Tackling identity theft with a

"Harmonized framework, allowing a sustainable and robust identity for European Citizens."

D7.2

Deliverable ID :	***D7.2***
Deliverable Name :	***Study on criminal law measures to tackle identity fraud and identity theft***
Status :	**Finished**
Dissemination Level :	***RE***
Due date of deliverable :	***M36***
Actual submission date :	**M36**
Work Package :	***WP7***
Organisation name of lead contractor for this deliverable :	***KUL CITIP***[1]
Contributing partners	AgID, UC3M, IDP, SPRL
Author(s):	***Kristel De Schepper and Helena Severijns (researchers)*** ***Frank Verbruggen (supervisor)***

1 CITIP (Center for IT and IP Law) has replaced "ICRI" (Interdisciplinary Center of Law and ICT) mentioned in the DoW.

This project is funded as a FP7- SEC-2013.1.1-2: "Stronger Identity for EU citizens" – Capability Project. The project has received funding from the European Community's Framework Programme (FP7/2007- 2013) under the Grant Agreement n° 607049.

Abstract: This deliverable focuses on substantive and procedural criminal law measures to tackle identity theft and its consequences. Because identity-related crime is such a complex and broad phenomenon, we first outline the context in order to detect the key challenges. Next, we look at the criminalisation of identity theft. Criminalisation is the shaping of particular wrongful behaviour into an offence. Hence the relevant features of the phenomenon are highlighted, different concepts clarified and the legal interests at stake in the context of identity theft identified. The paper further examines and evaluates different strategies to criminalise identity theft. It finds that existing criminal provisions do not adequately protect the role of identification information as a 'IT-personalised key', nor the interests of the primary victim of identity theft. New technologies make it more difficult for the primary victims to clean up the mess caused by the abuse of their data and to restore their compromised identity.

On basis of the ECtHR law we conclude that EU member states have a positive obligation not only to criminalise identity theft but also to bring the identity thief to Court and to restore a compromised identity. States cannot do this alone. Governments have to elaborate a legal framework that obliges third parties, in particular service providers, to cooperate with law enforcement. When dealing with identity theft, the following measures should be considered: reporting mechanisms and notification duties for the data controller; the identification of the perpetrator and the retention and preservation of data to assist law enforcement; and the blocking of access to and the rendering inaccessible of the illegal content, and/or the deletion of illegal content. For now it remains unclear if service providers have to take data offline upon the simple request of a data subject. We suggest that prior to taking data related to ID fraud offline, an assessment of the notified identity fraud should be made by an assessment centre with a high expertise in identification and ID fraud. Here the EKSISTENZ project's tools can be used to verify the identity of the person claiming to be an identity fraud victim. These centres should be complemented by hotlines for individuals to report ID theft. Once ID theft is established, these centres can then ask service providers (voluntarily) to take down or block certain data.

As identity theft mostly happens online, it is often a cross-border crime. International cooperation is thus critical to tackle ID theft. The final part of the deliverable focuses on

procedural jurisdiction and the enforceability of forced ISP cooperation in a cross-border context. The current framework is found unsatisfactory: measures in the fight against ID theft are excessively hindered by a lack of (enforcement) jurisdiction or by slow or inexistent mutual legal assistance.

Belgian legislation and case law feature prominently in the research, not just because of the access of the researchers to the sources, but mainly because Belgian courts and the Belgian legislators have been ambitious in their explicit, internationally resounding, effort to alter the existing legal status quo when it comes to cooperation duties for service providers in criminal law procedures. Furthermore, national legislation and case law from other EU countries and the U.S. was included to the extent that it provided us with new insights.

This deliverable is drafted based on literature research undertaken by KU Leuven Institute of Criminal Law and CiTiP, as well as input provided by the contributing partners: AgID, UC3M, IDP, SPRL as foreseen in the DoW. The research is kept up to date until 25 May 2017.

© Copyright by the EKSISTENZ Consortium

Table of contents

Introduction

OBJECTIVE. – The overarching objective of the EKSISTENZ Project (hereafter 'the Project') is to protect EU citizens from major threats to their identity. The Project will therefore propose innovative solutions to create a real and strong link between the citizen and his or her primary identity document. It will focus on the citizen, to propose solutions to prevent, detect, respond and recover from an identity theft incident. To this end, the Project will:

Strengthen existing electronic-based primary identity documents, and associated bearer authentication methods, using biometric features and/or prior knowledge about the legitimate holder.

1. Derive from the primary identity document some secondary identities, in controlled environments.
2. Uniquely and easily verify primary and secondary identities and the bearers of such identities.
3. Use the European Union funded STORK2.0 project in order to provide bilateral recognition solutions of primary identity between EU Member States.

The objective of this paper is to analyse the relevant criminal law framework needed to ensure secure citizen IDs and to provide suggestions to curtail the existing legal uncertainty with regard to identity fraud and identity theft. We will study criminal law measures to tackle the abuse of primary identities and secondary identities derived from this primary identity and the shortcomings of such measures. According to the EKSISTENZ terminology proposal 'primary identity' refers to a token:

- issued by a Member State;
- that is subject to an electronic identification scheme as defined in EU Regulation 910/2014 and appears in the list of such schemes that the European Commission maintains (and publishes) according to article 9 of that regulation;

Most often, it refers to an e-ID card. Such card can be regarded as a token or means to identify.

'Secondary identity' can be regarded as a token:

- the credentials of which have been (partly or wholly) validated based on a primary token of the entity to which these credentials pertain;
- the credentials of which have been issued by the token issuer;

- that is subject to an electronic identification scheme as defined in EU Regulation 910/2014
    - that is published by the token issuer;
    - that pertains to tokens issued by that token issuer;
    - and that satisfies the requirements of article 7 of the Regulation (replacing '(notifying) Member State' with 'token issuer').

