society).
 - To negotiate with trade partners to remove unnecessary barriers to cross border data flows (such as unjustified data localisation measures) (point 6.3., international data availability).
- [AI Council, 2021, AI Roadmap](#)
 - To create a cross-sectoral Information Management Framework that is AI-friendly and designed for clean, codified, real-time data (p. 20).
 - To provide examples of good data sharing practices to the private sector, notably to develop FAIR principles (findable, accessible, interoperable, reusable) in data sharing, and to foster the use of open licenses in data sharing agreements (p. 21).
 - To set up independent regulators for providing guidance on the application of existing data-rules (p. 22).
 - To set up a coalition of institutions and experts to develop standard data sharing agreements and to provide practical exemplars, especially for business-to-business data sharing (p. 22).

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

N/A.

[Questionnaire Germany](#)

1. Which authorities are competent for data economy?

There is no specific authority competent for data economy as such in Germany. However, the [Data Ethics Commission](#) has been tasked to provide the German Government with recommendations for action and suggestions for possible legislation in the field of data ethics.³⁹ In

³⁷ This proposal is also contained in: [AI Council, AI Roadmap, 2021, p. 20.](#)

³⁸ Smart Data enables consumers and SMEs to simply and securely share data that firms hold about them with authorised third parties, such as the Open Banking Initiative, according to [UK Government, National Data Strategy, 2020, 6.1. Data availability for the economy and society.](#)

³⁹ Its task is “to build on scientific and technical expertise in developing ethical guidelines for the protection of the individual, the preservation of social cohesion, and the safeguarding and promotion of prosperity in the information age”. See: https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html.

addition, the German data protection authority ([BfDI](#)) is competent to some extent, where the processing of personal data takes place.

2. Have the authorities under 1. published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Several documents were issued in Germany, regarding AI. A few relate to data economy

- German Government, 2021, [Data Strategy – Germany: a trailblazer for innovations](#)
- German Government, 2021, [Second Open Data Act proposal](#)
- Federal Commissioner for Data Protection and Freedom of Information, 2019, [Activity Report](#)
- Data Ethics Commission, 2019, [Opinion of the Data Ethics Commission](#)
- German Federal Government, 2018, [Artificial Intelligence Strategy](#)

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

Yes, a proposal that responds to one of the identified gaps was issued in Germany:

- Data Ethics Commission, 2019, [Opinion of the Data Ethics Commission](#):
 - o To create obligations for private entities to grant access to their data for public interest (p. 23 and 157).

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

- Federal Commissioner for Data Protection and Freedom of Information, 2019, [Activity Report](#)
 - o To grant non-discriminatory access to vehicle data and data generated in vehicles (p. 8 and 65-67).
- Data Ethics Commission, 2019, [Opinion of the Data Ethics Commission](#)
 - o To adopt industry specific codes of conduct and standards on the data portability right contained within the GDPR, in order to ensure that other providers can access data more easily (p. 21 and 140).
 - o To provide reference data infrastructures, in order to enhance data sharing (p. 22 and 155).⁴⁰
 - o To set up an ombudsman at the federal level to assist and support parties in the negotiation of access to data, and settle disputes (p. 22 and 155).
 - o To adopt legislation enabling European companies to cooperate in their use of data, for example by using data trust schemes, without running afoul of anti-trust law (p. 22 and 155).⁴¹
 - o To adapt existing legislation, notably by imposing a duty to enter into negotiations about data access between a party that has contributed to the generation of data

⁴⁰ This proposal is also contained in: German Federal Government, Artificial Intelligence Strategy, 2018, p. 32-33. This is notably done through the joint project from France and Germany: GAIA-X (see <https://www.data-infrastructure.eu/GAIA-X/Navigation/EN/Home/home.html>); see also German Government, Data Strategy – Germany: a trailblazer for innovations, 2021, p. 12-13.

⁴¹ This proposal is also contained in: German Federal Government, Artificial Intelligence Strategy, 2018, p. 34.

- in a value creation system and the controller of the data, by imposing default provisions for data contracts, or by creating sector-specific data access rights (p. 22-23 and 156).
- To enhance access to public and parapublic data (p. 23 and 156).⁴²
 - To promote and support voluntary data-sharing arrangements in the private sector (p. 23 and 157).
- German Federal Government, 2018, [Artificial Intelligence Strategy](#)
 - To increase the amount of data available for research and development by businesses and civil society (p. 32).
 - To fund open training data sets (p. 34).
 - To expand research on the exchange and the interoperability of industrial data (p. 36).
 - To fund the development of standards for data formats and interfaces (p. 36).
 - German Government, 2021, [Data Strategy – Germany: a trailblazer for innovations](#)
 - To ensure uniform legal interpretation and application of (personal) data protection rules, by all German supervisory authorities (p. 19-21).
 - To promote anonymisation procedures and methods, and hence to enhance the availability and sharing of (non-personal) data (p. 19-21).
 - To establish funding programs to develop and test innovative data fiduciaries and data sharing models (p. 36).
 - To empower SME's in the areas of data economy, data-utilisation, and data-based business models, Through funding programs (p. 45-46).
 - To expand the provision of metadata, to improve discoverability of public sector data (p. 54-56).

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1- Access to data: efficiency and budgetary aspects

A. Which purposes were identified/established?

To create obligations for private entities to grant access to their data for public interest.

B. How do the measures try to achieve their purpose?

No data available (no legislative proposal was made on this matter following the opinion of the Data Ethics Commission).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data available (no legislative proposal was made on this matter following the opinion of the Data Ethics Commission).

D. Where possible to assess, what impact did the measures have on the government budget?

No data available (no legislative proposal was made on this matter following the opinion of the Data Ethics Commission).

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

⁴² This proposal is now at its legislative stage (see German Government, 2021, Second Open Data Act proposal). See also German Government, , Data Strategy – Germany: a trailblazer for innovations, 2021, p. 12-13, and 54-56.

As there was no legislative proposal on this matter in Germany, it is not possible to answer this question. In addition, the recently proposed Data Governance Act might, if adopted, solve the gap pointed at in task I of the study (i.e. lack of a binding legal framework for B2G data sharing).

WP 4.3. ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR ELECTRONIC TRANSACTIONS (EIDAS REGULATION)

The [eIDAS Regulation](#) oversees electronic identification and trust services for electronic transactions in the European Union. It aims at providing a system building the trust in the use of electronic services. Some Member States took national legislations in order to complement and implement the regime established by the eIDAS Regulation. However, as far as we know, there is no national legal provision or other policy document especially dealing with the use of artificial intelligence in the field of trust services.

WP 4.4. E-COMMERCE

Questionnaire the Netherlands

1. Which authorities are competent for e-commerce?

- The national legislator and the government

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

No

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

N/A.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

N/A.

Questionnaire France

The various documents addressed in this section are not policy regulations aimed directly at AI. However, these laws may either influence the use made of AI or impose obligations that can be fulfilled by using AI. For that reason and as a result of discussions with the SPF, we decided that it was interesting in the light of this study to address these laws.

1. Which authorities are competent for e-commerce

- The national Parliament, the government, the CSA (Conseil supérieur de l'audio-visuel - Superior Audio-visual Council), and the Ministry of economy, industry and numeric.

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

- [Proposition of a Legislation to combat hate content on the Internet](#) (so-called "Avia Law")

It should be noted, however, that this legislation was partially annulled by the French Constitutional Council by its decision n°2020-801DC of 18 June 2020. According to the French constitutional Council, some provisions of the legislation infringed people's fundamental rights and freedoms. Indeed, the law allowed a private operator (the platform itself) to take the decision to remove content without any judiciary intervention. There was therefore a risk of (systematic) violation of people's freedom of expression and right to information. The decision is available [here](#).

The [enacted version](#) has been promulgated on the 24th of June 2020.

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

Initially, the Avia law provided for:

- An obligation for certain online platforms, under penalty of criminal sanctions, to remove or make inaccessible within twenty-four hours illegal content and the obligation of withdrawal within one hour for terrorist and child pornography content.
- The competence for the CSA to monitor the application of the law and sanction platforms not complying with it.

The [enacted text](#) still provides for:

- Proposal 1: obligation related to the use of technical means to tackle illegal content.

It contains an obligation to implement proportionate procedures by, where appropriate, technological means to ensure that the notifications received are processed as quickly as possible, that the notified content is examined appropriately so as to prevent the risk of unjustified withdrawal. They shall implement appropriate means to prevent the rebroadcasting or reupload of content removed.

Undertakings are required to take actions to fight against illegal content online and in a short period of time. When actors are required to react so quickly, eventually using technical means, the use of artificial intelligence systems is an appropriate and effective measure to put in place.

Concerns expressed during the legislative debates leading up to the adoption of the text of the law indicate that it is clear that platforms will use artificial intelligence to comply with the obligations imposed on them by this law. Indeed, many are concerned that algorithms will be left to decide whether a content is illegal or not. This shows that when we talk about technical

measures that platforms can put in place to react promptly to the appearance or following the knowledge of illegal content online, we are talking about algorithms and artificial intelligence.⁴³

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

- The creation of a specialised prosecutor's office.
- The creation of an online hate observatory attached to the CSA. It ensures the monitoring and analysis of the evolution of illegal contents.
- The obligation for notifications to contain mandatory information (surname, first name, e-mail address; corporate form, company name); confirmation of receipt of any notification; information about the decision to remove the content; the course of action available in case of content removal; etc.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Removal unlawful content: efficiency and budgetary aspects

A. Which purposes were identified/established?

The [removal of unlawful content](#) and the prevention of reappearance of the removed content.

B. How do the measures try to achieve their purpose?

By encouraging the platforms to use technical means when it is a necessary tool to remove or prevent the re-upload of removed illegal content.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data.

D. Where possible to assess, what impact did the measures have on the government budget?

No influence on the government budget. Indeed, those are measures to be taken by the firms. The firms will bear the costs of the acquisition and use of those technical tools.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

About the cancelled proposal of imposing the removal of illegal content within 24 hours : there is no obligation for platforms to react within 24h of the knowledge of the illegal content in Belgian law. The draft DSA does not provide for this either.

The DSA provides for an obligation on platforms to provide users with a system by which they can easily report content that they consider illegal (article 14 DSA). It should allow users to notify any

⁴³ "It is often easy to distinguish between lawful and unlawful content, but sometimes this is not the case. Therefore, the administrative authority should not be given too much discretion and content cannot be assessed by algorithms alone" (https://www.assemblee-nationale.fr/dyn/15/rappports/cion_lois/l15b2062_rapport-fond); "it fears that freedom of expression on the Internet will be undermined - a danger that I highlighted on several occasions at first reading - particularly because of the constraints that you are imposing on hosts and that you are going to entrust de facto to algorithms. When it comes to manifestly hateful comments, there is no problem; everyone agrees to ask for their removal. But how will the platform deal with the grey area? Since it is not natural persons who will do this, but algorithms, how will they distinguish between clearly hateful statements and messages that are disturbing but do not exceed the limits of freedom of expression, as defined by the European Court of Human Rights? (...) I think it is difficult and not desirable for freedom of expression in France to ask the algorithm of a private platform to censor a comment, especially in 24 hours. It would be said that algorithms are only an aid, but are not decision-making in themselves, as any decision can only be taken by a human being. This would prevent certain "grey" content from being systematically removed as part of the censorship exercised by the platforms."; "While we must try to keep the human factor in the process as much as possible, the technological approach is therefore indispensable. However, the regulator will have to check - and this is at the heart of our approach - that the means used, including the algorithm, make it possible to guarantee a balance; it must therefore have the technical capacity to do so, I am well aware of that." (https://www.assemblee-nationale.fr/dyn/15/rappports/cion_lois/l15b2583_rapport-fond)

content considered illegal. Although article 14 states that “Hosting service providers shall process the notifications they receive through the mechanisms provided for in paragraph 1, and shall make their decisions regarding the information to which the notification relates in a timely, expeditious and objective manner”, there is no obligation to react in a specific number of hours or days. In conclusion, the DSA does not impose a time period for the platform to react to the notification.

If, by any chance, the Belgian legislator wanted to impose such a measure, there is a risk that it would be considered unconstitutional by the Constitutional Court, as the French Constitutional Council decided for the Avia law.

About the proposal to recommend the use of technical means to tackle illegal content : the DSA takes into account the fact that the measures implemented by platforms to react to the appearance or reappearance of illegal content may consist of the development of algorithmic techniques. However, there is no clause specifically addressing such artificial intelligence mechanisms or encouraging firms to do so.

Questionnaire the United Kingdom

1. Which authorities are competent for e-commerce?

- The national legislator, the Government and Ofcom.

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Yes

- Consultation outcome, [Online Harms White Paper](#), 15 December 2020
- Policy paper, [Interim code of practice on online child sexual exploitation and abuse](#), 15 December 2020 (voluntary code of practice required by the Digital Economy Act 2017)
- Policy paper, [Interim code of practice on terrorist content and activity online](#), 15 December 2020 (voluntary code of practice required by the Digital Economy Act 2017)
- [Internet Safety Strategy - Green paper](#), October 2017
- Consultation outcome, [Online Harms White Paper: Full government response to the consultation](#), 15 December 2020
- [The Digital Economy Act](#), 2017
- [The Audiovisual Media Services Regulations](#), 2020

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

The Digital Economy Act 2017 required the issuing of voluntary code of practice. One has been made about terrorist content and another about child pornography content. Other codes of practice dealing with other types of unlawful content could be written. The Digital Economy Act 2017 requires that the code of practice include guidance about (section 103(5)) maintaining arrangements to enable individuals to notify providers of the use of their platforms for the specified conduct; maintaining processes for dealing with notifications; ensuring relevant matters are clearly included in the terms and conditions for using platforms; information given to the public about action providers take against their platforms being used for harmful conduct. Those code

of conduct might therefore contain dispositions about the use of AI to prevent the emergence of those content online. As of today, there are already two codes of conduct: the [Interim code of practice on online child sexual exploitation and abuse](#) and the [Interim code of practice on terrorist content and activity online](#). For example, the government has set out in the interim code of practice for online child sexual exploitation and abuse that companies should consider voluntarily using automated technology to identify child sexual exploitation and abuse⁴⁴.

The UK Government is currently discussing the adoption of a new regulatory framework for dealing with harmful and unlawful content online. Although it has not yet taken the form of a definitive regulation, the White Paper on Online Harm and the Government response to this paper give concrete insight on what the content of the regulatory framework will be. The Online Safety Bill, which will give effect to the regulatory framework, is supposed to be issued in 2021.

Two proposals are worth mentioning:

- Proposal 1: setting out the responsibilities of companies to their users by imposing a duty of care in general.
- Proposal 2 : encouraging better technological solutions and their widespread use.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

The Audiovisual Media Services Regulations 2020 impose obligations to video sharing platforms to protect their users from certain types of harm. The regulations include a requirement for the platforms to take appropriate measures to protect children from harmful content, and to protect the general public from incitement to hatred and violence and from criminal content. In our opinion, those measures could potentially include AI technology although this is not the primary purpose of the legislation.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Responsibilities: efficiency and budgetary aspects

A. Which purposes were identified/established?

Setting out the responsibilities of companies to their users by requiring companies to prevent the proliferation of illegal content and activity online.

B. How do the measures try to achieve their purpose?

By imposing a duty of care.

⁴⁴ There is no mention of artificial intelligence as such in the Codes but they reaffirm the importance and usefulness of technology in combating these offences and sometimes describe technological solutions, possibly using AI already in place. For example in the Code of conduct about online child abuse, we can see that : “Companies should consider factors such as the nature of their services, the underlying architecture of their systems, the risks to their users, and the availability of established or emerging technologies appropriate for addressing the issues identified (...)

A grooming detection technique has been developed by Microsoft in collaboration with The Meet Group, Roblox, Kik and Thorn. The technique uses artificial intelligence to analyse patterns in users’ speech and language to spot potential grooming conversations by which online predators intending to lure children for sexual purposes can be detected, addressed and reported. (...) The technique is available via Thorn to qualified online service companies that offer a chat function. Thorn is a technology non-profit that builds technology to defend children from sexual abuse. (...) The Internet Watch Foundation (IWF) provides a keywords list with over 4,000 words and terms known to be linked to child sexual abuse. This list is continually updated as the IWF’s intelligence and proactive searches evolve. The use of the IWF’s URL blocking list can also be helpful in assisting companies with and in line with the examples of best practice.”

For example in the Code of conduct on terrorist content, we can see that : “Some companies already identify and remove terrorist content and activity from their services in response to reports from users, through referrals from law enforcement, or through detection by automated technologies and/or human-led measures, either at the point of or after upload.(...) Companies should take reasonable steps to seek to identify and prevent the upload of terrorist content and activity using proactive measures such as automated technologies alongside human moderation (...) implement automated technologies and/or human moderation that enable expeditious identification of terrorist content and activity indicating an imminent threat to life or serious physical injury.”

The new regulatory framework will apply to companies whose services host user-generated content which can be accessed by users in the UK and/or facilitate public or private online interaction between service users in the UK. It will also apply to search engines. Unfortunately, the services qualified as intermediaries in the e-commerce directive which play a functional role in enabling online activity, such as internet service providers, will be exempt from the duty of care.

Ofcom will oversee and enforce companies' compliance with the duty of care.

The duty of care means that firms must put in place appropriate systems and processes to improve user safety. Firms must conduct a risk assessment and then take steps to address the risks they have identified.

They must also take safeguards for users' rights when designing and deploying content moderation systems and processes and give users a right to challenge content removal.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

Not enforced yet.

D. *Where possible to assess, what impact did the measures have on the government budget?*

Not enforced yet.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

The DSA proposal imposes such duty of care although it has been given a different name in the European regulation. Concretely, it encompasses all obligations aiming at protecting internet users.

First of all, Chapter III of the DSA provides for "Due diligence obligations for a transparent and safe online environment". It contains various obligations such as:

- The establishment of a single point of contact or the designation of a legal representative in the EU for allowing a direct communication between the authorities of a member state and the intermediary service provider (article 10 and 11 DSA).
- Transparency obligations (transparency reports, terms and conditions, online advertising,).
- Risk assessment obligation for very large online platforms (article 26 DSA).
- Mitigation of risks obligations when those risks have been identified following the risk assessment (article 27 DSA).
- The obligation to be subject to independent audit (article 28 DSA).
- The obligation to give access to their data to the Digital Services Coordination of establishment or the Commission upon request (article 31).
- The appointment of Compliance officers (article 32 DSA).

Besides, section 5 of the same Chapter III incorporates the following due diligence obligations:

- The promotion of the establishment of voluntary industry European standards (Article 34 DSA).
- The drawing up of codes of conduct (article 35 and 36 DSA) and crisis protocols (article 37).

3.2.2. Proposal 2 – Technological solutions: efficiency and budgetary aspects

A. *Which purposes were identified/established?*

The UK government recognises that the best solutions for keeping users safe online are technological ones.

B. *How do the measures try to achieve their purpose?*

The government will encourage the use of technical tools in the regulatory framework while taking into account the risks associated with the use of such systems.

Indeed, according to the [government](#), the technical tools are increasingly effective and accurate, the best example being tools based on artificial intelligence. (“The White Paper recognised the critical role of technology in improving user safety online, such as using artificial intelligence to identify harmful content quickly and accurately”)

The government made interesting observations about the use of technical tools in the fight against terrorist content and child sexual exploitation and abuse.

The government is aware of the possibility for firms to adopt an overly risk-averse approach to the identification and removal of material likely to be illegal. For that reason, the regulatory framework must contain strong and effective safeguards to protect the user’s fundamental rights including their freedom of expression such as the possibility for users to challenge the removal.

The regulatory framework will go even further when giving the regulator (Ofcom) the power to require companies to use automated technologies. However, the regulator can only impose the use of technologies highly accurate to identify the illegal content and after obtaining the approval from Ministers on the basis that sufficiently accurate tools do exist.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

Not enforced yet.

D. *Where possible to assess, what impact did the measures have on the government budget?*

Not enforced yet.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

Encouraging firms to create and use artificial intelligence tools capable of fighting illegal content is one solution to the problem of the appearance and reappearance of such content.

Although the use of these automated technologies is recognised in the DSA, platforms are not expressly required or encouraged to use these methods. As long as platforms meet their obligation to remove illegal content as quickly as possible, platforms are not required to do so by algorithmic means. This could be imposed on platforms. However, one should make sure that it is feasible and that it does not create disproportionate obligations upon platforms. Indeed, each provider has different resources. Imposing the use of algorithmic tools to small platforms could create a disproportionate burden upon them.

Questionnaire Germany

The various documents addressed in this section are not policy regulations aimed directly at AI. However, these laws may either influence the use made of AI or impose obligations that can be fulfilled by using AI. For that reason and as a result of discussions with the SPF, we decided that it was interesting in the light of this study to address these laws.

1. Which authorities are competent for e-commerce?

- The national legislator and the government

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

No.

- [Network Enforcement Act](#) (Netzdurchsetzungsgesetz, NetzDG), 1 September 2017

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

The legislation provides for obligations for Telemedia service providers which, for profit-making purposes operate internet platforms which are designed to enable users to share any content, and which have more than two million registered users in the Federal Republic of Germany.

- Proposal 1: [provide users with an effective and transparent procedure](#) for handling complaints by an easily recognisable, directly accessible and permanently available procedure for submitting complaints. In addition, the legislation imposes a reporting obligation for providers which receive more than 100 complaint per calendar year must produce half-yearly German-language reports on the handling of complaints.
- Proposal 2: [obligation to block or remove the content notified that is manifestly unlawful](#) within 24 hours of receiving the complaint. In addition, the legislation creates an obligation to block or remove any unlawful content immediately, this generally being within 7 days of receiving the complaint.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

- Designation of an administrative authority (Federal Office of Justice) with competence to monitor the enforcement of that act.
- Creation of regulatory offences for firms not acting in accordance with that act: fails to produce a report, fails to set up a procedure for dealing with complaints, fails to monitor the handling of complaints, ... Those offences can be sanctioned by a fine up to 500 000 EUR or even 5.000.000 EUR.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Notification procedure: efficiency and budgetary aspects

A. Which purposes were identified/established?

By imposing a procedure for notification and follow-up of notifications, the legislator ensured that the platform processes notifications correctly. If the platform uses AI for this purpose, it must not only comply with the requirements of the law, but also be accountable because of this reporting obligation.

B. How do the measures try to achieve their purpose?

By imposing requirements for the notification process set up by the Platform and for the review of the notification by the Platform which may be done through technical tools such as AI systems.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data.

D. Where possible to assess, what impact did the measures have on the government budget?

The government only had to pass the legislation. After that, the law imposes obligations on firms that enter the scope of the law. There is no budgetary implication for the government.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

The DSA impose obligation in terms of notification mechanism.

Article 14 of the DSA, "Notice and action mechanisms", establishes a notification mechanism for illegal content. It provides for conditions of access (easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means) as well as of substance. The same article states that the notification containing : (a) an explanation of the reasons why the individual or entity considers the information in question to be illegal content; (b) a clear indication of the electronic location of that information, in particular the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content; (c) the name and an electronic mail address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU; (d) a statement confirming the good faith belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete.) shall be considered to give rise to actual knowledge to the service provider which, as a consequence, must take action to remove the content. If he does not, its liability is engaged.

Article 14.6. DSA adds that if the service provider uses automated means for managing or processing the notification or if the provider uses AI techniques to make a decision about the notification, that provider must inform the notifier. There is no other specific disposition applying when the notification system is based on AI technologies.

3.2.2. Proposal 2 – Block/remove content: efficiency and budgetary aspects

A. Which purposes were identified/established?

Tackle efficiently illegal content online quickly. Although not preceded by the law, the mechanisms put in place by platforms to detect illegal content online or to respond to a notification (e.g. by informing the user that its content has been removed) can be done through the use of AI.

B. How do the measures try to achieve their purpose?

By imposing obligation to react to the notification of potential illegal content in a very short timeframe and pair this obligation with offences and high fines.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No data.

D. Where possible to assess, what impact did the measures have on the government budget?

The government only had to pass the legislation. After that, the law imposes obligations on firms that enter the scope of the law. There is no budgetary implication for the government.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

This obligation would affect the current legal framework set up by the e-commerce directive. This directive provides for the exoneration of liability for platforms under certain conditions. Here, the legislation imposes supplementary obligations on platforms. The legislation would also fix the sanctions those platforms face in case of noncompliance.

In theory, a similar law could be passed in Belgium. However, in light of the strict and rapid nature of the intervention imposed on the platforms and the absence of a mandatory judicial decision, there might be a risk that if such a law is passed in Belgium, it would potentially be annulled at least in part, as it has been the case in France. The Belgian Constitutional Court would have to conduct an analysis to determine whether this legislation is compatible with people's constitutional and fundamental rights. We can wonder whether the Belgian Constitutional Court would hold a reasoning similar to the French one and consider the legislation as a violation of the fundamental rights of citizens especially their freedom of expression and the right to information or if, on the contrary, it would consider the legislation as a proportionate and acceptable infringement of those rights.

CHAPTER 5 – INSURANCES (WP 5)

Questionnaire the Netherlands

1. Which authorities are competent for insurances?

- De Nederlandsche Bank – DNB
- Autoriteit Financiële Markten – AFM

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

Both the [AFM](#) (p. 19) and the [DNB](#) (p. 1-2) separately and in [cooperation](#) have published a variety of policy documents related to AI, even specifically drafted for the insurance sector, mostly between 2016-2021. The documents can be consulted on the website of the [AFM](#) and the [DNB](#). Generally, the [AFM](#) (p. 58) and [DNB](#) (p. 3) consider it important to cooperate amongst themselves and with other supervisors, especially since AI has an impact on several legal domains.

The AFM and DNB have also established an “[InnovationHub](#)” in 2016, complemented with a “[Regulatory Sandbox](#)” and an “[iForum](#)” (p. 2) in 2017 and 2019, that informs and supports entities that are active in amongst other things, the insurance sector with their innovative financial projects related to for example [artificial intelligence](#). The AFM and DNB also frequently request feedback from the industry.⁴⁵

In 2019 the AFM and the DNB [summarised](#) the points of attention as follows:

1. There is a risk that insurers may not have a fundamental vision on how to apply AI.

If insurers start using AI without a clear underlying strategy, the insurer faces, amongst other things, the following risks: (i) inconsistency with risk appetite/strategy, (ii) underwriting risks (mistakes in terms of customer acceptance, pricing, ...) and (iii) reputational risks (p. 16).

2. Insufficient knowledge sharing and testing can jeopardise the proper implementation of AI within the organisation.

If the insurer does not create (policy) awareness in the organisation and relevant departments, then the insurer could breach its own risk appetite framework. The insurer faces, amongst other things, the following risks: (i) operational risks and (ii) underwriting risks, increasingly so if the AI expertise is not centralised (but fragmented throughout the organisation) (p. 18).

3. Lack of sufficient, correct, complete or varied data may give rise to underwriting risks and discrimination.

AI applications function entirely on the optimal analysis of patterns inherent in data. Correct and representative data are crucial. Moreover, if a model is more complicated and less transparent, it will be more difficult to detect and solve errors or biases (p. 19).

4. Lack of explainability can lead to breaches of the law (e.g. GDPR) and undetected discriminatory biases.

Due to the complexity of AI algorithms, the outcome/decision of an AI tool/technique is not always easy to explain. However, without such an explanation the insurers risks breaching the law

⁴⁵ See for example AFM and DNB, Artificial Intelligence in the Insurance Sector, 2019, p. 6; AFM and DNB, Continuing dialogue – InnovationHub and Regulatory Sandbox: lessons learned after three years, 2019, p. 2; DNB, Insurtechontwikkelingen bij kleine en middelgrote verzekeraars, 2019.

(e.g. rules related to automated decision-making of the GDPR). Moreover, the insurer will face reputation risks (p. 21-23).

5. Outsourcing generates potential underwriting and operational risks.

Insurers frequently ask for external support/advice when developing AI tools/algorithms. The insurer risks acquiring data of dubious quality or might not fully understand the training/functioning of the AI tool/technique (p. 24-25).

6. Insufficient validation procedures can result in the insurer "losing control".

Without a clear view on the functioning of the AI tool/technique, the insurer cannot control the risks related to the AI tool/technique.

7. AI tools/techniques are not always in line with what is socially acceptable and explainable (and can thus result in a breach of the duty of care).

The decisions of AI tools/techniques cannot always be explained and might result in decisions that do not benefit the financial situation of the consumer (p. 27). Moreover, insurers must consider the impact that an AI tool/algorithm might have on certain groups of insureds (to avoid exclusion and increase solidarity).⁴⁶ Therefore, the [insurer](#) is once again confronted with amongst other things: (i) reputation risks and (ii) legal risks (p. 2).

Although the above risks could also exist in other sectors, the [DNB](#) emphasises that the financial sector faces additional pressure because the financial sector (i) is commonly held to a higher societal standard than many other industries, (ii) plays an important role in terms of financial stability, (iii) has an inherent international dimension, and (iv) has a specific data environment (p. 30-31).

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

Yes.

In 2019 the AFM and the DNB published two important documents with a variety of proposals. For the time being the [AFM and DNB](#) state that there is no real need for new legislation, and that easily accessible information/tailored explanations about the current rules often suffice for market participants.

1. General Principles for the use of Artificial Intelligence in the financial sector (DNB): the 'SAFEST' principles

The [DNB](#) formulated six principles characterising the responsible use (in conformity with the regulations and the societal expectations) of AI and formulated proposals related to each of the principles (p. 7):

1. Soundness
2. Accountability
3. Fairness

⁴⁶ See also: Verbond van Verzekeraars, Solidariteitsmonitor, 2018, <https://www.verzekeraars.nl/media/5375/solidariteitsmonitor-2018-eenmeting-versie-22-oktober-2018.pdf>.

4. Ethics
5. Skills
6. Transparency

The [principles](#) are linked to controlled and sound business operations and should be applied in a proportional matter (in light of the scale, complexity, materiality and role of the AI tool/algorithm) (p. 33). The principles are non-binding but serve as a starting point for the [DNB's supervision](#) on the use of AI (p. 6).

- 1.1. [Soundness](#): AI applications should be reliable, accurate, behave predictably and operate within the boundaries of the applicable rules and regulations (p. 34-35).
- 1.2. [Accountability](#): Financial institutions should understand that they are responsible for their AI applications and must demonstrate that they have operationalised accountability for these applications throughout their organisation (p. 35-36).
- 1.3. [Fairness](#): Financial institutions must define the concept of fairness and demonstrate how they ensure that their AI applications behave accordingly (p. 36-37).
- 1.4. [Ethics](#): Financial institutions should ensure that their customers, as well as other stakeholders, can trust that they are not mistreated, harmed – directly or indirectly – because of the deployment of an AI tool/algorithm (p. 37).
- 1.5. [Skills](#): On all levels, a sufficient understanding of the strengths and limitations of the organisation's AI systems is vital (p. 37-38).
- 1.6. [Transparency](#): Financial institutions should be able to explain how they use AI in their business processes and (where reasonably appropriate) how these applications function (to ensure auditability and supervision) (p. 38-39).
2. Artificial Intelligence in the Insurance Sector (DNB and AFM)

The AFM and the DNB have formulated a set of [key considerations](#) surrounding the design, implementation and use of AI tools specifically for the insurance sector.

- 2.1. An insurer's board should carefully consider whether and how AI should be used (AI Policy).
- 2.2. An insurer must foresee a clear governance structure, internal communication (guidance on the use of AI) and AI expertise (p. 18).⁴⁷
- 2.3. Insurers must be able to demonstrate that they are in control of the relevant input data. The availability of high-quality and varied input data is a precondition for applying AI (p.19-20).
- 2.4. Insurers should select an AI model on an informed basis. When deciding to use AI applications, insurers should take into account the statistical risks and the possible complexity of the applications (p. 20-21).
- 2.5. Insurers should select a model/technology with special attention for explainability (especially for sensitive processes) (p. 21-22).
- 2.6. If discriminatory biases in AI applications cannot effectively be avoided, the insurer should consider not deploying these applications (especially if there is a direct impact on the customer). An insurer must have systems and processes in place to prevent discriminatory outcomes of AI tools/algorithms (p. 23).

⁴⁷ As already foreseen under Solvency II through the roles of the key functions.

- 2.7. Insurers must monitor their AI applications, regardless of whether they have been developed in-house or outsourced to an external party with special attention for their outsourcing policy and the criteria for critical outsourcing contained therein (p. 25).
- 2.8. Insurers must establish a validation procedure for AI tools/algorithms, structured in such a way that it can be determined whether AI applications are fit for purpose and must ensure a minimum frequency for revalidations (p. 25-26).
- 2.9. Insurers must ensure that decisions made by their AI applications benefit the financial well-being of consumers (either consciously or unconsciously) with special attention for the consequences of behavioural pricing (p. 27-28).
- 2.10. Insurers must ensure that the outcomes of the AI application are justifiable (in social terms) with particular attention for (i) the type of input parameters that are used (and the intuitive relationships between parameters and the risk to be determined) and (ii) the categorisation of individuals into risk groups (p. 28-29).

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

/

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Establishment of an InnovationHub and a Regulatory Sandbox: efficiency and budgetary aspects

A. Which purposes were identified/established?

The AFM and DNB set up the [InnovationHub and the Regulatory Sandbox](#) to accommodate innovation, adequately address risks and gain knowledge about technological and other developments in the financial market (p. 4).

B. How do the measures try to achieve their purpose?

The InnovationHub offers support to market participants and answer questions about rules and policies applicable to the market participant's innovative financial products, services and business models. The Regulatory Sandbox allows parties to develop innovative concepts in compliance with the underlying objective of supervisory rules and policies (as a solution for unnecessarily restrictive supervisory rules or policies). The [laws and regulations](#) remain fully applicable (p. 4).

C. Where possible to assess, to what extent did these measures achieve their purpose?

The InnovationHub and Regulatory Sandbox have recently published their lessons learned after three years. Even though they formulate [some observations and working points](#), the aforementioned initiatives seem to achieve the abovementioned purpose(s) (p. 11-15).

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 5.1.3. and 5.1.4.). In Belgium, the concrete implications of new business models and the regulatory gaps are also not clear yet. Therefore, setting up an innovation hub/regulatory sandbox could be useful.

3.2.2. Proposal 2 – Compliance-by-design and appropriate governance: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose is to ensure compliance with a variety of laws and regulations applicable to AI tools/algorithms.

B. How do the measures try to achieve their purpose?

Insurers should take their obligations into account when designing an AI tool/technique (compliance-by-design) and must align the (outcome of) AI applications with their legal obligations, values and principles.