The main objective of the Project is to guarantee that the means of identification truthfully identify the person who uses it (the 'identity match'). The focus of this paper therefore lies on the abuse of (primary and secondary) identification means in the context of an identification process and on the role played by criminal law. The abuse of identities is not a new phenomenon. Long before the existence of the Internet, identity documents were stolen, forged and false names were used to hide one's own identity and to commit crimes.[2] The Internet and the digital technology have however created new opportunities and have rendered the problem more complex.[3] We will therefore pay specific attention to this new context. The research tries to detect shortcomings in the legislation available to tackle this phenomenon and to make suggestions for a clear, adequate criminal law framework to ensure secure citizen IDs.

VICTIM PERSPECTIVE: RESTORATION[4] – From the victim's perspective, the impact of identity abuse can be significant (*cf. infra*). One approach to the phenomenon is to look at possible criminal law mechanisms to repair the harm caused by the crime and to limit further damage in order to prevent repeat victimisation. It is important to distinguish clearly

---

2 Note that these acts are not always committed for criminal purposes but also for good reasons, e.g. the legitimate use of false identities by undercover agents or political refugees. 'False' does not necessarily have to be 'wrong', e.g. the use of pseudonyms to criticize the government to hide from authoritarian governments like Germany's before and during World War II (*cf. infra*).

3 W. BRUGGEMAN, R. VAN EERT, A. VAN VELDHOVEN (eds.), *What's in a name? Identiteitsfraude en – diefstal*, Antwerpen, Maklu, 2012, 82.

4 Consideration 9 of the EU Victim's Directive stresses the importance of crime as a societal wrong as well as a violation of the individual rights of victims. As such, victims of crime should be recognised and treated in a respectful, sensitive and professional manner. Victims of crime should be protected from secondary and repeat victimisation, from intimidation and from retaliation, should receive appropriate support to facilitate their recovery and should be provided with sufficient access to justice. This is the essence of restorative justice. Cf. Directive 2012/29/EU of the European Parliament and of the council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and of replacing Council Framework Decision 2001/220/JHA, *OJ* 2012 L 315, 57.

between the different types of victims, because the legal remedies will be different. First we have the 'primary victim', this is the natural person whose identity is abused without his or her consent and whose identity risks being compromised (the 'original identity bearer').[5] In the overall context of the Project it is however important to note that the impersonated person can also consent to this: there can be collusion with the identity fraudster. In that case he or she may even become an accomplice to the identity abuse. The Project also covers these types of abuse as the focus lies on any type of manipulation of identification means in the identification process; in other words, any fraud where a person pretends to be someone else, either with or without the consent of the original identity bearer. This can also be committed with a fictitious identity or even with the identity of a deceased person. Our research will however focus on the hypothesis that the original identity bearer does not consent, because criminal law faces some specific problems in dealing with it (*cf. infra*).

Secondly, there is the 'secondary victim', the third party who is defrauded or otherwise harmed by the perpetrator who is impersonating someone else.[6] The secondary victim can either be a private company that relies on the identification means in order to provide services, e.g. an airline company that sells airline tickets, or a governmental authority that relies on it to give citizens access to key governmental activities.

A third specific category of potential victims are the parties who store the identification information (the data controllers[7]). They will have a responsibility towards this

---

5 Note that this may also be a legal person. Most research on identity theft focus on the identity of natural persons. 'Stealing' a company's identity is however an equally significant phenomenon which relates more to intellectual property rights (trademarks etc.). Due to the scope of this paper, we will not study this type of identity 'theft' but indicate that this is also an interesting issue.

6 Centre for Strategy & Evaluation Services, *Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft*, 2012, 171, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf. (hereafter referred to as 'CSES Impact Assessment').

7 The data controller is the (natural or legal) person who (alone or jointly) decides to process personal data of others. The controller determines the purposes and means of the processing, f.i. a credit institution who decides to create a database for its defaulting customers. A data processor is the (natural or legal) person who processes data on behalf of the data controller, f.i. a marketing company who conducts a market analysis of the customer data on request of the credit institution. Both have responsibilities towards the data, but the overall responsibility lies with the data controller, who must ensure compliance with data protection law. A processor can also be a data controller in its own right, in relation to the personal data it processes for its own purposes. A processor furthermore also becomes a controller when he/she exceeds the limitations of the use as prescribed by the data controller, at least to the extent of the breach. EUROPEAN UNION AGENCY FOR

information (*cf. infra*). If their systems are targeted, they not only face direct damage but they will also risk liability claims and reputation loss.

RISK ACCEPTANCE - For our research, we assume that abuse can never be fully prevented. Studies have detected vulnerabilities in every step of the identification process. They have shown that risks can be reduced but never fully excluded.[8] Hence, the first step is to recognize this fact and to accept it (risk acceptance). Only then we can reflect on further alternatives to tackle the phenomenon, which for victims should entail measures to put an end to the harmful consequences of identity theft. We will therefore analyse which criminal law instruments are available for victims to ensure the restoration of their identity and whether they properly address their needs.

VICTIM RIGHTS - The EU Victims' Directive defines the victim as '*a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence*'.[9] In case of identity abuse, first and foremost this refers to the primary victim. According to consideration 52 and article 18, measures should be available to protect the safety and dignity of victims (and their family members) from secondary and repeat victimisation, f.i. interim injunctions. There should be measures which protect against the risk of emotional and psychological harm. Consideration 62 states that for victims of crime to receive the proper degree of assistance, support and protection, public services should work in a coordinated manner and should be involved at all administrative levels (EU, as well as national, regional and local). In order to avoid repeat referrals, victims should further be assisted when finding and addressing the competent authorities. This includes the development of 'sole points of access' that address victims' multiple needs when involved in criminal proceedings. They include the need to receive information, assistance, support, protection and compensation. All these points should be borne in mind when one studies the criminal law remedies available to the

---

FUNDAMENTAL RIGHTS and COUNCIL OF EUROPE, *Handbook on European data protection law*, Luxembourg, Publications Office of the European Union, 2014, 49-54.

8 FIDIS D12.7, 'Identity-related crime in Europe - Big problem or big hype?', www.fidis.net (hereafter referred to as 'FIDIS D12.7'); *Cf.* N. VAN DER MEULEN en B.-J. KOOPS, 'Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude', *NJB* 2012, 1414.

9 Art. 1.a.i. Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA.

victims as a proper response to identity fraud, including the *recovery* of a compromised identity.

Articles 21 and 22 oblige Member States to protect the privacy of victims and to assess the specific individual needs of the victim, depending on (among others) the type or nature of the crime. We will therefore investigate to what extent recovery of the 'compromised' identity can be seen as entailing a positive state obligation. Under the doctrine of positive human rights obligations, developed by the European Court of Human Rights ('ECtHR'), states can be compelled to implement an adequate criminal law framework in order to punish human rights violations and to apply it in practice through effective investigation and prosecution.[10] This contains three aspects[11]:

- An obligation to *criminalise*: to enact appropriate and adequate criminal law provisions. The question in this context is not whether States should criminalise forms of identity abuse. As we will see further, a variety of criminal law provisions can be applied in cases of such abuse. The relevant question is *how* this behaviour should be criminalised;
- An obligation to *investigate*: to guarantee effective criminal law protection against human rights violations through effective investigation and prosecution. This implies making the crime less profitable and appealing by increasing the risk of being caught and reducing the damages. This entails among other reporting mechanisms and identification of the perpetrator;
- An obligation to *remediate*: to guarantee effective remedies against human rights violations. As we will see below, a mere financial compensation does not suffice in this context. The most important concern of primary victims is that the compromised identity is 'restored'.

In this analysis, we will also look at corporate responsibilities, in particular those of internet service providers. They play a vital role in our digital information society. To what

---

10 ECtHR 20 March 2012, *C.A.S. and C.S. v. Romania*; ECtHR 27 September 2011, *M. and C. v. Romania*, ECtHR 2 December 2008, *K.U. v. Finland*; ECtHR 4 December 2003, *M.C. v. Bulgaria*; ECtHR 28 October 1994, *Murray v. United Kingdom*; ECtHR 26 March 1985, *X&Y v. the Netherlands*; J.-F. AKANDJI-KOMBE, 'Positive obligations under the European Convention on Human Rights A guide to the implementation of the European Convention on Human Rights', Human rights handbooks, No. 7, Council of Europe 2007. ; C. CONINGS, J. HUYSMANS, F. VERBRUGGEN, 'Dagelijkse kost: Europese ingrediënten die het Belgische strafrecht kruiden' in R. VERSTRAETEN en F. VERBRUGGEN, *Straf- en strafprocesrecht,* Brugge, Die Keure, 2012-13, 21-22.

11 P. DE HERT, 'Systeemverantwoordelijkheid voor de informatiemaatschappij' in *De Staat van Informatie*, Amsterdam, Amsterdam University Press, 2011, 39-42.

extent does this impose specific obligations on them?[12] Under the current legal framework internet service providers profit from a rather flexible liability regime which diverges from the normal regime for criminal liability (*cf. infra*).[13] Is this is still tenable in today's society or should their responsibilities be increased?[14] DE HERT describes two models: 1) a 'compliance model', where corporations merely have to ensure compliance with human rights but are not actively engaged in their protection and 2) an 'accountability' model, where the responsibilities of corporations are 'upgraded' and these corporations are forced to actively protect human rights.[15] States have a choice between these two models. A positive State obligation in this context could however mean that European Member States demand a certain 'co-responsibility' from service providers to ensure the protection of the human rights of citizens. DE HERT claims that, from a human rights perspective, an accountability model would be the most obvious choice.[16] Others tend to differ, fearful as they are of private, corporate intrusion on internet activities of users, of private intervention, censorship and exclusion.[17]

OUTLINE. – Because identity abuse is such a broad and complex problem, we will first identify and demarcate the scope of the research (chapter I). In chapter II we will examine the criminalisation. When, despite of all preventive measures taken by government, companies and citizens, the identity has indeed been abused, we need adequate substantive criminal law instruments to take the necessary action against the perpetrator. 'Adequate' however does not necessarily have to mean 'specific' legislation. We will look at different ways of criminalisation and analyse whether this contributes to the victim's right to restoration.

---

12 *Ibid,* 43.

13 Art. 12 to 15 e-Commerce Directive

14 S. BIJLMAKERS, *The Legalization of Corporate Social Responsibility: Towards a New Doctrine of International Legal Status in a Global Governance Context*, Thesis for the Degree of Doctor in Laws KU Leuven, 2017, 495 p; B. A. ANDREASSEN and V. KHANH VINH, *Duties across borders,* Antwerpen, Intersentia, 2016, 342 p.

15 P. DE HERT, 'Systeemverantwoordelijkheid voor de informatiemaatschappij' in *De Staat van Informatie*, Amsterdam, Amsterdam University Press, 2011, 37-38.

16 *Ibid*., 62.

17 A. KUCZERAWY, 'Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative' (ICRI Working paper 21), *Computer Law and Security Review* 2015, 46-56; P. VAN EECKE, 'Online service providers and liability: a plea for a balanced approach', *Common Market Law Review* 2011, 1455-1502; P. VAN EECKE and B. OOMS, 'ISP liability and the E-commerce directive: a growing trend toward greater responsibility for ISPs', *JIL* 2007, 3.

Criminalisation, the modelling of particular wrongful behaviour into an offence, is however not the only response to the phenomenon. As we will see later, new technologies make it more difficult for the primary victim to clean up the mess and to restore the compromised identity. Next to adequate substantive criminal law provisions, we also and urgently need to focus on procedural measures to end the crime immediately in order to limit further damages for the primary victim and to restore the harmful consequences.[18] We will study this in the chapter III.

As identity theft most of the time happens online, it is often a cross-border crime. Chapter IV of this deliverable therefore focuses on procedural jurisdiction and the enforceability of forced ISP cooperation in a cross-border context. In Chapter V we will focus on which steps can be taken to tackle ID fraud more efficiently.