They should, [amongst other things](#) mitigate financial and legal risks in the development and use of AI applications by:

- Involving domain experts in the development and implementation of AI applications.
- Setting up boundaries to constrain model outcomes.
- Defining and documenting evaluation metrics.
- Periodically retraining/recalibrating/assessing the AI tool/technique (e.g. in case of significant changes).
- Defining and documenting the criteria for significant change.
- Defining and documenting escalation procedures.
- Foreseeing [fall-back plans](#) (p. 34-35).
- A *priori* documenting criteria for the fitness of the model outcomes based on legal requirements and the firm's values and principles.
- Taking into consideration the customers' interests when designing or approving customer-oriented AI applications.
- Avoiding the exploitation of consumers' behavioural patterns/psychological biases in a way that would negatively impact their financial situation.
- ...

To ensure compliance with, for example, consumer related principles/obligations, an insurer could ask itself the [following questions](#) (p. 27-28):

- What may be expected from an 'average', rational consumer?
- What will be the impact on consumers if they make bad choices?
- How much effort does it take for an insurer to protect consumers from making choices that are not beneficial to their financial well-being?

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 4.2.1., 4.3.2., 5.1.3., 5.2.2., 6.1.). A predefined governance/compliance framework/strategy could prevent undesired breaches of rules/regulations on a systematic basis.

3.2.3. Proposal 3 – Use specific criteria and evaluation methods for model selection: efficiency and budgetary aspects

A. Which purposes were identified/established?

Choosing a wrong model can lead to undesired and unexpected results (as an example the [AFM and DNB](#) mention the phenomenon “overfit” (p. 20)).⁴⁸

B. How do the measures try to achieve their purpose?

Insurers should pay special attention to the [mitigation of model risks](#) (p. 35) for material AI applications by, amongst other things:

- Carefully selecting criteria for model choices including criteria other than quantitative evaluation metrics, but also criteria such as explainability.
- Choosing similar models for similar analyses.
- Assessing the impact of incorrect model outcomes.
- Regularly assessing the model outcomes against conventional models.

Before selecting an AI model the following questions are important according to the [DNB and AFM](#) (non-exhaustive list):

- For which processes and components in the chain does the insurer intend to use AI?
- What criteria serve as a basis for deciding whether to use AI (machine learning, big data)? (p. 17)
- Can the insurer systematically substantiate why a certain model and technology has been chosen?
 - Is the decision for a certain model based on the quantity, quality and diversity of the available input data?
 - When a certain model or technology was chosen, were factors such as explainability, complexity, and reliability taken into account alongside 'best fit' considerations?
 - Is there a certain degree of consistency between the models and technologies used for determining premiums and those used for determining technical provisions?
 - Were experts from the relevant business areas, e.g. the IT, Actuarial and Risk management (model validation) functions, involved in the selection process?
 - Can the insurer give insight on how the chosen technology works in a more general sense, and for which types of processes or types of datasets one specific technology is more suitable than others?
 - Can the insurer describe circumstances under which the use of the chosen technology would no longer be appropriate? Is this checked periodically and, if so, how? (p. 21)

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. The above measures (such as predefined criteria for model selection) could ensure that Belgian insurance companies (i) take model risks into account from the start and (ii) monitor that the desired/expected outcomes are guaranteed.

3.2.4. Proposal 4 – Definition of data quality standards and controls: efficiency and budgetary aspects

A. Which purposes were identified/established?

⁴⁸ The model produces “erroneous results for insured persons with characteristics that differ from those in the training set applied”.

[Data quality](#) is important to ensure compliance with a variety of laws, regulations and principles applicable to AI tools/algorithms (e.g. explainability, non-discrimination and the duty of care) and to avoid risks (e.g. underwriting risks). An AI tool/technique is highly dependent on data as it basically analyses the patterns that are inherent in the data that has been inserted in the tool (p. 19).

B. How do the measures try to achieve their purpose?

The [DNB and AFM](#) (p. 19-20) encourage insurers to pay particular attention to data quality and corresponding controls, including by emphasising that insurers should, amongst other things, safeguard and improve the quality of data by:

- Defining minimal requirements regarding data quality.
- Continuously putting in the efforts to ensure correct, complete and representative data.
- Paying attention for missing/incorrect data-points, sources of bias in data, features and inference results.
- Introducing procedures and safeguards to maintain and improve data integrity and security during the data collection/preparation/management processes.
- Structurally documenting and evaluating the data integrity and bias issues.
- [Archiving the original data sets](#) (p. 34-35).
- Clearing the datasets used of unwanted biases and assumptions (to the greatest extent possible).
- ...

[DNB and AFM](#) (p. 19-20) emphasise the following questions (non-exhaustive list):

- Does the insurer have an up-to-date overview of the data elements to be used?
- Have data quality standards been drawn up for the input data to be used?
- Are controls in place to monitor the quality of the input data on an ongoing basis?
- Has a risk assessment been conducted of the quality and completeness of the input data?
- Are any shortcomings in the data remediated appropriately?
- Does the input data satisfy the data quality standards set by the insurer?

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 2.2.1.). The above measures (such as predefined data quality and verification requirements) could ensure that Belgian insurance companies (i) take data quality into account from the start and (ii) monitor that the data quality remains intact.

3.2.5. Proposal 5 – AI Policy and Communication: efficiency and budgetary aspects

A. Which purposes were identified/established?

Without a clear vision on the use of AI, insurers risk that the application of AI tools/techniques are not in line with the defined risk appetite and strategy. This could result in amongst [other things](#) reputational damage and underwriting risks (p. 17).

B. How do the measures try to achieve their purpose?

Insurers must consider their overall strategy and AI policy decisions and communicate the strategy/policy throughout the entire organisation.

Concretely, financial institutions, including insurers, should, amongst other things:⁴⁹

- Define a clear policy at board level regarding the deployment of AI applications (including a clear risk policy on the use of AI).
- Be transparent about the policy and decisions regarding the adoption and use of AI internally.
- Communicate the AI policy throughout the organisation.
- Document and justify any material decisions regarding AI applications, their underlying models and data.
- Document and communicate the limitations of the adopted models, data sets and circumstances triggering discontinuation.
- Document the reasons for opting for a particular AI model.
- Motivate/document/approve decisions favouring accuracy over traceability and explainability.
- ...

The [AFM and DNB](#) (p. 17) also offer a list of questions that the insurers can take into consideration when formulating the policy (non-exhaustive list):

- What criteria serve as a basis for deciding whether to use AI (machine learning, big data)?⁵⁰
- For which processes and components in the chain does the insurer intend to use AI?⁵¹
- What rules does the insurer apply for training and retraining models? How often does the insurer want to retrain its models? How does the insurer structure the processes related to training and retraining?⁵²
- In the field of ethics and social accountability⁵³:
 - o How much differentiation does the insurer consider justified, both with regard to risk assessments and price optimisation (dynamic pricing, behavioural pricing)?
 - o What type of input data does the insurer intend to use for differentiation?
 - o To what extent does the insurer intend to use AI to enable customers to improve their risk profile (risk prevention in healthcare or in the home, or behind the wheel)?
 - o Is the insurer considering offering a premium discount in exchange for submitting data?
- How does the insurer assign decision-making responsibilities, processes and roles within the defined policy frameworks?⁵⁴
- How does the insurer guarantee that the responsibility for AI applications has been clearly assigned within the board, and that the responsible board member is sufficiently knowledgeable and experienced to estimate, test and manage the risks of AI applications?⁵⁵

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available

D. Where possible to assess, what impact did the measures have on the government budget?

⁴⁹ See: DNB, General Principles for the use of Artificial Intelligence in the financial sector, 2019, p. 38-39; AFM and DNB, Artificial Intelligence in the Insurance Sector, 2019, p. 17.

⁵⁰ Cf. Proposal 3.

⁵¹ Cf. Proposal 3.

⁵² Cf. Proposal 2 and 3.

⁵³ Cf. Proposal 7.

⁵⁴ Cf. Proposal 2 and 6.

⁵⁵ Cf. Proposal 6 and 8.

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 4.2.1., 5.1.3.). A predefined strategy with a corresponding governance framework, documented in a policy, could prevent undesired breaches of rules/regulations/strategies on a systematic basis.

3.2.6. Proposal 6 – Ensure control and accountability: efficiency and budgetary aspects

A. Which purposes were identified/established?

Accountability for the decisions and outcomes of AI tools/techniques should be guaranteed.

B. How do the measures try to achieve their purpose?

Accountability can be achieved if insurers, amongst other things:

- [Define and consistently apply](#) the organisation's AI policy (Proposal 5) on in-house and external applications (p. 34-35).
- Ask themselves how they can [effectively assign](#) decision-making responsibilities, processes and roles within the defined policy frameworks (p. 17).
- [centralise the internal supervision](#) (p. 18) to ensure that models can be carefully validated while guaranteeing continuity (specific methods include centralising data science expertise in a specific team, initiating a structured approach in sharing expertise throughout the organisation⁵⁶).
- Define/divide roles and responsibilities regarding AI across the entire organisation (including at board level).⁵⁷
 - o Final accountability for AI applications and the management of associated risks should be clearly assigned at the board of directors level (i.e. the final accountability for AI applications and their outcomes should be assigned to one or more board member(s) also for externally developed/sourced AI applications).
 - o Accountability should be integrated in the organisation's risk management framework (i.e. clear roles and responsibilities must be assigned throughout the organisation to ensure the responsible use/management/auditability of AI applications).
- [Operationalise accountability](#) with regard to external stakeholders (i.e. on request/where appropriate specific AI decisions/outcomes must be reviewed by a domain expert to obtain a verification/explanation, verified/relevant supplementary customer data must be taken into account when performing a review of an AI decision/outcome, ...) (p. 35-36).

The already [existing functions, based on Solvency II](#), can also assume AI specific roles (p. 18).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

⁵⁶ Cf. Proposal 8.

⁵⁷ See: DNB, General Principles for the use of Artificial Intelligence in the financial sector, 2019, p. 35-36; AFM and DNB, Artificial Intelligence in the Insurance Sector, 2019, p. 17.

Yes. In Belgium as well, it might be useful to have a point of contact and to have someone accountable when it comes to the use of AI by an insurer/another related entity.

3.2.7. Proposal 7 – Implementation of ethical and fairness standards, procedures and controls (e.g. “human-in-the-loop”) in AI tools/techniques, with a special attention for (unintentional) biases, discrimination and social acceptance: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose is to achieve compliance with ethical standards, the principle of fairness, non-discrimination and solidarity.

B. How do the measures try to achieve their purpose?

Amongst other things, the AFM and DNB suggest the following:

- [Define “fairness”](#) (qualitatively defined in terms of group fairness and/or individual fairness) and “ethical” behaviour (p. 36-37).
- [Provide](#) procedures, systems, processes and evaluation methods to detect and prevent possible breaches (such as discriminatory outcomes) (p. 23).
- Fairness and ethical behaviour must be taken into account in the design and training of the AI application, both in the selection of input parameters, evaluation metrics and potential sources of unintentional bias.⁵⁸
- trade-offs between process fairness, outcome fairness and accuracy must be substantiated/documented/available for review.
- material AI tools/algorithms should be designed with a “human-in-the-loop” and/or “human-on-the loop” process to prevent unintentional bias.
- [procedures](#) for after the fact reviews and instigation of customer/stakeholders must be put in place (p. 36-37).
- [objectives, standards and requirements must be specified in an ethical code](#) (p. 37),⁵⁹ to guide the adoption and application of AI (i.e. definition of criteria to ensure consistent decision making on whether specific processes and functions are suitable for AI⁶⁰ and on the use of specific models/methods/data in AI applications,⁶¹ formulating procedures to ensure that ethical and other material concerns are raised to an ethics commission/another suitable body⁶², ...).
- generally the review of (the outcomes of) the AI applications for unintentional bias must be [foreseen](#) (p. 36-37).

The insurer should also ask itself the following questions (non-exhaustive list):

- How are input variables challenged to detect possible discriminatory bias?
- How are outcomes checked for discriminatory bias?
- How can [checks for discriminatory bias](#) be refined and made more robust (p. 23)?
- To what extent are the patterns and proxies found and used by the AI application fair and explainable from a social point of view? And how has this been tested?
- How strong is the correlation between the patterns and proxies and the insured risk?

⁵⁸ DNB, General Principles for the use of Artificial Intelligence in the financial sector, 2019, p. 36-37; AFM and DNB, Artificial Intelligence in the Insurance Sector, 2019, p. 23.

⁵⁹ See also: Verbond van Verzekeraars, Ethical Framework for the application of AI in the Insurance Sector, 2020 (binding, as self-regulation, for members of the Dutch Association of Insurers).

⁶⁰ Cf. Proposal 2 and 5.

⁶¹ Cf. Proposal 3 and 4.

⁶² Cf. Proposal 6.

- To what extent is there an intuitive link between the patterns and proxies found and used on the one hand, and the claim likelihood and risk for the insurer on the other?
- To what extent and how is it possible for individuals to identify, demonstrate and draw attention to any deviations from the peer group in which they are placed?
- To what extent is the choice for more far-reaching or less far-reaching [microsegmentation](#) socially explainable (p. 28-29)?

The [DNB and AFM](#) also suggest some evaluation methods to assess whether the AI tool/technique engages in discriminatory behaviour (p. 23-24):

- Adversarial modelling.
- Sample testing with identical test groups (where a discriminating variable is the only difference between the groups).
- Specific checks for biases in false positive outcomes (rather than restricting tests to overall model outcomes).

The [DNB and AFM](#) (p.30) do not list separate measures (“Key considerations”) to ensure compliance with the solidarity principle.⁶³ However, the DNB and AFM emphasize that the deployment of AI underlines the need for a debate on solidarity in the insurance sector. Although the degree of solidarity is part of a broader debate, the use of AI can increase the risk that some people would be excluded or would pay (unnecessarily) high(er) premiums. This is because AI allows insurers to make a more detailed and personal assessment of the risk related to a particular individual. An initiative that the DNB and AFM promote is the (annual) “Solidarity Monitor” published by the Dutch Association of Insurers. The Solidarity Monitor, monitors the solidarity by assessing the difference between the premiums of certain reference persons.⁶⁴

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. The concern for unfair/discriminatory/socially unacceptable outcomes also exists in Belgium (see Part1 Ch5 2.2.2.8., 2.2.9., 2.2.10.). The above measures (such as evaluation methods and predefined criteria) could ensure that Belgian insurance companies (i) take fairness, non-discrimination and other ethical/social standards into account from the start and (ii) monitor that they continue to act in conformity with the set standards.

3.2.8. Proposal 8 – Training and expertise requirements: efficiency and budgetary aspects)

A. Which purposes were identified/established?

The purpose is to avoid behaviour contrary to the insurer’s risk appetite and the applicable rules/regulations.

B. How do the measures try to achieve their purpose?

Individuals working with AI tools/techniques, on all levels, should be trained (via awareness programs and/or specific training depending on the circumstances).

⁶³ Cf. Proposal 5.

⁶⁴ Also see: Verbond van Verzekeraars, Solidariteitsmonitor Verbond toont stabiel beeld, <https://www.verzekeraars.nl/publicaties/actueel/solidariteitsmonitor-verbond-toont-stabiel-beeld>.

The [DNB](#) suggests the following (p. 37-38):

- Ensure that senior management has a suitable understanding of AI in relation to their roles and responsibilities (i.e. the board of directors' competence and expertise include relevant and up to date knowledge and/or experience of AI, managers responsible for AI applications are trained,...).
- Train risk management and compliance personnel in AI.
- [Develop awareness and understanding](#) of AI within the organisation (i.e. personnel working with AI tools/algorithms are trained, educational programs can be used to create and improve awareness regarding the use of AI and the associated risks throughout the organisation, ...) (p. 37-38).
- Enable [structured sharing](#) of knowledge/experiences (p. 18).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 5.1.3.). Training programs can mitigate the risk that the insurer breaches rules/regulations or its own (risk) policies.

3.2.9. Proposal 9 – Explainability requirements: efficiency and budgetary aspects

A. Which purposes were identified/established?

If the outcome/decision of an AI tool/algorithm cannot be explained this can result in undesired/unexpected outcomes, possibly, in breach of the applicable rules/regulations/policies. Adherence to the [explainability principle](#) enables proper risk management and auditability (p. 38).

B. How do the measures try to achieve their purpose?

The [AFM and DNB](#) (p. 21-22) state that not every process requires the same degree of explainability. For example, back-office processes (limited impact on the customer) require a lower degree of explainability compared to models for pricing, customer acceptance and fraud detection (direct impact on the customer).⁶⁵

The [DNB](#) stated, amongst other things, the following (p. 39):

- Where reasonable, improve the reproducibility of operations and outcomes of AI systems for review processes.
- The traceability and explainability should be (constantly) improved on aggregate/individual level via processes/tools/interfaces.
- Periodic expert evaluation of the model outcomes should be foreseen especially in case of obscurity.
- Procedures for after the fact reviews and instigation of customer/stakeholders should be put in place.
- ...

The insurer must also ask itself the [following questions](#) (p. 22) (non-exhaustive list):

⁶⁵ Cf. Proposal 3 and 10.

- To what extent are models used in processes that have a direct and large impact on customers - and thus possibly involve risks for the insurer with regard to product development, duty of care, legal and reputation risks - or in processes that have a direct and large impact on the insurer's stability?
- To what extent can the model technology be explained? What degree of explainability is appropriate for that specific process?
- What degree of explainability is appropriate for that specific process?⁶⁶

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 2.2.2., 4.3.2., 5.1.3., 5.2.2., 6.1.). A preselected explainability method combined with periodic evaluations could ensure that Belgian insurance companies (i) systematically think about the explainability concerns related to AI tools/techniques and (ii) monitor that the explainability level remains intact.