---

18 N. VAN DER MEULEN en B.-J. KOOPS, 'Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude', *NJB* 2012, 1414.

I The (ab)use of identity in the digital information society

1 The key to unlock many doors

IDENTITY AND IDENTIFICATION. - In contemporary society, identity is a concept that has expanded and diversified. Therefore, as we will see later on, many situations may lead to impersonation (the taking over of another identity or pretending to be someone else). An identity is construed by multiple elements that represent a person. These attributes must be included in its definition.[19] Identity is thus the set of information that can be used to establish who we are as unique individuals in order to distinguish us from another with certainty.[20]

This functional definition links identity to *identification*, a practical pocess to verify the identity of individuals in order to conduct social, governmental or commercial activities.[21] Identity in this context must be understood as 'civil' or 'bureaucratic' identity.[22] Governments rely on identity to give citizens access to specific key governmental activities related to immigration, taxation, national and social security and criminal records. The private sector uses it for a range of commercial activities, such as access to financial services, medical health care services, telecommunication services and so forth.[23] Identity thus allows a person to be qualified as a 'legal subject' to whom the government and other parties can attribute specific acts in a reliable way.[24]

---

19 T. CASSUTO, 'Usurpation d'identité numérique, *AJ Pénal* 2010, 220.

20 N. ROBINSON, H. GRAUX, D.M. PARRILLI, L. KLAUTZER and L. VALERI, *Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report*, 2011, 1, http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf (hereafter referred to as 'RAND Study'); S. REVEL, 'Précision sur la notion d'usurpation d'identité ou l'inexistence de l'ubiquité', *AJ Pénal* 2010, 218.

21 RAND Study, 5.

22 U.R.M.Th. DE VRIES, H. TIGCHELAAR, M. VAN DER LINDEN en A.M. HOL, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, 2007, 32.

23 RAND Study, 1; B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, 'A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 2.

24 S. REVEL, 'Précision sur la notion d'usurpation d'identité ou l'inexistence de l'ubiquité', *AJ Pénal* 2010, 218.

Identification is to ensure that the identity actually belongs to the person who claims to be that person. It is the match between the identification information and the individual.[25] Information that can be used to identify is called the 'identifiers'. It however does not guarantee that the found identity is an authentic description of that person.[26] Identification is based on the assumption that the identifier is indeed a reliable proof of the identity match. This proof is usually given on the basis of what a person possesses (e.g. an identity card), knows (e.g. a password) and/or is (e.g. fingerprints).[27]

Identifiers, such as the name, date of birth, fingerprints, etc., are intangible information. In order to serve as evidence of an identity, they are registered in authentic acts. These acts, which have a specific legal status, guarantee the link between the identifier and the individual (birth or death certificate, passport,…).[28] These proofs of the identity are the *means* of identification (which contain identifiers). They can either be tangible (such as the identity card) or intangible (such as the biometric data digitally stored on the identity card).

ELEMENTS OF IDENTITY AND CONNECTED RISKS. – The individual characteristics which constitute an identity are[29]:

- physical and biometric information, e.g. height, signature, DNA, fingerprint, iris, bone structure, teeth, voice, keystroke dynamics, body heat, medical history,…. These attributes are closely linked to an individual and are more or less unique[30];

---

25 B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 3.

26 An Eksistenz terminology proposal

27 FIDIS D5.2b, 'ID-related Crime: Towards a Common Ground for Interdisciplinary Research', 2006, 79-80, www.fidis.net (hereafter referred to as 'FIDIS D5.2.b').

28 T. CASSUTO, 'Usurpation d'identité numérique, *AJ Pénal* 2010, 220.

29 B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, 'A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 3 ; U.R.M.Th. DE VRIES, H. TIGCHELAAR, M. VAN DER LINDEN en A.M. HOL*, Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid, Universiteit Utrecht 2007, 34.

30 Excluded are the personality characteristics, such as 'friendly', 'arrogant', 'pleasant',…. Which are not relevant in the formal identification process. U.R.M.Th. DE VRIES, H. TIGCHELAAR, M. VAN DER LINDEN en A.M. HOL*„ Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid, Universiteit Utrecht 2007, 34.

- functional attributed information, e.g. name, address, unique identification number, social security number, password[31], account and account number, date and place of birth, badge, licence plate, credit card number, telephone number, IP address, …. These elements are attributed to an individual, either in a vertical relationship by states or in a horizontal relationship by private parties. Some of them may have a special legal status because of their specific function (e.g. a passport, a driving licence,…).[32] Apart from the name, these elements are instinctively further removed from the individual as they usually reduce a person to a number or an objective fact;
- Biographical information, e.g. civil state, criminal record, employed/unemployed, adult/minor, diploma, student, etc.). These elements divide people into certain categories. These categories tell something about the life development of an individual and his position in society;[33]
- Chosen (or user-created) information, e.g. nickname, pseudonym, avatar, a (chosen) password.[34] This type of information becomes increasingly relevant in our information society as a so-called 'unique' identifier although it remains an artificial specification in the sense that it is created by the individual himself.

A chosen or user-created identity is highly volatile and unstable. This makes it the least reliable as a means to identify, verify and authorize. Some chosen or user-created information that does provide access, for instance usernames and passwords, are really at the core of identity-related crime[35] because they are often easy to obtain. On the other hand, they are also easy to restore. Other user-created information, like a Facebook profile,

---

31 Some passwords are attributed by the service provider and not chosen.

32 U.R.M.Th. DE VRIES, H. TIGHELAAR, M. VAN DER LINDEN and A.M. HOL, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid, Universiteit Utrecht 2007, 34.

33 *Ibid.*

34 Some e-mail addresses are not chosen but attributed to a person, i.e. your work e-mail address. B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 4.

35 *Cf. infra* for an explanation of the use of the term identity-related crime.

are wanted for social engineering.[36] The question therefore arises which legal value should be given to this type of identifier in the identification process. The popular and common use of pseudonyms moreover disrupts the identification process.[37]

Biographical information also fluctuates but not in the same way. These are personal, societal attributes build up over time and which change during a person's life ('life events'). They usually do not provide access but are nonetheless attractive because they tell something about who or what a person is. They are therefore mostly used for profiling means (profiling of customers, criminals, for statistics etc.) or social engineering, to lure people into false beliefs.