3.2.10. Proposal 10 – Risk and impact assessments: efficiency and budgetary aspects)

A. Which purposes were identified/established?

The purpose is to ensure that all (sorts of) risks and impacts related to the AI tool/algorithm are identified. Linked thereto a risk/impact assessment can avoid that all AI tools/algorithms receive the same (level of) treatment (proportionality).

B. How do the measures try to achieve their purpose?

The AFM and DNB stress on multiple occasions that insurers must make informed decisions (e.g. on the selection of the model⁶⁷) and offer a variety of questions that the insurers can ask themselves to uncover the risks related to a certain decision/option.

Related to proportionality, the [DNB](#) (p. 33) stated that the SAFEST principles should be applied in a proportional matter (in light of the scale, complexity, materiality and role of the AI tool/algorithm). The [DNB](#) published a so-called 'heat map' to demonstrate this (p. 33-34).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

3.2.11. Proposal 11 – Establish validation procedures: efficiency and budgetary aspects)

A. Which purposes were identified/established?

⁶⁶ Cf. Proposal 3 and 10.

⁶⁷ Cf. Proposal 3.

The purpose is to ensure that the AI tool/technique functions (on an ongoing basis) [within the boundaries](#) as defined and accepted in the design phase (in conformity with the applicable rules/regulations and policies/procedures) (p. 25).

B. How do the measures try to achieve their purpose?

In general the entire AI tool/algorithm should be validated periodically and/or based on defined criteria.

[Possible validation methods](#) are (non-exhaustive list) (p. 25-26)

- Sanity checks on the outcomes of the model.
- Periodic retraining with newly available data.
- Questioning whether the outcomes are plausible.
- Determining/checking crash barriers (i.e. outcomes that fall outside a predetermined scope).
- Manual checks.

[Relevant questions](#) that the insurer should ask itself include (non-exhaustive list) (p. 26):

- How important/critical is the model in terms of impact on the customer and the stability of the insurer, and does the validation procedure focus on the significance of the model?
- How does the validation procedure differentiate between various types of machine learning technologies, between different training methods for models (supervised, unsupervised learning) and between self-learning and non-self-learning algorithms?
- How is the quality (accuracy, completeness, suitability) of the input data taken into account in the validation?
- For a non-self-learning algorithm/model: what is the minimal frequency of the validations?
- How are 'major' and 'minor' changes defined in the model? How big do the changes need to be before formal revalidation must take place?

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 5.1.3.). Requiring insurers to regularly check their AI tools could help to avoid unintentional breaches of rules/regulations/policies.

3.2.12. Proposal 12 – Outsourcing requirements: efficiency and budgetary aspects

A. Which purposes were identified/established?

The purpose is to ensure that the insurer retains control (and accountability) over the AI tool/algorithm.⁶⁸

B. How do the measures try to achieve their purpose?

[Insurers](#) should (p. 25)

- Have an outsourcing policy in place.
- Determine which outsourced AI applications are critical.

⁶⁸ Cf. Proposal 6.

- Have a process in place for monitoring their AI applications (also if they have been outsourced).
- Act in accordance with their outsourcing policy and the criteria/principles for critical outsourcing.⁶⁹

The AFM and DNB refer in particular to the DNB's Good practice document for outsourcing by insurance companies and the guidance on checking Solvency II data quality by insurers. [Insurers](#) could also take steps to prevent outsourcing of AI applications that undermine continuity (p. 25).

Lastly it is important that the insurer asks itself the [following questions](#) (p. 25)

- Does the insurer possess sufficient expertise to understand how the external application works?
- Have agreements been made with external parties regarding the quality and origin of the data provided, and on how the external models have been trained/calibrated?

The AFM and DNB state that if the above questions are not adequately addressed that the insurer should reconsider the relationship with the external party in question.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

No information available.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No information available.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

Yes (see Part1 Ch5 2.2.6., 4.2.1., 5.1.3.). The above measures could ensure that Belgian insurance companies retain control (and accountability) over their outsourced AI tools/algorithms.

3.2.13. Proposal 13 – Legal basis for the processing of health data for insurance purposes: efficiency and budgetary aspects

Article 30.3 b) Uitvoeringswet AVG states that: "In view of Article 9, second paragraph, part h, of the Regulation, the prohibition to process health data does not apply if the processing is carried out by insurers as referred to in Article 1: 1. of the Financial Supervision Act or financial service providers who mediate in insurance as referred to in Article 1: 1 of that Act, insofar as the processing is necessary for (1) the risk assessment of the insured risk and the data subject did not object to the processing; or (2) the execution of the insurance contract or assisting in the management and execution of the insurance contract".

It follows that the Dutch legislator made use of the option in article 9, 2 h) GDPR to create an exemption to the prohibition to process health data by insurance companies and insurance intermediaries. Moreover, it follows from the wording of the article that this Dutch provision applies to the processing of health data in all insurance contracts, and not only in health insurance policies. Subsection 1 regulates the situation in which someone completes a medical questionnaire in order to obtain a specific insurance policy. These data are necessary to assess the insured risk. Subsection 2 deals with situations that may arise during the execution of the insurance contract, in which insurers process health data.⁷⁰ The exemption only applies if the processing of health data is necessary for two these purposes.

⁶⁹ Cf. Proposal 6

⁷⁰ MvT, Kamerstukken II 2017-2018, 34 851, nr. 3, 113.

So far, there is no legal basis allowing insurance companies to apply automated individual decision-making, including profiling. Article 40 Uitvoeringswet AVG only allows for automated individual decision-making if it is necessary to comply with a legal obligation resting on the controller (article 6, 1 c) GDPR) or necessary for the fulfilment of a task of general interest (article 6, 1 e) GDPR).

A. Which purposes were identified/established?

The Dutch Government argued that it is not always possible for insurers to rely on explicit consent. To create legal certainty, the Government created an exemption to the prohibition to process health data specifically for insurance companies and insurance intermediaries.

B. How do the measures try to achieve their purpose?

The Dutch Government created an exemption for the processing of health data for insurance purposes on the basis of article 9, 2 h) GDPR.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

Questionnaire France

1. Which authorities are competent for insurances?

- ACPR, l'Autorité de contrôle prudentiel et de résolution, part of the « Banque de France ».

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

The ACPR has issued a variety of relevant policy documents in the last 10 years, mostly between 2016-2021, and often refers to artificial intelligence in its annual reports.

The ACPR established a multidisciplinary [Fintech Innovation Unit](#)⁷¹ in June 2016 to support the so-called digital revolution in the financial sector.⁷² The Fintech Innovation Unit also encompasses a [Fintech Innovation Hub](#). The Fintech Innovation Hub informs and supports entities that are active in amongst other things, the insurance sector with their innovative financial projects related to for example artificial intelligence.

The ACPR also frequently requests feedback through [public consultations](#) (standardised questionnaires). In a [discussion paper from December 2018](#), the ACPR summarised the following relevant challenges related to artificial intelligence as follows:

- Data processing: risks associated with artificial intelligence

The [ACPR](#) (p. 16) emphasises the importance of data quality and the lack of (explicit or implicit) bias in processing data to protect firms and customers from discrimination risks or inadequate advice (due to the so-called “filter bubble” effect).

⁷¹ In early 2018 another task force was established (ACPR, Artificial intelligence - challenges for the financial sector, 2018).

⁷² See for example: ACPR, Annual Report, 2017 (https://acpr.banque-france.fr/sites/default/files/medias/documents/2017_annual_report_acpr.pdf) and ACPR, La data représente un « potentiel de changement majeur », 2017, https://acpr.banque-france.fr/sites/default/files/medias/documents/20170926_interview_n_beaudemoulin_point_banque.pdf.

- The risk of players' dependency and the change of power relationships in the market

Since a couple of players might dominate the artificial intelligence sector, the financial market might become dependent on their services, with the usual negative consequences related to concentrated market power (e.g. high prices, difficulty in accessing and auditing the financial activity, ...). Specifically related to [artificial intelligence](#) (p. 17), this could worsen the risk of lack of explainability (see below).

- Challenges to financial stability and sovereignty

Artificial intelligence (algorithms) can lead to financial instability and systemic risks, amongst other things because (i) the algorithms use historical data and are trained to function in normal situations (not in crisis situations) and (ii) the algorithm, using a certain set of variables, can lead to (negative) "[sheep-like behaviour](#)" (p. 18).

- Governance and "explainability" of the algorithms

The ACPR recognises the variety of regulatory issues related to artificial intelligence (e.g. in relation to capital requirements, allocation of assets, internal modelling, risk management, customer protection, ...) and states that artificial intelligence will challenge the traditional methods of *a priori* tracing and controlling (internally and externally) the decisions or actions taken by artificial intelligence algorithms (currently taken by humans).

More in particular the [ACPR](#) (p. 19) recognises, amongst other things, the importance of controlling the risks accepted by the company, the duty of loyalty to customers (i.e. based on regulations) and respecting the obligations related to automated processing of personal data and transparency on decisions taken.

From the regulator's perspective, the [ACPR](#) (p. 24-25) concludes that regulators must do the following:

- In the short term: accompany the market to ensure the development of artificial intelligence algorithms while respecting the compliance with regulatory objectives.
- In the medium term: anticipate market changes to adapt (existing) regulations and supervisory methods.
- Focus on using artificial intelligence for their own missions (SupTech).

In 2020 the ACPR published [an approach to govern the issues of explainability and governance of AI/ML](#). Other relevant, but more general documents include amongst other things, [a survey on the digital revolution in the French insurance sector](#) and [a presentation](#) named "La révolution numérique dans les banques et les assurances françaises".

The documents can be consulted on the website of the [ACPR](#).

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

- In 2018

In the abovementioned discussion paper from December 2018 the [ACPR](#) already formulated the following high-level recommendations.

1. [Define appropriate governance of algorithms](#) (p. 19-20)

The ACPR states that the design of algorithms should require particular attention from supervised entities and supervisors (while respecting the already existing principles and objectives of governance and internal control).

As with the GDPR principle “privacy by design”, the purpose of the regulation should be integrated from the first steps in the design of the artificial intelligence tool, to accurately identify and take into account each of the objectives set by internal policy in accordance with the applicable regulation (be it prudential, customer protection or other domains).

Moreover, the ACPR task force, as well as the questioned market players, emphasises the need for an industry specific code of conduct/ethics (for the banking- and insurance sector) although the timing of the introduction of this code should not be premature (so it cannot obstruct the development of artificial intelligence in the sector).

2. [Ensure the reliability of algorithms and achieving their objectives](#) (p. 20-21)

The ACPR also notes that the reliability of artificial intelligence algorithms is of importance.

They express that the focus should be on data quality requirements (as already foreseen by several sectoral regulations), e.g. minimal use of public external data, using external data from sources considered reliable, regular checks on data quality, regular update of the customer’s personal data, ... The reliability can be derived from the verification that the data use is appropriate for the determined purposes and does not result in biased decisions. Several approaches are highlighted by the ACPR based on the input from industry actors:

- Expert validation of the variables used (and the relevance thereof), so that unnecessary variables and sources of biases can be eliminated.
- The use of a safe and traditional parallel process on part of the test data.
- Test the algorithms by using a standard dataset to monitor the relevance and non-discriminatory aspects of the algorithms.
- The development of tools to monitor the “conceptual drift” and to control the risk of automatic learning.
- The performance of tests on datasets independent from those used for algorithm learning (methodology to be defined), to test the performance of the artificial intelligence algorithm on a given date (independent from the version “historisation”).

In general the ACPR expects that firms can explain (i) the mechanisms and criteria followed by the algorithm during the analysis process and (ii) for any given action/decision, the objective criteria and elements that determined the action in question (instead of an alternative action)

3. [Possible concentration or fragmentation phenomena](#) (p. 23-24)

Supervisors should revise their supervisory methods and take the dependency between different market players into account and must review their current methodologies for addressing systemic risks (because certain risks might transfer to technology providers).

The ACPR insists that supervisors should take the impact of artificial intelligence on the nature or size of financial institutions, their interactions with technology providers and the possible displacement of risks between different actors into consideration.

The ACPR refers for example to the current outsourcing rules and questions the effectiveness of the aforementioned rules when it comes to the interaction with major technology providers (who could potentially be more powerful than the financial institution, turning the classic power balance between the financial institution and a subcontractor around).

4. [Consider mutualisations](#) (p. 22-24)

Since the development of artificial intelligence is costly, the ACPR suggest to consider mutualisations.

Supervisors can analyse on the one hand standardisation and mutualisation opportunities for processes for the common good, and on the other hand individual risk management rules (to be defined/applied per market player).

- **In 2020**

In the abovementioned [discussion paper of 2020](#) (p. 5-6) the ACPR also published an approach to govern the issues of explainability and governance of AI.⁷³ The ACPR formulated its recommendations by using three topics: (i) Anti-money laundering and combatting the financing of terrorism, (ii) internal models in banking and insurance, (iii) Customer protection (which particularly focused on non-life insurance product sales and the corresponding duties to properly inform the customer and offering a non-life insurance product consistent with the expressed customer's needs and requirements).

A. How to evaluate an artificial intelligence tool/algorithm according to the ACPR?

The below [4 principles](#) should be used (p. 7-18):

1) Data management (during each stage of the design/implementation process)

All data processing should be thoroughly [documented](#) (p. 10). This documentation enables risk assessments related to regulatory compliance and ethics and the implementation of tools for detecting and mitigating undesired biases.

Regarding regulatory compliance the ACPR states that:

- The compliance with the GDPR can be assessed by “well-proven methods”: undesired biases can be detected, prevented or suppressed (in any stage of the design/implementation process) dependency on sensitive variables can be suppressed, etc (the ACPR does not offer more details).
- The compliance with sector specific requirements, such as the requirement to offer insurance prospects, products that are consistent with their demands and needs and the obligation for insurance distributors to “always act honestly, fairly and professionally in accordance with the best interests of their customers” (and not driven by/based on sales maximisation/the customer's capacity to pay/subscribe), calls for suitable explanatory methods (see below).⁷⁴
- The concerns related to ethics and fairness should be [tackled](#) (p. 7-10) as follows:
 - i. Define what is a problematic bias
 - ii. Determine to what extent biases present in the data are reflected (if not reinforced) by AI algorithms
 - iii. Mitigate biases whenever possible (on data/algorithm level)

2) Performance

⁷³ See also: ACPR, Governance of artificial intelligence in finance (Summary of consultation responses), 2020, https://acpr.banque-france.fr/sites/default/files/medias/documents/summary_-_ai_governance_in_finance_-_def.pdf.

⁷⁴ The ACPR acknowledges that a human can better evaluate the customer's needs than an algorithm.

[Performance metrics](#) (p. 10) have to be carefully selected, so as to evaluate the technical efficacy of the algorithm or alternatively its business objectives. The trade-off between the algorithm's simplicity and its efficacy has to be taken into account.

3) Stability

Potential [instability sources](#) (p. 12) which may affect AI algorithms should be identified, the associated risks (including compliance risks) should be assessed and detection and mitigation methods should be implemented (e.g. temporal drift, generalisation, re-training, ...).

4) Explainability

For each AI case, the firms must determine/describe:

- i. The impacted business processes and the roles filled.
- ii. The types of recipients targeted by an explanation
- iii. Nature of the associated risks

All stakeholders in the algorithms' governance must agree with the (above) level and form of an appropriate explanation for the AI algorithm.

According to the ACPR the firm must be able to answer the following questions:

- What are the causes of a given decision or precision?
- What inherent uncertainty does the model carry?
- Are the errors made by the algorithm similar to those due to human judgment?
- Beyond the model's prediction, what other pieces of information are useful (for example to assist a human operator in making the final call)?

The explanation should be: accurate, comprehensive, comprehensible, concise, actionable, robust and reusable. However, the ACPR acknowledges that this must be balanced against other principles (such as performance) dependent on the specific case at hand.

The ACPR suggest the following methods:

- Level 1: Observation (empirically and analytically) to answer the questions: "How does the algorithm work?" and "What is the algorithm's purpose"?
- Level 2: Justification to answer the question: "Why does the algorithm produce such a result?"
- Level 3: Approximation (by using explanatory methods which operate on the model being analysed, via a structural analysis of the algorithm, the resulting model and the data used) to answer the question "How does the algorithm work?" (in addition to level 1 – 2 methods)
- Level 4: Replication (by detailed analysis of the algorithm, model and data being a line-by-line review of the source code, a comprehensive analysis of all datasets used and an examination of the model and its parameters) to answer the question: "How to prove that the algorithm works correctly?" (in addition to level 1 – 3 methods)

The firm must choose the explanation level depending on the type of AI algorithm, the intended recipients of the explanation and the risks associated with the considered process. Consequently, the same algorithm might require a lower or higher explanation level dependent on the circumstances.⁷⁵

⁷⁵ See for a table illustrating the explanation levels, ACPR, Governance of Artificial Intelligence in Finance (Discussion document), 2020, p. 18.

To evaluate the AI algorithms the firm must list at each stage of the lifecycle, which design and development principles (data management, performance, stability, explainability) apply in particular, and which evaluation method is appropriate for that stage (see below, e.g. performance monitoring, fairness monitoring, explanations evaluation, training, model tuning, benchmark dataset, ...).⁷⁶

B. How to govern AI algorithms?

Incorporating AI into business processes has an impact on governance. The ACPR considers that the governance of AI algorithms requires careful consideration for the validation of each of the decision-making processes of AI algorithms. The ACPR formulates the [following governance concerns](#) (p. 21-35) that must be taken into consideration (as soon as possible when designing an AI algorithm/tool):

1) Integration of AI into traditional business processes

When integrating AI into (traditional) business processes, [firms](#) must (p. 3, 21-24):

- Cover the entire algorithm lifecycle and select a proper engineering method (e.g. dependent on the purpose of the AI algorithm).
- Ensure the full traceability of the AI design and engineering process (the engineering process should follow a well-defined methodology in terms of reproducibility, quality assurance, architectural design, auditability and automation).
- Take into consideration the end users, the purpose and the risks.
- Ensure that human interactions with the AI tool (if any) are well-defined, remain independent from the machine and are governed by rules documented in internal control procedures because human responsibility becomes engaged (to avoid undesired liability issues) and because the algorithm may modify human behaviour and judgment.

2) Impact of this integration on internal controls

The risks related to AI should be carefully identified and mapped. Internal control procedures of AI algorithms should involve both technical specialists and domain experts. The [monitoring](#) of algorithms requires initial technical validation of the components involved (this process must be re-examined on a recurrent basis), their continuous monitoring and adequate management of compliance risks generated or reinforced by AI algorithms (p. 3, 24-28).

3) Relevance of outsourcing the design or maintenance phases

The decision whether to outsource the design, implementation, hosting or operations of an AI system, or to use third-party products or services, must be preceded by an ex-ante risk analysis and take into account its results, especially with regard to reversibility.

Firms must ensure:

- (i) the proper documentation of deliverables
- (ii) the traceability of the process (for auditing purposes);
- (iii) access (technical, practical, legal, ...) to (the source code of) the AI model, to themselves and the supervisor (audit missions).

⁷⁶ See for an illustrating scheme, ACPR, Governance of Artificial Intelligence in Finance (Discussion document), 2020, p. 19.

4) Internal and external audit functions

It remains important that an AI tool can be audited, already in the design phase. The audit process will vary according to the algorithm's end users, the type of algorithm, the application scenario and to the circumstances/risks of the validation process itself.

The [ACPR](#) mentions two types of audits (p. 31-35):

- 1) Analytical evaluation: for example assess as a first step whether the organisation has assigned the correct level of explainability to the tool. Other analytical techniques are the review of information sheets describing the algorithm, the model and the data used or the analysis of the code and data themselves.
- 2) Empirical evaluation: when dealing with a "black box" algorithm, the auditor will observe the output/behaviour of the AI tool based on the input. Several methods are possible.

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

/

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Establishment of a multidisciplinary Fintech Innovation Unit: efficiency and budgetary aspects

A. Which purposes were identified/established?

The [ACPR](#) (p. 3) established this multidisciplinary [task force](#) to respond to the growing deployment of artificial intelligence algorithms and to cover the potential systemic impacts and other impacts on the financial sector (e.g. consumer protection). The goals of the task force were/are amongst other things (i) summarising the implications of using AI in the financial sector (with particular focus on the regulatory implications) and (ii) conduct exploratory works to produce guidelines for the financial sector.

B. How do the measures try to achieve their purpose?

The task force/innovation unit has done a variety of research via public consultations and exploratory works by which they have worked with industry players to assess/question real AI algorithms to formulate their industry-specific guidelines.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The measure achieves its purpose, as demonstrated by the documents discussed under point 3.1 (Discussion paper of December 2018 and the Discussion document on the governance of artificial intelligence of June 2020).

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (if applicable)

Yes (see Part1 Ch5 5.1.3. and 5.1.4.). In Belgium, the concrete implications of new business models and the regulatory gaps are also not clear yet. Therefore, setting up a hub/innovation unit could be useful.

3.2.2. Proposal 2 – Definition of appropriate governance of algorithms: efficiency and budgetary aspects

A. Which purposes were identified/established?

To ensure compliance with a variety of laws and regulations (incl. insurance law, consumer protection law, GDPR, ...).

B. How do the measures try to achieve their purpose?

In 2018 the ACPR has generally formulated that a governance framework is of importance for AI algorithms, while also referring to the need for an industry specific code of conduct/ethics and the need to take the purpose of the applicable regulations into consideration from the start of the design of an artificial intelligence tool.

In 2020 the ACP formulated additional high-level guidance in this respect:

- Adjust (operational) procedures and implement procedures.
- Segregate duties between different business units (four-eyes principle).
- Perform risk mapping.
- Initial technical validation, continuous monitoring and adequate management of compliance risks.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The ACPR has quite generally listed the (classical) control/governance principles that insurance actors should take into consideration from the beginning of their “AI projects”. It remains to be seen if this will suffice to ensure compliance (given the lack of details and defined supervision measures). A code of conduct/ethics might provide more details but has not been developed by the ACPR.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 4.2.1., 4.3.2., 5.1.1., 5.1.3., 5.2.2., 6.1.). A predefined governance framework could prevent undesired breaches of rules/regulations on a systematic basis.

3.2.3. Proposal 3 - Data quality requirements and verification of data use: efficiency and budgetary aspects

A. Which purposes were identified/established?

If compliance of AI tools/algorithms is ensured, the second obstacle is the **reliability** of AI tools/algorithms. Proposal 3 aims to ensure this reliability.

B. How do the measures try to achieve their purpose?

The use of artificial intelligence relies on the use of a large volume of data from diverse sources. By ensuring the quality of the data, the reliability of the AI tool increases (bad quality data could result in the faulty functioning of the AI tool/algorithm, and in – unforeseen – breaches of the law). To ensure this the ACPR proposes an additional layer of verification (different methods are proposed).

C. Where possible to assess, to what extent did these measures achieve their purpose?

The ACPR has not yet defined a mandatory set of data quality or verification requirements specifically for the use of AI tools, but has made some suggestions (expert validation, algorithm tests using a standard dataset, ...). [The sector](#) does not seem to dispute the proposed measures.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 2.2.1.). Predefined data quality and verification requirements could ensure that Belgian insurance companies (i) take data quality into account from the start and (ii) monitor that the data quality remains intact.

3.2.4. Proposal 4 – Explainability requirements and methods: efficiency and budgetary aspects

A. Which purposes were identified/established?

To remediate the lack of explainability of decisions or actions taken by AI tools/algorithms.

Amongst other things, the explainability requirements aim to ensure compliance with the requirement to explain to the customers that the offered insurance product is consistent with their demands and needs and the obligation for insurance distributors to “always act honestly, fairly and professionally in accordance with the best interests of their customers”. Generally, the aim is to ensure compliance with sector specific requirements.

B. How do the measures try to achieve their purpose?

In 2018 the ACPR already expressed the expectation that firms should be able to explain the mechanism, criteria and any given action/decision (and the objective criteria/elements on which the action/decision was based), ... of the AI tool/algorithm.

In 2020 the ACPR complemented this with formulating a method to ensure this explainability (as described in chapter 3.1) using a multi-level approach, with different requirements based on the context, explanation recipients and associated risks. The level must be set with approval of all stakeholders.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The use of AI is still growing, therefore it cannot be assessed yet whether the proposal will achieve the desired result. However, [the sector](#) (p. 1-2) reacted positively to the approach which already offers a great level of detail, but may need to be finetuned based on the industry input. Moreover, the proposal was formulated based on exploratory works in cooperation with some industry players, which suggests that the first tests achieved the desired result.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 2.2.2., 4.3.2., 5.1.3., 5.2.2., 6.1.). A predefined explainability method based on the context, explanation recipients and associated risks could ensure that Belgian insurance companies (i) systematically think about the explainability concerns related to AI tools/techniques and (ii) create a way to properly explain the outcome of the AI tool/algorithm.

3.2.5. Proposal 5 – Outsourcing requirements, including an ex-ante risk assessment: efficiency and budgetary aspects

A. Which purposes were identified/established?

The aim is to avoid concentration, fragmentation, systemic and “black box” risks, e.g. because of the outsourcing to a selected number of major technological companies. This is also the reason why the ACPR questions the effectiveness of the existing outsourcing rules.

B. How do the measures try to achieve their purpose?

In 2020 the ACPR stated that the decision to outsource or to use third-party products/services for any task related to an AI tool/algorithm must be preceded by an ex-ante risk analysis. Moreover, everything must be well-documented and access and traceability must be guaranteed.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The use of AI is still growing, therefore it cannot be assessed whether the proposal will achieve the desired result. However [the sector](#) (p. 4) confirmed the concerns expressed by the ACPR. Moreover, the proposal was formulated based on exploratory works in cooperation with some industry players, which suggests that the first tests achieved the desired result.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 2.2.6., 4.2.1., 5.1.3.). An ex-ante risk analysis and documentation requirements could also ensure access, traceability and compliance for Belgian insurance companies.

3.2.6. Proposal 6 – Mutualisation and standardisation: efficiency and budgetary aspects

A. Which purposes were identified/established?

The aim is to avoid that some actors fall behind in comparison to others (this issue has mainly been raised in the context of anti-money laundering and combatting the financing of terrorism).

B. How do the measures try to achieve their purpose?

By formulating common standardisation and mutualisation of processes for the common good.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Not all [market participants](#) respond positively to mutualisation (p. 7). In any case, the idea has not developed further, so the extent to which this measure achieves its purpose is unclear.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes. Developing common processes for the entire Belgian market could prevent that some actors fall behind.

3.2.7. Proposal 7 – Risk assessment methodologies: efficiency and budgetary aspects

A. Which purposes were identified/established?

The aim is that the firms know to which risks (e.g. regulatory risks/non-compliance) they are exposed so that they can take the proper mitigating measures.

B. How do the measures try to achieve their purpose?

The ACPR reiterates the need for **documentation** and **corresponding risk assessments** on multiple occasions, i.e. related to the **4 principles** mentioned by the ACPR for evaluating an AI tool/algorithm: data management, performance, stability and explainability.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The proposal guides the market participants in evaluating their AI tools/algorithms based on 4 principles. The use of AI is still growing, therefore it cannot be assessed whether the proposal will achieve the desired result. However, the sector does not seem to oppose the ACPR's proposal. Moreover, the proposal was formulated based on exploratory works in cooperation with some industry players, which suggests that the first tests achieved the desired result.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 2.2.1., 2.2.2., 5.1.3.). Evaluating AI tools/algorithms using a predefined method can expose the risks related to the use of an AI tool/technique and could prevent undesired breaches of rules/regulations on a systematic/periodic basis.

3.2.8. Proposal 8 – Govern human intervention: efficiency and budgetary aspects

A. Which purposes were identified/established?

The ACPR sets out guidance for the integration of AI into (traditional) business processes. Specific attention should be given to end users but also to human interactions with the AI tool (if any).

Human interaction can also have undesired consequences, as it introduces a new kind of risks, namely potential liability (when contradicting the decision taken by the AI tool/algorithm), independence concerns (to avoid liability) and the introduction of bias (when the explanation is not connected to the underlying factors which led to the output), lack of transparency for the algorithm,....

B. How do the measures try to achieve their purpose?

For now, the ACPR has only formulated the above recommendations in the context of integrating AI into traditional business processes.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The use of AI is still growing, therefore it cannot be assessed whether the proposal will achieve the desired result. However, [the sector](#) (p. 3) does not seem to fully oppose the ACPR's proposal (but has formulated some concerns). Moreover, the proposal was formulated based on exploratory works in cooperation with some industry players, which suggests that the first tests achieved the desired result.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 2.2.4., 4.3.2., 5.1.1., 5.1.3., 5.2.2., 6.1.). Designing a (risk-based) policy on how humans interact with an AI tool/algorithm can prevent undesired consequences (i.e. liability) of such human interventions.

3.2.9. Proposal 9 – Audit methodologies: efficiency and budgetary aspects

A. Which purposes were identified/established?

The ACPR has formulated a variety of requirements and measures to monitor/audit the AI tool/algorithm throughout its lifecycle (using the 4 principles and specific evaluation methods).

The purpose is to avoid breaches of rules/regulations (defined by the law and by internal policies and procedures based on the ACPR's guidance).

B. How do the measures try to achieve their purpose?

The ACPR has provided some methodologies and formulated its expectations.

C. Where possible to assess, to what extent did these measures achieve their purpose?

The proposal guides the market participants in monitoring/auditing their AI tools/algorithms. The use of AI is still growing, therefore it cannot be assessed whether the proposal will achieve the desired result. However, [the sector](#) (p. 4) does not seem to fully oppose the ACPR's proposal (but has formulated some remarks/feedback). Moreover, the proposal was formulated based on exploratory works in cooperation with some industry players, which suggests that the first tests achieved the desired result.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes (see Part1 Ch5 5.1.3.). Requiring insurance companies to regularly check their algorithms and datasets could help to avoid unintentional breaches of rules/regulations.

Questionnaire the United Kingdom

1. Which authorities are competent for insurances?

The competent authority for the conduct supervision of the insurance sector in the United Kingdom is the Financial Conduct Authority (FCA). The competent authority for the prudential supervision of the insurance sector in the United Kingdom is the Bank of England.

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

The FCA has published a variety of documents related to digitalisation, mostly between 2015 and 2020.

In 2015, the FCA launched a [Call](#) for inputs on Big Data in retail general insurance to gain a better understanding of the issues. The [feedback statement](#), including the results of the call for inputs and the next steps to be taken, was published in 2016.

In 2016, the FCA published an [occasional paper](#) relating to the access to financial services in the UK. With this paper, the FCA wants to bring together a range of issues for debate for the regulator and other stakeholders to consider.

In 2018, the FCA launched a [public debate](#) on the fairness of certain pricing practices in financial services. It also published a [framework](#) on how to approach this. As this is a complex issue, the FCA wanted to take into account stakeholder views on its approach. In 2019, the FCA published a [feedback statement](#), including a summary of the responses and the next steps to be taken. In

September 2020 the [final report](#) of a market study on general insurance pricing practices was published and a [consultation on Handbook changes](#) has been launched.

In 2019, the FCA and the Bank of England cooperated on a [joint project](#) to produce a snapshot of the application of AI and ML in UK financial services, which resulted in a report. Building on this, the Bank and the FCA established a Public-Private Forum to facilitate the dialogue, as well as to explore whether principles, guidance, regulation and/or industry good practice could support safe adoption of AI/ML.

In 2019, the UK Government also published a [Snapshot Paper](#) concerning AI and Personal Insurance. This paper examines the potential use cases of AI across the insurance industry and looks in particular at the ethical concerns associated with hyper personalised risk assessments. It finishes by setting out several proposals for how AI could be used more responsibly by insurers.

In 2019, the Chartered Insurance Institute, a professional body dedicated to building public trust in the insurance and financial planning profession, also adapted its [ethics code](#) to the digital context.

The documents published by the FCA are available on the [website](#) of FCA. The documents published by the Bank of England are available on the [website](#).

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

The UK Government [states](#) (p. 6) that while there has been an increase in AI-led innovation in recent years, both among incumbents and new market entrants, it is important to not overstate the changes witnessed to date. A closer look at the industry shows there to be multiple barriers to the adoption of AI. Incumbent insurers often struggle to implement new computer infrastructure. Innovation is also made complicated by the number of players in the insurance value chain, including price comparison websites, brokers and reinsurers, each of which have their own operation systems that are difficult to align. At a more basic level, insurers find it difficult to attract staff with the necessary technical skills. Nevertheless, the industry is seeing meaningful experimentation with AI, and it may only be a matter of time before the pilots that are underway today are turned into fully established products.

The UK Government stresses the fact that the use of AI could be beneficial to insurance companies as well as for consumers. However, at the same time concerns are raised. In what follows, these concerns are listed together with the proposals formulated by the competent authorities to deal with those concerns.

1. Transparency

In order to ensure transparency, the UK Government proposes to [make privacy notes more available and to set up data discrimination audits and industry-wide registers for third party suppliers](#) (p. 3).

1.1 Undertake data discrimination audits

The UK Government proposes that insurers should [audit their algorithms and training datasets](#) (p. 13) as a matter of course to check for unwarranted bias – before, during and after their deployment.⁷⁷

The Chartered Insurance Institute, in its Digital Ethics Code, requires insurance companies to carefully manage data and analytics so as to ensure that nothing discriminatory is allowed to influence the outcomes that consumers experience. They add that it is also important to [ensure the fair and equal treatment of consumers on a group basis](#). Insurance companies should understand how their decisions influence not just the individual, but groups of people sharing similar characteristics.

1.2 Review third party data and software suppliers

The UK government proposes that the ABI (Association of British Insurers) or FCA could assist due diligence checks by [maintaining an industry-wide register](#) (p. 13) that documents complaints and instances of poor standards among data sellers and brokers.

The Chartered Insurance Institute, in its Digital Ethics Code, requires insurance companies to make sure that, when working together with internal and external partners, [responsibilities for delivering the right outcomes are clearly understood](#).

1.3 Make privacy notices more accessible

The UK Government proposes that in partnership with user experience designers, insurers could [produce 'key facts' data statements](#) (p. 13) that convey in straightforward terms how they use customer data and how customers can seek redress. Insurers should also [establish dedicated teams](#) (p. 13) to answer customer queries about their data rights.

The Chartered Insurance Institute, in its Digital Ethics Code, requires insurance companies to [make sure that their services are suitable for each client, transparent in their delivery and meet the expectations](#).

2. Reconsider the types of data that should not be used in risk assessments

The UK Government states that it will [reconsider the types of data that should not be used in risk assessments](#) (p. 12). Lessons can be learned from the Code on Genetic Testing and insurance.

3. Innovation Hub

FCA created an [Innovation Hub](#) (p. 56) to support innovator businesses to understand the regulatory framework and apply for authorisation, as well as identifying ways to adapt the regulatory framework to allow further innovation.