As they are stable, functional identifiers were traditionally used most to identify an individual and to recognize him or her as a legal subject with rights and obligations (vertical vis-à-vis the government and horizontal vis-à-vis third parties). For people intent on crime, functional attributed information is therefore most appealing. As they are principally used for verification, authentication and authorization[38], they are valuable. They are also relatively easy to obtain and to abuse through stealing, forgery, hacking etc. Especially functional information in the electronic form appears to introduce considerable vulnerabilities (*cf. infra*).

The use of biometrics has significantly increased the ability to compare characteristics of human beings in order to exclude or link with high probability.[39] They are therefore used ever more as identifier, specifically as a back-up of functional information in order to prevent identity abuse, and thus as a countermeasure against identity-related crime. Yet, research has shown that biometrics can also be misused. Especially since biometrics are usually not secret.[40] The 'stealing' or forging of biometric information becomes more and more attractive as biometrics are deemed very stable and safe. As we will see further,

---

36 B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 4-5.

37 T. CASSUTO, 'Usurpation d'identité numérique, *AJ Pénal* 2010, 220.

38 Verification in order to check the correctness of *the information* (i.e. verifying if the entered pin code is the correct code), authentication in order to verify *the person*, i.e. to verify if person X (who enters the pin code) is actually person X., and authorization to assess the claim connected to the identity, i.e. X wants to get access to service Y. Is he authorized to do so? Cf. B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, 'A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 3.

39 T. CASSUTO, 'Usurpation d'identité numérique, *AJ Pénal* 2010, 220

40 E. KINDT, *Privacy and Data Protection Issues of Biometric Applications: a Comparative Legal Analysis*, Springer, Dordrecht, 2013, 335.

biometrics are thus a double-edged sword in tackling identity-related crime. A major concern for instance is that the detection of fraud involving biometrics is difficult and once the biometrics are compromised, they become useless as a reliable identification tool.[41]

41 FIDIS D5.2b, 93.

2 Identifying the challenge: protecting the 'IT-personalised key'

IDENTIFICATION IN THE DIGITAL INFORMATION SOCIETY. – The digitisation has made it possible to introduce technical standards in order to identify, with a high degree of trust, users of certain IT-systems. Digital signature, authentication protocols and encryption ensure the regularity of transactions.[42]

At the same time, this digitisation introduces new risks for the identity information and the identification process, which is still mostly nationally organised and based on traditional methods of verification. First of all, identity information is increasingly digitised and stored in IT systems and that makes it available for illegal access and thus more vulnerable.[43] Secondly, the technology makes it possible for perpetrators to act quasi anonymously. This anonymity gives them an obvious advantage. Online verification and authorization of identity is less obvious than offline because the Internet lacks traditional ways of identity control.[44] Face-to-face verification is for instance replaced by machine verification or even no verification at all.[45] By simply creating an email-account without the need of identity verification, one can create a false identity.[46] Online authentication procedures are therefore considered as intrinsically less secure than offline procedures.[47] They often merely rely on the combination of a public or semi-public identifier and a password.[48] Because it is so easy to create fictitious identities, the only reliable identifier is often the IP–address. The reliability of this type of identifier is however relative as it technically very

---

42 T. CASSUTO, 'Usurpation d'identité numérique, *AJ Pénal* 2010, 220.

43 RAND Study, 2; B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 2.

44 E. KINDT, *Privacy and Data Protection Issues of Biometric Applications: a Comparative Legal Analysis*, Springer, Dordrecht, 2013, 343; S. TOSZA, 'Online social networks and violations committed using I.T. Identity fraud and theft of virtual property' (AIDP Global Report), *Revue Internationale de droit penal* 2013, Vol. 84, n. 1, 115.

45 B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 2; M. GERCKE, 'Internet-related identity theft. A discussion paper', 8, www.coe.int/cybercrime.

46 J. CLOUGH, *Principles of Cybercrime*, Cambridge, Cambridge University Press, 2010, 6.

47 FIDIS 5.2b, 78. That does not mean that 'offline' procedures are flawless or secure. We just want to note that other security issues arise when these procedures are automatized and that the law has to deal with this shift.

48 T. CASSUTO, 'Usurpation d'identité numérique, *AJ Pénal* 2010, 220.

easy to hide it (using proxies or other anonymizing tools). Thirdly, its communication is routed through a number of jurisdictions, leaving only digital traces which are volatile and can easily be removed. Some jurisdictions do not regulate identity theft or the retention of data and provide 'digital safe havens' to offenders. Fourthly, the risk of detection is very low. Many abuses are not reported by the victim and even if they are, law enforcement has very few adequate means to address it. Simply identifying the offender is problematic because it requires international legal assistance and relies on the cooperation of ISPs. Finally, the ubiquitous nature of the Internet and its global reach, the transferability of data and the fact that the data are often in the hands of (multiple) third parties challenge the way to deal with the problem *after* the identity-related crime has been committed and to redress the situation. Law enforcement faces many difficulties to take offending information offline (jurisdictional problems, technical issues, effectiveness…) and companies are driven by their own economic interests. The victim is therefore confronted with plenty of problems to recover his 'compromised' identity.

DIGITISATION AND PERSONALISATION OF IDENTIFICATION. – The importance of physical, biometric information as an identifier has increased. At the same time, the digitisation of this information and its processing has resulted in an anonymization of the identification process. These two evolutions have an impact on the concept of identity and on the importance of its protection.[49]

The combination of digital identification information, like an e-ID, backed up by (digitally stored) biometrics not only increases the risk of identity-related crime but also the damage of this crime. It makes it more difficult for the victim to prove the abuse of his identity[50], to end the crime and to recover his or her compromised identity. Victims have no control over this information, reason why they lack possibilities to restore inaccuracies.[51]

The paradox therefore is that the more the link between an individual and his or her identity is being strengthened, the more the identity is endangered if another person gets

---

49 U.R.M.Th. DE VRIES, H. TIGHELAAR, M. VAN DER LINDEN and A.M. HOL, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid, Universiteit Utrecht 2007, 24.

50 FIDIS D12.7, Executive Summary.

51 U.R.M.Th. DE VRIES, H. TIGHELAAR, M. VAN DER LINDEN and A.M. HOL, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid, Universiteit Utrecht 2007, 24-25.

hold of this link.[52] This paradox specifically counts for biometrics: once biometric features are compromised, they are not easily revoked or changed. Their utility is therefore inherently limited. One can have a hundred passwords, but only ten fingers.[53] Moreover, in the digital world identification processes and protection mechanisms can easily be circumvented (via physical means or even 'voluntary' disclosure of information by the victim). No system is 100 % safe.[54] Therefore, we have to look further than the mere prevention and also develop an adequate criminal law framework to end the abuse and to limit further damage (detect – respond – recover).

THE CHALLENGE: PROTECTION OF IDENTITY AS AN 'IT-PERSONALISED' KEY. – In sum, regarding the practical matter of identification, we see several evolutions:

- A digitisation of primary identification information: a shift from physical, paper identity documents to 'e-ID';
- This comes with a shift from identification on the basis of what a person possesses and knows to what a person is, or at least a combination of the three. A classic example is the increasing reliance on biometrics in the identification process.[55]
- A merger between such digital identification information and 'personal' access keys into an 'IT-personalised key', a tool to verify, authenticate and authorize.

The scope of the research is to protect identity, understood as such an 'IT-personalised key'. This is necessary because of the growing importance of this function in today's information society. Previously, only physical objects, such as paper documents and cards, were suitable to verify and authenticate one's identity and to get access to certain well-defined facilities, like social security, tax on web, personal medical files, etc. Nowadays, we see that digital identification information is increasingly being used as a key to get access to a whole range of facilities, i.e. the use of e-ID to get access to a chatroom, the use of digitised fingerprints to access a smartphone, cash transfer apps, e-commerce, etc. Where a key (to open a door or a safe) used to be 'identity-neutral', this key is now connected to identity information in order to improve the identification process. These shifts may

---

52 FIDIS D12.7, Executive Summary.

53 E. KINDT, *Privacy and Data Protection Issues of Biometric Applications: a Comparative Legal Analysis*, Springer, Dordrecht, 2013, 348; FIDIS, D.5.2b, 93.

54 N. VAN DER MEULEN en B.-J. KOOPS, 'Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude', *NJB* 2012, 5.

55 FIDIS D5.2b, 81.

simplify commercial and daily life and may reduce time-consuming identity checks. They however also increase the risks of the abuse of one's identity. One's identity becomes more attractive to appropriate because it can be used for multiple purposes. Its value thus increases.

Due to the registration of identification information in automated systems, the identity becomes more exposed to appropriation and abuse.[56] We also see a shift from traditional and laborious identity document fraud and forgery to 'quasi-effortless' online forms of fraud, like IT-forgery, hacking,… Especially single and 'stable' identification data (like passport numbers, social security numbers…) that are not sufficiently protected by secure systems are vulnerable.[57] This leads to an increase of identity-related crimes.

IDENTIFYING THE KEY ISSUES. – Tackling identity-related crime, and notably a very specific form of this phenomenon: identity theft (*cf. infra*), confronts us with some particular difficulties. First of all, identity-related crime can cause different types of social and economic harm, such as distrust in identification and authorization procedures, especially in an online environment. This affects the trust in e-commerce and other online services (such as e-banking, e-commerce and e-government) in general. To restore trust and to ensure the privacy of their clients, these companies have to invest in secure IT-systems, IT-management, etc. Due to the risks created by the automated processing of identification information, they are thus confronted with new responsibilities and liabilities. The increasing distrust may also lead to stronger and tighter security measures, such as logging and profiling. The financial and administrative burden of these measures will eventually lie on the end user or client. They also have to carry other costs, such as loss of convenience, privacy and liberty.[58] Strong security measures that at the same time ensure the identification as well as the privacy and liberty of citizens are thus the challenge. This is an important element in the context of the Project as it emphasizes the possibility and importance of anonymous or semi-anonymous identity checks.

---

56 B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 2.

57 I.e. the Social Security Number in the United States. M. GERCKE, 'Internet-related identity theft. A discussion paper', 6, www.coe.int/cybercrime.

58 FIDIS 5.2.b, 66 - 69.

Furthermore, identity-related crime (and identity theft in particular) causes specific harm to the rights and freedoms of the *primary victim*, the person whose identity has been 'stolen' and is being compromised.[59] This makes the phenomenon so unique and complex. First of all, the perpetrator gains access to the personal sphere of the victim. By pretending to be the victim, he can also obtain all kinds of personal information that is normally only available to the victim. Secondly, the victim can be confronted with numerous problems, such as being addressed by creditors demanding payments for goods or services that he or she has never ordered, being blacklisted and rendered unable to obtain certain services (loans, airline tickets, etc.), even being wrongfully accused of or arrested for crimes committed under the cover of his or her identity.[60] This affects the victim's dignity, autonomy and privacy.[61] He or she can thus suffer different types of damage, financial and non-financial: money that has been stolen, costs to reconstitute one's name (e.g. starting a criminal investigation, defending oneself in procedures started by creditors), reputational damage, psychological damage, time and effort spent in taking restorative action and damage from being mistakenly associated with crimes (e.g. false accusation or even imprisonment).[62] Once their identity has been compromised, victims of identity theft spend enormous amounts of time, money and effort to clear their name.[63] For them it is therefore important to clean up the mess as soon as possible and limit further damage from occurring.[64]

Note that the rectification of this harmful situation is also crucial for the entity that has to verify the identity of somebody (the 'identity verifier'). We cannot expect from the identity verifier to make a 'Solomon judgement' when somebody claims an identity or denies the alleged behaviour alleging identity abuse. The identity verifier often has no other choice

---

59 CSES Impact Assessment, 171.

60 M. CHAWKI and M.S. ABDEL WAHAB, 'Identity Theft in Cyberspace: Issues and Solutions', *Lex Elektronica* 2006, Vol. 11, n° 1, 4.

61 FIDIS 5.2b, 69.

62 J. VAN WILSEM, 'Slachtofferschap van identiteitsfraude. Een studie naar aard, omvang, risicofactoren en nasleep', *Justitiële Verkenningen* 2012, afl. 1, 102; RAND Study, viii; FIDIS 5.2.b, 67.