4. Regulatory Sandbox

The FCA also created a [Regulatory Sandbox](#) (p. 56).

5. Government intervention to avoid uninsurability

According to the [UK Government](#) (p. 10), commercial insurers are not obliged to insure riskier prospects. If some people become uneconomical to insure, a wider debate is needed on whether the government should be called on to intervene, and if so, on what terms. One proposal is to [financially incentivize insurers to cover individuals they would otherwise choose not to](#) (p. 12).

This consideration has also led to the creation of the [Flood Re scheme](#) (p. 103) to ensure access to home insurance for people living in flood-prone areas.

⁷⁷ This is also recommended by Insurance Europe, see response consultation draft guidelines trustworthy AI, 2019.

Moreover, the ABI closed an agreement on [a moratorium on the use of predictive genetic testing](#).

6. Data storage standards

The UK Government advises the industry to [draw up data storage standards](#) (p. 9), that discourages insurers from storing data that is not central to their mission. Such standards could include an expectation for insurers to review their datasets on a regular basis to determine whether they are material to their core business practice, and if not eliminate them from company records.

7. Establish clear lines of accountability

Insurers should consider whether they need to [allocate individual board members responsible for overseeing uses of AI](#) and other forms of data-driven technology (p. 14).

8. Fair pricing framework

The FCA established a [fair pricing framework](#) to help assess concerns about fairness in price discrimination in financial services.⁷⁸

9. Signposting service

ABI and BIBA (British Insurance Brokers' Association) have agreed a non-statutory agreement with the Government which includes [signposting for older people struggling to find motor and travel insurance](#) (p. 102-103). Under the agreement, when an older person is turned down for motor or travel insurance because of their age, the insurer or broker concerned must refer the person to another service that can provide cover or to a suitable signposting service. This agreement also requires the ABI to publish annually data on how age affects risk and premiums.

10. Require firms to offer a renewal price that is no higher than the equivalent new business price for the costumer through the same sales channel

The FCA [proposes](#) (p. 7) to require firms to offer a renewal price that is no higher than the equivalent new business price for the costumer through the same sales channel. This way, the renewal price is tied to the equivalent new business price. This proposed remedy would apply to retail home and motor insurance products.

11. Legal basis for the processing of health data in private health insurance

The UK Government inserted a specific provision for the processing of health data in the context of insurance in the Data Protection Act 2018:

“20(1) This condition is met if the processing—

(a) is necessary for an insurance purpose,

(b) is of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health, and

(c) is necessary for reasons of substantial public interest, subject to sub-paragraphs (2) and (3).

(2) Sub-paragraph (3) applies where—

(a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject, and

(b) the data subject does not have and is not expected to acquire—

⁷⁸ Also see: FCA, General insurance pricing practices. Final Report, Market Study MS18/1.3, September 2020 (Updated December 2020), 32 p. <https://www.fca.org.uk/news/press-releases/fca-sets-out-proposals-tackle-concerns-about-general-insurance-pricing> and <https://www.fca.org.uk/publication/consultation/cp20-19.pdf>.

(i) rights against, or obligations in relation to, a person who is an insured person under an insurance contract to which the insurance purpose mentioned in sub-paragraph (1)(a) relates, or

(ii) other rights or obligations in connection with such a contract.

(3) Where this sub-paragraph applies, the processing does not meet the condition in sub-paragraph (1) unless, in addition to meeting the requirements in that sub-paragraph, it can reasonably be carried out without the consent of the data subject.

(4) For the purposes of sub-paragraph (3), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph—

- “insurance contract” means a contract of general insurance or long-term insurance;
- “insurance purpose” means—

(a) advising on, arranging, underwriting or administering an insurance contract,

(b) administering a claim under an insurance contract, or

(c) exercising a right, or complying with an obligation, arising in connection with an insurance contract, including a right or obligation arising under an enactment or rule of law.

(6) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.

(7) Terms used in the definition of “insurance contract” in sub-paragraph (5) and also in an order made under section 22 of the Financial Services and Markets Act 2000 (regulated activities) have the same meaning in that definition as they have in that order.”

The parliamentary [documents](#) explicitly refer to article 9, 2 G) GDPR as legal basis (nr. 621). So far, there is no specific provision in UK law allowing automated individual decision-making by insurance companies.⁷⁹

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

N/A.

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Undertake data discrimination audits: efficiency and budgetary aspects

A. Which purposes were identified/established?

Insurers are already prohibited by law from discriminating against costumers on the basis of certain characteristics. However, the FCA fears that insurance companies are at [risk of indirectly discriminating via proxy variables](#) (p. 13).

B. How do the measures try to achieve their purpose?

By requiring insurance companies to audit their algorithms and data training sets on a regular basis, the FCA wants to avoid unintentional bias and discrimination.

⁷⁹ Article 22 GDPR is implemented in Section 14 UK Data Protection Act 2018.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, we have no evidence that this measure has already been implemented.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium as well, insurance companies are prohibited from pricing based on certain by law protected criteria (unless objectively justified). However, AI could lead to the application of other criteria that are not protected by law. Moreover, the use of those factors could even lead to proxy discrimination. In addition, the general rule on prohibiting any segmentation unless objectively justified is limited to only certain specific consumer insurance contracts (see Part1 Ch5 5.2.2). Requiring insurance companies to regularly check their algorithms and data sets could help to avoid unintentional (proxy) discrimination.

3.2.2. Proposal 2 – Review third party data and software suppliers: efficiency and budgetary aspects

A. Which purposes were identified/established

Insurers might have legitimate reasons to purchase data from third party providers. The UK Government wants to [ensure that insurance companies get assurances from third party suppliers](#) (p. 13) that the information they are being given is accurate, unbiased and collected with the knowledge of the data subject.

B. How do the measures try to achieve their purpose?

By maintaining an industry-wide register that documents complaints and instances of poor standards among data sellers and brokers, the ABI and FCA can assist insurance companies with due diligence checks.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, we are not aware this register has already been set up by the ABI and/or FCA.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

Belgian insurance companies also might have incentives to work with third party suppliers (e.g. tech companies). This raises a number of potential risks (see Part 1 Ch5 2.2.6). It might therefore be useful to create this kind of register to assist insurance companies.

3.2.3. Proposal 3 – Make privacy notices more accessible: efficiency and budgetary aspects

A. Which purposes were identified/established?

The UK Government wants to avoid privacy notices that are lengthy, opaque and confusing.

B. How do the measures try to achieve their purpose?

'Key facts' data statements and straightforward terms could help customers to understand better what their data is being used for and how they can seek effective redress. Establishing teams that are trained to answer queries could also be helpful for consumers to understand their rights, especially if they are not educated to read and understand lengthy privacy statements.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, the UK Government has not implemented specific measures to improve transparency.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

The problem of information overload and privacy statements that are difficult to understand for consumers also exists in the Belgian context (see Part 1 Ch5 2.2.2).

3.2.4. Proposal 4 – Reconsider the types of data that should not be used in risk assessments: efficiency and budgetary aspects

A. Which purposes were identified/established?

The [UK Government](#) (p. 12) fears hyper personalised risk assessments and exclusions caused by the expansive collection of customer data.

B. How do the measures try to achieve their purpose?

By forbidding insurance companies to use some types of data in their risk assessments, the UK Government wants to avoid potential policyholders getting excluded from insurance or having to pay a higher premium.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, the UK Government has not implemented such a measure.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

Also in Belgium, the fear for hyper personalised risk assessments caused by the growing amount of data available to insurance companies rises (see Part1 Ch5 2.2.8). In Belgium, the use of certain data for pricing is already prohibited, or regulated. However, it might be necessary to reassess this rules in the light of new developments (see Part1 Ch5 6.2).

3.2.5. Proposal 5 – Innovation Hub: efficiency and budgetary aspects: efficiency and budgetary aspects

A. Which purposes were identified/established?

The FCA wants to [support innovator businesses](#) (p. 56) to understand the regulatory framework and apply for authorisation, as well as identifying ways to adapt the regulatory framework to allow further innovation.

B. How do the measures try to achieve their purpose?

The innovation hub offers the following services:

- a dedicated team and contact for innovator businesses
- help for these businesses to understand the regulatory framework and how it applies to them
- assistance in preparing and making an application for authorisation, to ensure the business understands our regulatory regime and what it means for them
- a dedicated contact for up to a year after an innovator business is authorised

The Innovation Hub will identify areas where the regulatory framework needs to adapt to enable further innovation in the interests of consumers.

Through international engagement the Innovation Hub supports the FCA's competition objective by promoting the UK as a centre for innovation in financial services. It does this by:

- Facilitating the entry of innovative overseas firms to the UK, thereby increasing innovation and competition in UK financial services markets.
- Facilitating the expansion of UK-based innovative firms into overseas markets, making them potentially more sustainable challengers in the UK.

The FCA signed co-operation agreements and frameworks with overseas regulators in order to support the above.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

No information available.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No information available.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

Yes.

In Belgium, the concrete implications of new business models and the regulatory gaps are also not clear yet. Therefore, setting up an innovation hub could be useful.

3.2.6. Proposal 6 – Regulatory sandbox: efficiency and budgetary aspects

A. *Which purposes were identified/established?*

The FCA wants to provide a 'safe space' for businesses to [test innovation in products and services, business models and delivery systems](#) (p. 56).

B. *How do the measures try to achieve their purpose?*

The sandbox seeks to provide firms with:

- The ability to test products and services in a controlled environment.
- Reduced time-to-market at potentially lower cost.
- Support in identifying appropriate consumer protection safeguards to build into new products and services.
- Better access to finance.

The FCA oversees the development and implementation of tests, for example by working with firms to agree bespoke consumer safeguards.

Sandbox tests are expected to have a clear objective (e.g. reducing costs to consumers) and to be conducted on a small scale. Firms will test their innovation for limited duration with a limited number of customers.

The regulatory sandbox provides access to regulatory expertise and a set of tools to facilitate testing. The tools are not always needed and their value will depend on the nature of each business and their test.

C. *Where possible to assess, to what extent did these measures achieve their purpose?*

No information available.

D. *Where possible to assess, what impact did the measures have on the government budget?*

No information available.

E. *Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)*

Yes.

In Belgium, the concrete implications of new business models and the regulatory gaps are also not clear yet. Therefore, setting up a regulatory sandbox could be useful.

3.2.7. Proposal 7 – Government intervention to avoid uninsurability: efficiency and budgetary aspects

A. *Which purposes were identified/established?*

The UK Government wants to avoid uninsurability and exclusions of higher risks.

B. *How do the measures try to achieve their purpose?*

The [UK Government](#) proposes a wider debate on whether the government should be called on to intervene, and if so, on what terms (p. 10). One proposal is to [financially incentivize insurers to cover individuals they would otherwise choose not to](#) (p. 12).

By creating the [Flood Re scheme](#) (p. 91) the [UK Government](#) ensures access to home insurance for people living in flood-prone areas (p. 103). This Flood Re scheme is a not-for-profit flood reinsurance fund, owned and managed by the insurance industry, established to ensure that domestic properties in the UK at the highest risk of flooding can receive affordable cover for the flood element of their household property insurance. Under the scheme, insurers are able to reinsure (pass on the risk) of flood cover at a cost linked to the Council Tax band for each home concerned. Flood Re is financed by an industry-wide levy. Consumers in high-risk areas still buy insurance as normal but should find more insurers willing to provide cover. Insurers paying the levy are likely to pass on the cost of it by increasing the premiums they charge to all insured homeowners. In this way, every consumer in the wider insurance pool will cross-subsidise insured owners in flood-prone areas (p. 91).⁸⁰

The creation of a [moratorium on genetic testing](#) (p. 103) both protects some consumers from being refused cover and helps to ensure that the price of life and health insurances remains affordable. Under the agreement, predictive genetic test results will only be used at all for underwriting life cover greater than 500.000, critical illness cover over 300.000 or income protection insurance paying more than 30.000 a year, and only where an independent panel has agreed that the test should be disclosed if the insurer asks about it.⁸¹ On the flip side, consumers can voluntarily tell

⁸⁰ See about the Flood Re scheme <https://www.floodre.co.uk/faq/how-does-flood-re-work/>.

⁸¹ ABI, Code on Genetic Testing and Insurance, 2018.

insurers about favorable test results and the insurer might reflect that in the price and cover offered.⁸²

C. Where possible to assess, to what extent did these measures achieve their purpose?

Concerning [the moratorium on genetic testing](#) (p. 91): so far, only one predictive genetic test had been approved for disclosure (which is a predictive test for Huntington's Disease in the case of life cover above the 500.000 limit).

In its annual report of 2019, the [ABI](#) (p. 5-7) reports that 95% of life insurance policies fall within the financial limit of £500,000; 91% of income protection policies fall within the limit of £30,000 (per annum); and, 98% of critical illness policies and 94% of accelerated critical illness policies fall under the limit of £300,000. It therefore concludes that there is no indication in the compliance data of a current information asymmetry that might have an adverse effect on the provision of life insurance policies. The ABI continues to review the data annually and monitors advances in genetic testing.

D. Where possible to assess, what impact did the measures have on the government budget?

There is no information concerning the impact on the government budget. However, one can assume that the impact of the measures already in place (Flood Re scheme and moratorium on genetic testing), had no impact since the government did not intervene or subsidised the measures.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

In Belgium, there is already a legal ban on the communication and use of genetic information and testing and a mandatory coverage of natural disasters and a Tariferingsbureau Natuurrampen in household insurance (eenvoudige risico's) (see Part1 Ch5 4.3.1).

3.2.8. Proposal 8 – Data storage standards: efficiency and budgetary aspects

A. Which purposes were identified/established?

New sources of data – including telematics devices – may lead insurers to find more information than necessary to deliver their core services. Insurers might be tempted to store this data, perhaps in the expectation they will be able to put it to use in the future. Moreover, consumer data might be sold to third parties without reimbursement. The collection of more data may also increase the chance that algorithms pick up biases. The UK Government wants to limit these harms by discouraging insurers from storing data that is not central to their mission.

B. How do the measures try to achieve their purpose?

So far, we are not aware of data storage rules.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium as well, the concern is raised that traditional datasets will be increasingly combined

⁸² FCA, Access to Financial Services in the UK, Occasional Paper 17, 91. See about the Code on genetic testing and insurance <https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/health-insurance/genetics-and-insurance/>.

with new types of data (e.g. behavioural data) making the decision-making process biased (see Part 1 Ch5 2.2.1).

3.2.9. Proposal 9 – Establish clear lines of accountability: efficiency and budgetary aspects

A. Which purposes were identified/established?

The UK Government wants insurance companies to be able to name a dedicated staff member who had ownership over their pricing strategy. This way, it is easier to have someone accountable.

B. How do the measures try to achieve their purpose?

By requiring insurance companies to appoint individual board members responsible for overseeing uses of AI and other forms of data-driven technology, it is easier to have someone accountable. Moreover, this measure installs a point of contact for consumers or other stakeholders.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, we have no information of concrete measures being implemented by the UK Government.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium as well, it might be useful to have a point of contact and to have someone accountable when it comes to the use of AI by the firm.

3.2.10. Proposal 10 – Fair pricing framework: efficiency and budgetary aspects

A. Which purposes were identified/established?

The FCA aims at [ensuring fairness in discriminatory pricing](#) (p. 3) as issues of fairness in pricing are likely to become increasingly prevalent and complex in the future as insurers will use new technologies and data becomes more sophisticated.

B. How do the measures try to achieve their purpose?

The FCA already had [an established framework](#) for identifying and assessing distortions of competition and market efficiency. But what this framework was missing is a consideration of whether the outcomes price discrimination produces are fair. The FCA created a framework that they will use to assess fairness when considering cases of price discrimination in retail markets.

The [framework](#) (p. 6) consists of six key questions when weighing up distributive fairness concerns (= the fairness of some consumers paying more than others). Considerations that are taken into account are, e.g. who is harmed by the price discrimination, is the product/service essential, ... Any conclusions drawn from applying this framework in practice may differ from market to market as the specific circumstances vary. Ultimately, the [FCA](#) (p. 1-2) will always assess the pros and cons of price discrimination on a case by case basis.

Should it conclude that it is appropriate for the FCA to intervene, there is a range of measures at the FCA's disposal. Examples are price caps, constraints in the way certain types of data are collected or used, ... The principle of [proportionality](#) (p. 8-9) provides an important guide when we consider what remedy is most appropriate.⁸³

⁸³ For a more elaborate explanation read: FCA, Fair Pricing in Financial Services: summary of responses and next steps, 2019.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium as well, the risk of price discrimination arises, as AI could enhance insurance companies' understanding of consumer's individual price sensitivity (Part1 Ch5 2.2.3). This kind of framework might help supervisory authorities when assessing fairness in pricing strategies of insurance companies. Moreover, this framework is also useful for insurance companies when determining their pricing strategy.

3.2.11. Proposal 11 – Signposting service: efficiency and budgetary aspects

A. Which purposes were identified/established?

The agreement was made in the context of a specific exception to the Equality Act 2010 which allows age to continue to be used as a discriminating factor across the financial services sector. The [UK Government](#) wanted to protect older persons against getting turned down for motor or travel insurance because of their age (p. 102).

B. How do the measures try to achieve their purpose?

The [UK Government](#) found that non-standard costumers may be able to find cover if only they know where to look, although they will typically have to pay extra. Therefore, an important way to improve consumer's wellbeing is to signpost them to appropriate sources of cover or brokers who can help. Under the agreement, where an older person is turned down for motor or travel insurance because of their age, the insurer or broker concerned must refer the person to another source that can provide cover or to a suitable signposting service (p. 102).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

There is no information about the impact on the government budget available. However, one may assume that the impact on the government's budget is limited as the service is set up by BIBA.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

No. Unless mistaken, older persons do not have problems to obtain on the Belgian insurance market an affordable and suitable motor or travel insurance because of their age. All persons not being able to find an affordable motor liability insurance have recourse to the Tariffication Bureau.

3.2.12. Proposal 12 – Require firms to offer a renewal price that is no higher than the equivalent new business price for the costumer through the same sales channel: efficiency and budgetary aspects

A. Which purposes were identified/established?

The FCA's market analysis and feedback from stakeholders confirmed that some firms gradually increase the price to customers who renew with them year on year. This is called price walking.

When setting a price, most firms take account of the likelihood that a customer will switch supplier at their next renewal or in the future. Some firms also use practices that make it more difficult for consumers to make more informed decisions and raise barriers to switching. Therefore, the remedy aims to [prevent firms from price walking](#) (p. 5-7) customers by tenure.

B. How do the measures try to achieve their purpose?

The remedy ties the renewal price to the equivalent new business price. This way, firms would not be able to increase prices for renewal customers without also increasing the prices they offer the new business customers. In a competitive market, where customers shop around and switch provider, a firm that raises its prices for new business customers would lose market share. As a result, the FCA expects that this proposal will also tackle high prices for existing customers who have already been price walked.

In its [report](#), the FCA states that the remedy will help to achieve the aims by (p. 8):

- Preventing firms from increasing prices at renewal – and where they want to, this will need to be reflected in their new business prices which will make them less competitive.
- Reducing the costs to customers in having to search and switch to avoid paying higher renewal prices because of price walking.
- Reducing firms' marketing spend to attract highly profitable long term customers.
- Increasing competition, by making the new business price a better indication of the long-term cost of the policy.
- Helping to ensure firms compete to attract new customers by providing fair value at the outset and throughout a customer's relationship with them.
- Increasing price transparency and building consumer trust.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

The problem of price walking and, more in general, price discrimination is also apparent in Belgium (see Part1 Ch5 2.2.3)

3.2.13. Proposal 13 – Legal basis for the processing of health data in private health insurance: efficiency and budgetary aspects

A. Which purposes were identified/established?

No information available.

B. How do the measures try to achieve their purpose?

The UK Government created a specific legal ground allowing insurance companies to process sensitive personal data for certain purposes.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

The absence of a specific legal basis for the processing of health data in the context of insurance in Belgium causes legal uncertainty (see Part1 Ch5 2.2.2).

Questionnaire Germany

1. Which authorities are competent for insurances?

- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
- In 2018, the Federal Government established a Data Ethics Commission (Datenethikkommission). The task of this commission is to build on scientific and technical expertise in developing ethical guidelines for the protection of the individual, the preservation of social cohesion, and the safeguarding and promotion of prosperity in the information age.

2. Have the identified authorities published relevant policy documents related to AI in the last 10 years? If yes, where can these be found?

BaFin has published a variety of relevant documents concerning digitalisation, mostly between 2018 and 2020.

In its “[Big data meets artificial intelligence](#)” report of 2018, BaFin sets out the challenges and implications for the supervision and regulation of financial services. BaFin requested feedback from the industry on this report. The results from this consultation were [published](#) in 2019. The Deutsche Bundesbank, responsible for the financial supervision of banks, also reacted on the proposals of BaFin and added some [insights](#) specifically related to the banking sector.

In 2018, BaFin also published its [digitalisation strategy](#) in order to illustrate how it plans to respond to digitalisation. For each area of activity, BaFin defined overarching goals and describes a selection of next steps to achieve these goals.

In its supervisory priorities for 2020, BaFin defined a framework for action for supervised entities on the basis of five initiatives within the context of principle-based supervision. The objective is to provide greater legal certainty for the use of Big data and AI. In addition to the supervision of algorithms and automated processes, [BaFin](#) is taking a closer look at market analyses of Big data and AI, the significance of data in competition, the limits of financial supervision as new market participants and business models emerge and the use of big data and AI in the prevention of money laundering.

In addition, speeches of and interviews with the President of BaFin and expert articles were used to support the findings in some of the other documents.

The documents published by BaFin are available on the [website](#) of BaFin. The documents published by the Deutsche Bundesbank are available on the [website](#) of the Deutsche Bundesbank.

The proposals discussed below have been analysed from these documents, but have not been formulated as concrete proposals as such in these extensive texts.

In 2019, the Data Ethics Commission provided its opinion regarding data and algorithmic systems. The document can be found [here](#).

3. Discussion of documents

3.1. Have they formulated relevant proposals that respond to the identified issues/gaps in your work package?

3.1.1. If yes, briefly list these proposals

BaFin states that the use of AI in the insurance sector is still in its early stages. There is currently no evidence that AI technologies are widely used in the insurance market at the time of the study. In [Germany](#) a few insurance companies have already launched and implemented their first Big data and AI initiatives mainly in motor vehicle, household and health insurance (p. 94). According to [BaFin](#) (p. 94-95), there are two main challenges that have delayed market penetration of AI in the insurance sector. First, compared to other sectors, some insurance companies still lack both the expertise and experience in dealing with technologies. The recruitment and training of personnel represent key challenges for many insurance companies planning to implement AI applications. Second, the data household of insurance companies is often inadequate for the use of AI. AI can only be fully realised within an appropriate IT architecture. To achieve this, heavy investments are needed.

BaFin stresses the fact that the use of AI could be beneficial to insurance companies as well as for consumers. However, at the same time concerns are raised. In what follows, these concerns are listed together with the proposals formulated by BaFin to deal with those concerns.

1. Addressing providers that have not been regulated to date and making sure that the current legal framework is applicable to them; adapting outsourcing systems

In its supervisory priorities for 2020, BaFin commits to [take a closer look at the limits of financial supervision](#) (p. 10) as new market participants and business models emerge, as well as the significance of data in competition.

The respondents to the consultation of 2019 made concrete proposals to adapt outsourcing systems. One proposed option would be to use a type of [digital signature](#) (p. 20), especially for products that are created in a fragmented value creating process. Every company in the value creation process would have to be named when using such a signature. Another option to sustain value chains is the use of [smart contracts with a back-up party](#) (p. 20) that would take on any element within the value chain if a company cannot provide it. Other proposals are [minimum technical standards, targeted scenario analyses and volume limits](#) (p. 20).

2. Re-evaluate the concept of systemic importance

BaFin proposes to [re-evaluate the concept of systemic importance](#) (p. 169) and to assess whether the concept needs to be redefined in order to keep pace with new business models and market structures.

3. Test scenario to evaluate algorithms and no acceptance of black box models

In 2018, BaFin suggested to evaluate the results produced by an algorithm in [a test scenario](#) (p. 169) set by the supervisory authorities.

BaFin proposes that supervisory and regulatory authorities will [not accept any models presented as an unexplainable black box](#) (p. 169).

4. Traffic light system and public availability of data protection impact assessments

BaFin suggests to [simplify privacy policies](#) (p. 51) that are written in language geared towards the particular target group that would enable consumers to think through the consequences of providing data for that particular purpose. For example, transparency could be improved by

working with a traffic light system that highlights the risks inherent in data usage. Moreover, BaFin suggests that the [results of the data protection impact assessment](#) (article 35 GDPR) (p. 51) should also be made available to consumers in simplified form to give them a basis for making decisions on the provision of data.

5. Adequate monitoring and transparency mechanisms to tackle discrimination

BaFin states that algorithms must be programmed in such a way that legal particularities are adequately taken into consideration. As a result, firms must ensure that [adequate monitoring and transparency mechanisms](#) (p. 177) are in place to prevent their models from drawing such false or unauthorised conclusions.

6. Only use data that is actually relevant for risk assessment

According to BaFin, it must be guaranteed that algorithms used for assessing risks [only use and analyse the data that is actually relevant](#) (p. 126), i.e. the data that is directly related to the risk to be assessed. Some of the respondents of the questionnaire propose [to create binding definitions in order to determine what data is actually necessary for appropriate differentiation](#) (p. 35).

7. Responsibility

BaFin stresses that it is important that [responsibility for the results of AI-supported process is not shifted to machines](#) (p. 172) but remains with the senior management of the firm.

8. Provide alternative products

BaFin suggests for supervisory and regulatory authorities to ensure that [sufficient alternatives](#) (p. 179) in the form of “conventional financial” services and/or services that are “economical with personal data” continue to be offered in order to prevent consumers from being coerced virtually into releasing data. How exactly “conventional” and “economical with personal data” are to be defined in this context are matters to be discussed.

9. Hub-and-spoke

BaFin has [implemented](#) (p. 5) a hub-and-spoke concept to enable it to keep pace with digitalisation-driven market developments and to capture and assess financial technology innovations on a cross-sector basis.

10. Providing process and criteria to ensure data quality

BaFin states that [processes and criteria need to be provided that can guarantee appropriate data quality](#) (p. 53) for the respective use case. The specific criteria can vary depending on the respective use case. Typical criteria include completeness, consistency, validity and accuracy and/or timeliness.

11. Cooperation with financial supervisors and data protection authorities

BaFin proposes that [financial supervisors and data protection authorities should cooperate](#) (p. 179).

12. Creating a consumer-centred data portal

Germany's Advisory Council for Consumer affairs proposed to [create a consumer-centered data portal](#) (p. 52).

13. Utilising technical options for using Big data and AI with anonymised data

BaFin proposes to [use technical protection measures](#) (e.g. privacy-preserving data mining) (p. 15).

14. Specific legal basis for automated individual decision-making, including profiling, in the context of providing services pursuant to an insurance contract

In their [Federal Data Protection Act of 30 June 2017](#), the German government inserted section 37 which takes into account the specific interests of the insurance sector:

“Section 37: automated individual decision-making, including profiling

(1) In addition to the exceptions given in Article 22 (2) (a) and (c) of Regulation (EU) 2016/679, the right according to Article 22 (1) of Regulation (EU) 2016/679 not to be subject to a decision based solely on automated processing shall not apply if the decision is made in the context of providing services pursuant to an insurance contract and

1. the request of the data subject was fulfilled, or

2. the decision is based on the application of binding rules of remuneration for therapeutic treatment and the controller takes suitable measures, in the event that the request is not granted in full, to safeguard the data subject's legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision; the controller shall inform the data subject of these rights no later than the notification indicating that the data subject's request will not be granted in full.

(2) Decisions pursuant to subsection 1 may be based on the processing of health data as referred to in Article 4 no. 15 of Regulation (EU) 2016/679. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.”

According to [the Parliamentary documents](#), this article is based on Article 22, 2 (b) GDPR which allows Member States to create admissibility criteria for automated decisions in individual cases that go beyond those set out in Article 22, 2 (a) and (c) GDPR. The existence of a contractual relationship between the person affected by the automated decision and the controller is not a mandatory requirement for this article to be applicable. Rather, it is sufficient that the automated decision is made in the context of the provision of services under an insurance contract.⁸⁴

Following Paragraph 1 number 1, allows automated decisions for the provision of insurance services pursuant to an insurance contract if the request of the data subject receives a positive outcome.⁸⁵ The Parliamentary documents state that Paragraph 1 number 1 can be applied, for example, for the automated settlement of claims between the motor vehicle liability insurance of the liable party and the injured party. The prerequisite is that the request of the claimant, who is at the same time the data subject according to data protection law, is fulfilled.

Paragraph 1 number 2 allows for automated decisions on insurance benefits of private health insurance when applying binding rules of remuneration for therapeutic treatment.⁸⁶ Even if the request of the applicant as the person affected by the decision is not granted or not granted in full, the automated invoice verification by the private health insurance company is permissible if the person responsible takes appropriate measures to protect the legitimate interests of the person affected. This includes at least the right to human intervention, to express one's own point of view and to contest the decision. The measures listed correspond to the safeguards of Article 22, 3 GDPR. What is particularly innovative is the different approach on the basis of the outcome: automated decision-making practices must be provided with suitable measures only if the request

⁸⁴ Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Bundesrat Druksache 110/17, 107.

⁸⁵ G. MALGIERI, “Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations”, *Computer law & Security Review* 2019, vol. 35, 105327.

⁸⁶ For example, fees for doctors (GoÄ), fees for dentists (GoZ), DRG case fees for hospital billing, ... See G. MALGIERI, “Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations”, o.c.

of the data subject is not fulfilled. If the customer's request is granted, on the other hand, the automated decision-making does not need any particular "suitable safeguard" to protect insureds.⁸⁷

If a policyholder applies for a benefit using personal data of a third party, for example a co-insured family member under private health insurance, there is no decision within the meaning of Article 22, 1 GDPR vis-à-vis the data subject - the third party. Rather, the insurance company makes a fully automated decision on claims arising from the insurance contract with the applicant as policyholder. In this process, personal data of the third party are processed automatically, which requires a legal basis pursuant to Article 6(1) of Regulation (EU) 2016/679, but not an exemption from the general prohibition of automated decisions in individual cases.⁸⁸

Paragraph 2, first sentence, allows insurance undertakings to process health data in the context of automated decisions pursuant to paragraph 1. This is particularly necessary for the automated settlement of benefit claims by private health insurance. According to the Parliamentary documents, Paragraph 2 is based on Article 22, 4 in conjunction with Article 9, 2 (g) GDPR. According to the German government, ensuring affordable and functional health insurance cover in private health insurance constitutes a reason of substantial public interest.⁸⁹

Following the examples given by the German Government in the parliamentary documents, it seems that the case mentioned in Section 37 refers merely to insurance companies decisions pursuant to the request of reimbursements for losses, damages, health issues, etc. of their customers.⁹⁰ For the calculation of risk, it seems that section 31 is applicable:

"(1) For the purpose of deciding on the creation, execution or termination of a contractual relationship with a natural person, the use of a probability value for certain future action by this person (scoring) shall be permitted only if

- 1. the provisions of data protection law have been followed;*
- 2. the data used to calculate the probability value are demonstrably essential for calculating the probability of the action on the basis of a scientifically recognized mathematic-statistical procedure;*
- 3. other data in addition to address data are used to calculate the probability value; and*
- 4. if address data are used, the data subject was notified ahead of time of the planned use of these data; this notification shall be documented."*

15. Stringent requirements and limitations should be imposed on the use of data for personalised risk assessment

In its [opinion](#) (p. 19), the Data Ethics Commission states that stringent requirements and limitations should be imposed on the use of data for personalised risk assessment (e.g. the "black box" premiums in certain insurance schemes). In particular, the processing of data may not intrude on intimate areas of private life, there must be a clear causal relationship between the data and the risk, and the difference between individual prices charged on the basis of personalised and non-personalised risk assessments should not exceed certain percentages (to be determined). There should also be stringent requirements in respect of transparency, non-discrimination and the protection of third parties.

⁸⁷ G. MALGIERI, "Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations", o.c.

⁸⁸ Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Bundesrat Druksache 110/17, 108.

⁸⁹ Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Bundesrat Druksache 110/17, 108.

⁹⁰ G. MALGIERI, "Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations", o.c.

In particular, the [Data Ethics Commission](#) believes that personalised risk assessments must comply with the following ethical requirements (p. 106-107):

- a) data processing must not intrude into the core of an individual's private life. It must be restricted to areas where the individual is already in contact with the exterior world and must therefore expect conclusions to be drawn on the basis of his or her behaviour. This principle dictates that it would be ethically acceptable for a car insurance company (for example) to record the miles driven or traffic offences committed by a driver, but not purely private behaviour inside his or her vehicle, even if this behaviour might be relevant from a risk perspective (e.g. how often he or she yawns, whether he or she chats to passengers), or even the driver's state of health (e.g. heart problems) or other lifestyle factors (e.g. purchasing behaviour in relation to coffee or alcohol);
- b) a clear causal relationship must exist between the data being processed and the risk to be determined, and any linking of data must avoid discriminatory repercussions;
- c) the data must not allow conclusions to be drawn directly that have implications for relatives or other third parties;
- d) full transparency is required as regards the specific parameters and their weighting, and the impacts on pricing or other conditions. The individual must also be provided with clear and comprehensible explanations of how to improve these conditions;
- e) in order to keep unwanted chain reactions in check, the difference between the "optimal" conditions and the conditions that apply if consent is refused must not exceed a certain ceiling (e.g. maximum price difference).

3.1.2. If no, briefly explain what other proposals relevant to your work package they may have formulated

/

3.2. Discussion of relevant substantive proposals identified under 3.1.1.

3.2.1. Proposal 1 – Addressing providers that have not been regulated to date and making sure that the current legal framework is applicable to them; adapting outsourcing systems: efficiency and budgetary aspects

A. Which purposes were identified/established?

Big data and AI give rise to new types of business models and market participants (e.g. tech companies) that are not yet adequately covered by the current legal framework. It is vital that these are identified and that the range of firms and providers to be supervised is expanded accordingly. Therefore, BaFin wants to [identify new players and new types of business models](#) (p. 167) that are not yet adequately covered by the current legal framework.⁹¹

B. How do the measures try to achieve their purpose?

BaFin commits to map and monitor the rise of new business models and new players in the insurance sector. For example, it needs to be checked whether groups of policyholders formed on the basis of Big data and AI for realising P2P insurance, are subject to approval.