63 One harrowing example of the aftermath of identity 'theft' is illustrated by the Dutch case or Mr. Kowsoleea. His identity was abused for many years by a drug criminal. As a consequence, he was arrested several times and was 'blacklisted' as a drug criminal. Cf. N. VAN DER MEULEN en B.-J. KOOPS, 'Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude', *NJB* 2012, 1414.

64 Cf. Roadmap on a Legislative Proposal on criminalisation of identity theft, http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2011_home_013_identity_theft_en.pdf.

than to rely on the available identification means and has no or insufficient instruments to check the veracity of the identity match. This affects society as a whole, as it must be able to count on the authenticity of identification means and builds further upon that assumption.

The Project will therefore propose innovative techniques to create a real strong link between the citizen and his or her primary identity. Such a link is necessary, not only to *prevent* the crime from being committed but also to *limit* further damage and to *restore* the situation after identity abuse. Specific challenges should indeed be taken into account and covered. One such issue which has been underestimated, is the aftermath of identity abuse for persons whose identity has been compromised and their lack of control over the information. Most countermeasures focus on making it more difficult to obtain or access identification information. These efforts are however faced with a dilemma: at the one hand the identification information should be held confidential in order to avoid abuse, on the other hand it is needed as a reliable access key to certain services and is therefore available to many actors, making secrecy impossible.[65] Moreover, the key identification information (e.g. name, social security number, biometric data) usually remain the same throughout a person's lifetime. Therefore, once compromised, it will be very difficult to restore them.[66]

Finally, the 'e-aspect' confronts the victim with extra difficulties, such as:

- The online context often implies remote communication. The perpetrator can therefore commit the crime from any part of the world, thereby transferring communication through servers and computers located in several countries. This generates specific cross border issues, such as jurisdiction conflicts, mutual legal assistance problems, extradition issues,… They can strongly complicate criminal investigations and undermine the effectiveness of territory-based policies[67];
- Online information is largely intangible and volatile. Once compromising information is transferred online, it is very difficult to take it offline, and thus to

---

65 L. LOPUCKI, 'Human Identification Theory and the Identity Theft Problem', *Texas Law Review* 2001, 94; U U.R.M.Th. DE VRIES, H. TIGHELAAR, M. VAN DER LINDEN and A.M. HOL, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid, Universiteit Utrecht 2007, 25.

66 L. LOPUCKI, 'Human Identification Theory and the Identity Theft Problem', *Texas Law Review* 2001, 94.

67 M. CHAWKI and M.S. ABDEL WAHAB, 'Identity Theft in Cyberspace: Issues and Solutions', *Lex Elektronica* 2006, Vol. 11, n° 1, 8.

end the crime and limit further damages. Online identity theft can therefore exceed offline identity theft in scale of harm[68].

- Because the online environment is dominated by private entities, such as internet service providers, in fighting illegal activity online public-private partnerships became a growing trend in the past few years.[69] Tackling identity theft requires participation of the private sector, governments cannot handle it alone. Private sector interests, such as business costs and reputation, may collide with the victim's interests. Therefore Regulation may sometimes be needed to force these entities to cooperate. Lawmakers are however striving to find ways to develop regulatory frameworks which reconcile the economic interests of these private entities with those of the victims of online crime. Due to the complexity and variety of the online environment, regulatory domains often overlap, creating confusion over which applies. Lastly, enforcing such cooperation in a global, digitised context has proven to be challenging (*cf. infra*);
- The online context is a playground for identity 'thieves' because they can commit the crime with great speed and profit and a low probability of getting caught. Online perpetrators can very easily create a fictitious identity and use technologies to conceal their identity (sometimes by abusing someone else's) or their real location. The internet also makes it easy to gather identification information from unsecured or poorly secured information systems or even open sources, such as social media accounts with limited privacy settings. It is also an interesting market place to sell 'stolen' identification information to interested third parties. The identification information is therefore easier to 'commercialise';

In sum, the online context makes it easier and more attractive to commit identity theft, to profit from it and to escape from prosecution. Mere financial compensation will not suffice to restore abuse victims.[70] An active legislative and supervisory policy may be necessary in this context.

---

68 *Ibid.* 5.

69 T. TROPINA, 'Fighting money laundering in the age of online banking, virtual currencies and internet gambling', ERA Forum 2014, 80.

70 Cf. P. DE HERT, 'Systeemverantwoordelijkheid voor de informatiemaatschappij' in *De Staat van Informatie*, Amsterdam, Amsterdam University Press, 2011, 49.

II Criminalisation of identity theft: a matter of criminal policy

1 EU initiatives with regard to criminalisation of identity theft

EU INITIATIVES. – In short, identity-related crimes relate to the security of documents and IT-systems. The perpetrator profits from weaknesses in the identification process or the lack of care with personal data. The digital context poses extra difficulties with regard to the detection, prosecution and ending of the criminal behaviour.

One way to tackle the phenomenon is to adopt specific criminal offences. In the recent years, the EU has paid attention to identity-related crime, and more specific identity theft. In 2010, DG Home Affairs launched a legislative proposal on criminalisation of identity theft.[71] In this context, a comparative study on the legislation of EU Member States was prepared.[72] It does not directly support the conclusion that there is need for EU action. Despite the lack of a single pan European instrument, the study identified no instances in which an act of identity theft could not be punished at national level.[73] No clear regulatory gap could be identified as this issue largely depends on how identity theft is defined and how broadly one wishes to criminalise specific behaviour, especially in the absence of harm to the victim and outside the context of existing crimes.[74] The study suggests to concentrate on non-legal responses, such as awareness campaigns, efficient reporting mechanisms etc. Furthermore, as long as there is no common understanding of 'identity theft', drafting a clear common definition will be extremely challenging. There is also a substantial risk of overlap with existing criminal provisions, such as fraud and forgery. It is therefore more important to ensure consistency in national criminal law enforcement, rather than to create a new offense. Based on these observations, the study concluded that any regulatory initiative aiming to introduce new criminal concepts into national criminal

---

71 Roadmap on a Legislative Proposal on criminalisation of identity theft, http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2011_home_013_identity_theft_en.pdf.