Concrete measures were proposed by the respondents to the consultation to adapt outsourcing systems. One proposed option would be to use a type of [digital signature](#) (Issue 1, 2019, p. 17), especially for products that are created in a fragmented value creating process. Every company

⁹¹ Also see: BaFin, Perspectives: Issue 1, 2019, p. 17, https://www.bafin.de/EN/PublikationenDaten/BaFinPerspektiven/AlleAusgaben/BaFinPerspektiven_alle_node_en.html.

in the value creation process would have to be named when using such a signature. Another option to sustain value chains is the [use of smart contracts with a back-up party](#) (issue 1, 2019, p. 20) that would take on any element within the value chain if a company cannot provide it. Other proposals are [minimum technical standards, targeted scenario analyses and volume limits](#) (issue 1, 2019, p. 20).

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, we are not aware of any concrete measures being implemented.

In its [consultation](#) (issue 1, 2019, p. 17), the majority of the respondents consider the existing technology-neutral and principle-based financial market regulatory framework to be adequate in principle – also in relation to financial stability issues. However, the respondents also highlighted that restricting the application of existing regulations to institutions and insurance companies could lead to distortions of competition. Therefore, the respondents propose to examine the effect to which new sales channels are subject to adviser liability. The respondents also highlight the fact that new players do not contribute to the funding of supervisory authorities, which leads to distortions of competition.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

Belgian insurance companies also might have incentives to work with third party suppliers (e.g. tech companies). This raises a number of potential risks (see Part1 Ch5 2.2.6). It might therefore be useful to monitor the market and assess whether the new players and business models are covered by the current legal framework.

3.2.2. Proposal 2 – Re-evaluate the concept of systemic importance: efficiency and budgetary aspects

A. Which purposes were identified/established?

Market analyses indicate that markets and market participants will become more connected than before. This interconnectedness can arise both indirectly, e.g. if the same models, data or platforms are used, and directly through new contractual and trade relationships made necessary by Big data and AI usage. As this interconnectedness increases the risk of domino effects, [BaFin wants to evaluate and address the changing structure of the dynamic of the market and the resulting risks](#) (p. 167).

B. How do the measures try to achieve their purpose?

By monitoring new structural relationships, BaFin wants to [identify new types of business models and market participants that are not yet adequately covered by the current legal framework](#) (p. 167) in order to be able to expand the range of firms and providers that are supervised accordingly. This way, BaFin might also [assess whether the concept of systemic importance needs to be redefined](#) (p. 167) in order to keep pace with new business models and market structures.⁹²

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, we are not aware of any concrete measures being implemented.

⁹² Also see: BaFin, Perspectives: Issue 1, 2019, p. 18.

In the [consultation](#) (issue 1, 2019, p. 19), respondents argued that it would be premature or even impede innovation to lay down new definitions and criteria. So far, it is not clear whether Big Data and AI actually increases systemic risk. According to the sector, it must first be clearly demonstrated on empirical grounds that certain risks may arise in a way that would actually jeopardise the existence of institutions. It was also noted that interconnectedness and complexity are already covered by the current definition of systemic importance.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

The risk for interconnectedness of companies active on the insurance market, as well as the rise of new business models is also a concern in Belgium (see Part1 Ch5 2.2.6)

3.2.3. Proposal 3 – Test scenario an no black box explanation: efficiency and budgetary aspects

A. Which purposes were identified/established?

BaFin wants to [increase explainability and transparency of models](#) (p. 13). AI may lead to very complex models. This makes it difficult to gain insight into how these models work and the reasons behind the decisions. BaFin wants the results of the algorithms to be sufficiently clear to ensure that they can be understood and used by the competent authorities and law enforcement agencies.

B. How do the measures try to achieve their purpose?

By inserting a test scenario and refuse to accept black box explanations, BaFin wants to monitor process results of complex models, in addition to documentation requirements.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, there is no test scenario implemented, nor any other measure to increase explainability.

The [Bundesbank](#) (p. 5) does not support the view of BaFin concerning refusal of black box explanations. According to the Bundesbank, black box is not a no go if risks remain under control.

In the [consultation](#) (issue 1, 2019, p. 25), some of the respondents doubt the usefulness of these test scenarios since the inclusion of predefined scenarios entails the risk of overfitting in such scenarios. Some of the respondents to the consultation add that the reasons behind the decision are the most important for the consumer. Therefore, the individual steps in the decision-making must be traceable at all times (p. 24). One way to ensure traceability is to run existing models and those based on AI in parallel. In doing so, it is possible to understand which influencing factors exist. Other respondents argue that it is unrealistic to require that every customer profile – i.e. every individual decision – is checked and that this would stifle innovation. What is important, in their opinion, is to provide evidence on the forecast and quality and stability of the models used (p. 25).

In 2020, BaFin states in an [expert article](#) that large-scale reviews of algorithmic decision-making processes is not feasible. In order to remain technology-neutral, BaFin's supervision does not focus solely on the algorithm itself but on the overall algorithm-based decision-making process – from the data to the results – and on the associated risks. BaFin reviews and raises objections to algorithm-based decision-making processes in the same manner in which it also deals with human decision-making processes. Moreover, there is no legal basis for a general approval of algorithms or algorithm-based decision-making processes. From BaFin point of view, there is no need to have

a general approval process in place. This view is also supported by the Bundesbank. According to the [Bundesbank](#) (p. 3), the supervisory focus does not lie on AI itself but rather on the risks resulting from its deployment. Supervisors need to carefully take the risks connected with the impact of AI on the respective outcome or decision into account. Risk type, range of application, level of use or decision type are possible criteria to consider.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium, the concern of black box or inexplainsability of algorithms also arises (see Part1 Ch5 2.2.2).

3.2.4. Proposal 4 – Traffic light system and public availability of data protection impact assessments: efficiency and budgetary aspects

A. Which purposes were identified/established?

BaFin states that the increasing complexity and variety of data usage could make it more difficult for consumers to fully grasp how their data is being used. With these measures, BaFin wants to improve transparency.

B. How do the measures try to achieve their purpose?

A traffic light system enables customers to quickly understand the risks involved, without having to read lengthy and complex privacy statements.

Making the data protection impact assessment publicly available, might also help consumers to make decisions regarding their personal data.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, no concrete measures have been implemented.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

Information overload and complex privacy statements that are difficult to understand for consumers is also a point of concern in the Belgian context (see Part1 Ch5 2.2.2).

3.2.5. Proposal 5 – Adequate monitoring and transparency mechanisms to tackle discrimination: efficiency and budgetary aspects

A. Which purposes were identified/established?

The risk of discrimination could increase as algorithms could be based on features for which differentiation is prohibited by law. BaFin also wants to tackle the risk that customer segments could be differentiated on the basis of false assumptions or false conclusions made by algorithms on the basis of these assumptions and that costumers may in fact be discriminated against even if this is unintentional.

B. How do the measures try to achieve their purpose?

By requiring firms to ensure that adequate monitoring and transparency mechanisms are in place, BaFin wants [to prevent models from drawing such false or unauthorised conclusions](#) (p. 177).

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, BaFin did not implement a concrete measure to tackle the risk of discrimination by algorithms.

Some of the [respondents](#) (issue 1, 2019, p. 33) to the consultation call for algorithms to be checked regularly. Potential discrimination should be looked into during the developments of models, using methods such as bias correction. Others argue that imposing a ban on discrimination would be a difficult task, from a technical point of view. According to them, retrospective spot checks of individual decisions are the only feasible approach (issue 1, 2019, p. 33). In 2020, BaFin states in an [expert article](#) that large-scale reviews of algorithmic decision-making processes is not feasible (see proposal 3).

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium as well, insurance companies are prohibited from pricing based on certain by law protected criteria. However, AI could lead to the application of other criteria that are not protected by law. Moreover, the use of those factors could even lead to proxy discrimination (see Part1 Ch5 2.2.9). Requiring insurance companies to regularly check their algorithms and data sets could help to avoid unintentional (proxy) discrimination.

3.2.6. Proposal 6 – Only use data that is actually relevant for risk assessment: efficiency and budgetary aspects

A. Which purposes were identified/established?

The analysis of Big data and AI in the insurance sector has shown that, under certain conditions, a more precise assessment of the risk exposure for individual policyholders could result in increased selection. Hence, Big data and AI could disproportionately limit individual consumers' access to certain financial services. This situation can be particularly precarious if consumers are disadvantaged by having access to a narrower range of products but are unaware that this is caused by the personal data they have supplied. So, with these measures, BaFin wants to [ensure insurability and access to financial services](#) (p. 177).

B. How do the measures try to achieve their purpose?

By forbidding insurance companies to use data that is not actually relevant for their risk assessments, BaFin wants to avoid potential policyholders getting excluded from insurance or having to pay a higher premium.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, no concrete measures were taken.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

Also in Belgium, the fear for hyper personalised risk assessments caused by the growing amount of data available to insurance companies rises (see Part1 Ch5 2.2.10). In Belgium, the use of certain data is already prohibited. Moreover, the rules regarding segmentation criteria already prohibit insurance companies from using data that is not objectively justified for risk assessment. However, it might be necessary to reassess this rules in the light of new developments (see Part1 Ch5 6.2).

3.2.7. Proposal 7 – Responsibility: efficiency and budgetary aspects

A. Which purposes were identified/established?

BaFin wants to [ensure that responsibility for decisions stays with persons](#) (p. 172) and is not shifted to machines.

B. How do the measures try to achieve their purpose?

BaFin states that responsibility for automated processes is to remain with the senior management of the firm. When designing automated processes, firms must ensure that they are embedded in an effective, appropriate and proper business organisation. [Appropriate documentation](#) (p. 172) is required to ensure this.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, no concrete measures have been implemented.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium as well, the concern for accountability and responsibility for the decisions of AI tools is raised.

3.2.8. Proposal 8 – Provide alternative products: efficiency and budgetary aspects

A. Which purposes were identified/established?

BaFin wants to [ensure that consumers have an actual freedom of choice](#) (p. 15). Moreover, the use of Big data and AI might result in greater perceived or de facto pressure on consumers to provide their data, for instance to be able to take out insurance at affordable premiums.

B. How do the measures try to achieve their purpose?

By requiring insurance firms to provide less data-intensive products, consumers might feel less compelled to share their personal data.

C. Where possible to assess, to what extent did these measures achieve their purpose?

Some of the respondents to the consultation argue that defining when a contract is non-digital or conventional is very complex. Others propose that legislators should [guarantee basic coverage](#) (p. 35). Another proposal is to [create a certificate for financial services requiring limited amounts of data](#) (p. 36). However, some of the respondents warned that this might suggest that the principle of data minimisation does not apply to other financial products.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium as well, concerns about fairness are raised when it comes to individualised insurance products. Interest groups also advise that consumers should continue to be able to access insurance policies that do not rely on intrusive data processing practices or behavioural analytics (see Part1 Ch5 3).

3.2.9. Proposal 9 – Hub-and-spoke concept: efficiency and budgetary aspects

A. Which purposes were identified/established?

On the one hand, the [objective](#) is to derive supervisory consequences and potential courses of action, and extending the scope for supervisory action and reaction. On the other hand, the objective is to establish any need for regulatory change (p. 5).

B. How do the measures try to achieve their purpose?

The [hub](#) (p. 5) is formed by the Innovations in Financial Technology division that has been established in the President's Office. It is connected to the relevant divisions and works closely with them. The hub-and-spoke architecture is used to identify financial technology innovations at an early stage, to formulate realistic scenarios for the near future and to elaborate implications for supervisors and regulators on that basis.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium, the concrete implications of new business models and the regulatory gaps are also not clear yet. Therefore, setting up a hub could be useful.

3.2.10. Proposal 10 – Providing processes and criteria to ensure data quality: efficiency and budgetary aspects

A. Which purposes were identified/established?

BaFin wants to [prevent the risk of incorrect decisions due to insufficient data quality](#) (p. 53).

B. How do the measures try to achieve their purpose?

BaFin wants to [provide processes and criteria, including completeness, consistency, validity and accuracy and/or timeliness](#) (p. 53). In principle, however, market players have the responsibility to prevent the risk of incorrect decisions being made as a consequence of data bias due to insufficient data quality and scope.

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

The concern of insufficient data quality also arises in Belgium (see Part1 Ch5 2.2.1).

3.2.11. Proposal 11 – Cooperation with financial supervisors and data protection authorities: efficiency and budgetary aspects

A. Which purposes were identified/established?

Data protection authorities are responsible for monitoring the implementation of data protection requirements. However, if data protection violations become more frequent in the insurance sector, this could also have implications for financial supervisors.

B. How do the measures try to achieve their purpose?

If there is an institution or company that frequently violates data protection standards, this may constitute an irregularity that also concerns BaFin. In cases like this, [BaFin](#) will take appropriate measures as part of its supervisory activities (p. 7).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium as well, more intense cooperation between supervisors might be helpful to monitor the market and to tackle potential concerns.

3.2.12. Proposal 12 – Creating a consumer-centred data portal: efficiency and budgetary aspects

A. Which purposes were identified/established?

The aim of this measure is [to give consumers more control over the use of their individual data](#) (p. 52) by the various providers. For companies, this kind of portal also intends to offer legal certainty within the context of the EU GDPR.

B. How do the measures try to achieve their purpose?

This data portal enables consumers to centrally delete and change their data as well as to manage the access rights to their data centrally by using a single portal.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, this measure has not been implemented yet.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium, this kind of portal might also be useful to enable consumers to have more control over their data.

3.2.13. Proposal 13 – Utilising technical options for using Big data and AI with anonymised data: efficiency and budgetary aspects

A. Which purposes were identified/established?

With this measure, BaFin wants to [further bolster customer trust in Big data and AI innovations](#) (p. 15). In addition, BaFin wants to ensure the secure handling of personal data.

B. How do the measures try to achieve their purpose?

BaFin proposes to use technical data protection measures as a privacy by design concept.

C. Where possible to assess, to what extent did these measures achieve their purpose?

So far, this measure has not been implemented yet.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

The secure handling of personal data is also a concern in Belgium.

3.2.14. Proposal 14 – Specific legal basis for automated individual decision-making, including profiling, in the context of providing services pursuant to an insurance contract: efficiency and budgetary aspects

A. Which purposes were identified/established?

The German Government wanted to create a legal basis allowing automated individual decision-making, including profiling, in order to meet the particularities of the insurance sector. Following the German Government, automatic processing is important for insurance companies to remain economically viable. Moreover, the government wants to ensure affordable and functional private health insurance.

B. How do the measures try to achieve their purpose?

The German government made use of the possibility following article 22, 2 b) GDPR for member states to create a legal basis allowing automated individual decision-making, including profiling, in the context of providing services pursuant to an insurance contract. Moreover, it established that ensuring affordable and functional private health insurance cover is a matter of substantial public interest (article 9, 2 g) GDPR).

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

The question of whether insurance companies should be allowed to apply automated individual decision-making, including profiling, is also raised in a Belgian context (see Part1 Ch5 5.1.1).

3.2.15. Proposal 15 – Stringent requirements and limitations on the use of data for personalised risk assessment: efficiency and budgetary aspects

A. Which purposes were identified/established?

First, the [Data Ethics Commission](#) (p. 106) fears that some potential insureds might feel pressured to give consent for the processing of their data. Processing of additional personal data for the purpose of personalised risk assessments regularly requires consent from the data subjects. Individuals who hope to gain economic advantages as a result are particularly likely to grant such consent, yet the granting of consent by one individual may have significant impacts on others, and give rise to chain reactions that are problematic from an ethical viewpoint (unravelling effects). This may put data subjects under disproportionate pressure, and jeopardise the voluntary nature of consent.

Second, the [Data Ethics Commission](#) (p. 106) fears that the solidarity principle underlying insurance might come under pressure. The goal of increasingly granular risk assessments runs counter to the basic principle of collective risk sharing by the community of all insured persons. Taken to its extreme (i.e. if the insurer has access to “comprehensive” information and adjusts the price to the individual risk), the whole concept of insurance would be reduced to absurdity.

B. How do the measures try to achieve their purpose?

The Data Ethics Commission proposed some ethical requirements personalised insurance products must comply with in order to counter the concerns, such as strict requirements in respect of transparency, non-discrimination and the protection of third parties

C. Where possible to assess, to what extent did these measures achieve their purpose?

No information available.

D. Where possible to assess, what impact did the measures have on the government budget?

No information available.

E. Are the abovementioned findings applicable to the Belgian context and purposes, as well as to the gaps? (If applicable)

Yes.

In Belgium, the same concerns regarding personalised insurance contracts arise (see Part1 Ch5 2.2.2 and 2.2.8-10).

CHAPTER 6 – CONCLUSIONS

In this report, we conducted a legal comparative analysis with regard to intellectual property and trade secrets, consumer protection and competition law, as well as diverse fields of ICT law, including AI-safety and cybersecurity, data sharing, the eIDAS Regulation, e-Commerce and insurance legislation. We aimed to identify how other jurisdictions are dealing with AI-related issues in those field, and especially whether policy actions have already been taken by Belgium's neighbouring countries – the Netherlands, France, Germany and the United Kingdom. This comparative research will be used for our recommendations that will form the object of a third study in which we will attempt to provide normative recommendations.

Contributing authors (alphabetical): Jeffrey Amankwah, Jan De Bruyne, Alexandre de Streel, Thomas Gils, Daphné Hof, Hervé Jacquemin, Michael Lognoul, Victoria Ruelle, Nele Stroobants, Jozefien Vanherpe, Caroline Van Schoubroeck, Peggy Valcke & Koen Vranckaert



FPS Economy, S.M.E.s, Self-employed and Energy

Rue du Progrès 50
1210 Brussels
Enterprise no: 0314.595.348
economie.fgov.be