72 RAND Study (*cf.* footnote 18).

73 *Ibid*. 114.

74 *Ibid*. 115-116.

law should undergo a formal regulatory impact assessment.[75] An Impact Assessment was subsequently undertaken for DG Home in order to inform the Commission's decision on whether criminal law measures in the field of identity theft are appropriate at the EU Level. This study supported the idea of the need for a Directive including a common definition of identity theft as a framework for further initiatives, including possible criminalisation. The best policy option would be to adopt a Directive on identity theft focussing on primary victims combined with non-legislative actions such as the establishment of a platform for victims and specialists to exchange experience and knowledge, information exchange and awareness raising and the adoption of a common definition of identity theft.[76] The development of such comprehensive legislative proposal has however not yet been finished.

In the meanwhile, a specific form of identity abuse has been included in the Directive on attacks against information systems (further 'the Directive on Cyber-attacks'[77]) from 2013, as an optional aggravating circumstance of system and data interference.[78] Article 9, 5° states that the Member States shall take the necessary measures to ensure that when such offences are committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with national law, be regarded as an aggravating circumstance, unless those circumstances are already covered by another offence, punishable under national law. The Directive on Cyber-attacks only seems to cover one specific type of identity abuse, namely committing illegal system or data interference by abusing somebody's personal data thereby causing harmful consequences for the primary victim. The Directive leaves the discussion on Union-wide criminalisation of identity theft and other identity-related offences to be decided in the future. Consideration 14 states: '*Setting*

---

75 *Ibid*. 119.

76 CSES Impact Assessment, 175-177.

77 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, 8-14.

78 The Commission will facilitate implementation by means of a contact committee where experts from Member States can exchange information on national implementation measures and discuss challenges that may arise. The European Cybercrime Centre (EC3) within Europol also focuses on the fight against identity theft and fraud, including through its Focal Point Terminal, which deals with non-cash payment fraud, one particularly harmful form of identity theft. *Cf.* http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2014-000896&language=EN

up effective measures against identity theft and other identity-related offences constitutes another important element of an integrated approach against cybercrime. Any need for Union action against this type of criminal behaviour could also be considered in the context of evaluating the need for a comprehensive horizontal Union instrument.'

FIRST STEP: COMMON UNDERSTANDING. – As pointed out by the RAND Study and the Impact Assessment, the first step in adopting a policy is to come to a common understanding of the phenomenon. The main issue in the debate on criminalising identity theft as a discrete offence, does not seem to be the lack of criminal law provisions but, on the contrary, the multitude of applicable criminal law provisions and the disparate approaches to the phenomenon. Most Member States seem to approach identity theft as a preparatory act of *fraud*, thereby focussing on the subsequent illegitimate use made of the identity (e.g. committing financial fraud like skimming). Identity theft is therefore not always criminalised in its own right.[79] In this point of view, identity is not regarded as a target but as a means to facilitate other crimes. The question therefore arises whether identity is a specific legal interest in need of protection, legitimising a separate criminalisation. We will examine this on the basis of existing legal studies and will further analyse the legal interests in need of protection. We believe this can create a clear framework for further regulatory action.

79 CSES Impact Assessment, Executive Summary.

2 Defining the illicit behaviour and the legally protected interests

2.1 Identity theft and identity fraud: a demarcation

ID THEFT *VERSUS* ID FRAUD? – The development of a policy to combat the abuse of identity starts with the demarcation of the phenomenon[80], which is multifaceted and complex. In literature and common parlance, it is often referred to as 'identity theft'. This term might be confusing because it treats identity as a property concept instead of an informational concept.[81] 'Theft' normally requires that the owner is deprived of the good, reason why only tangible goods could fall within the scope of the criminal offence (*cf. infra*). 'Theft' further only seems to refer to the act of the illegal *acquisition* or *gathering*. In identity abuse situations the initial gathering can however be lawful but its further use can be unlawful. The abuse of identity is therefore much broader a problem and can cover a wide range of illegal activities, such as the unlawful access, possession, transfer, process, disclosure or use.[82]

Due to the multiplicity and variety of possible illegal acts, it is very difficult to find a term which covers the entire phenomenon of identity abuse. We therefore prefer to use the container concept 'identity-related crime' to refer to the problem. Identity-related crime can be defined as '*all punishable activities that have identity as a target or as a tool*'.[83] KOOPS *et al.* stress that this phenomenon should be understood '*as a distinct, novel category of crime, because combating these crimes requires special knowledge and understanding of IMS* (the information management systems) *and their vulnerabilities, as victims suffer from these crimes in special ways, for instance, by being blacklisted, and because public awareness is low and should be raised*.'[84] To demarcate the problem, they take the perspective of an

---

80 Cf. U.R.M.Th. DE VRIES, H. TIGHELAAR, M. VAN DER LINDEN and A.M. HOL, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid, Universiteit Utrecht 2007, 271 p.

81 RAND Study, 5.

82 Cf. i.e. the criminalisation of identity theft in 18 U.S.C. §1028 en §1028A; M. GERCKE, 'Internet-related identity theft. A discussion paper', 13, www.coe.int/cybercrime.

83 E.g. human trafficking, drug trafficking. Here the identity facilitates the crime but is not the main target or principal tool. B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 8.

84 B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 9.

observer of the identification process and look at possible mismatches between the identify information (the 'identifier') and the identity during the identification process which leads to unjust authentication.[85]

Unlawful use of identity can be divided into three main categories[86]:

- Unlawful *identity obstruction*: an identifier is intentionally deleted (identifier erasure) or the link fails to be made due to an intentional act (identification obstruction) e.g. the deletion of a patient record with the goal to destroy that person's identity[87], intentionally blocking or erasing someone's identification data, destroying an identity card, the taking away of someone's passport by a human trafficker,… ;
- Unlawful *identity restoration*: the 'compromised' link is being wrongfully restored or re-established, e.g. somebody claims to have lost his identity card in order to receive a new one. The old one can be handed over to someone to abuse it, e.g. to human traffickers; [88]
- Unlawful *identity change* or **identity fraud**: the fraud or any other unlawful activity committed with identity as a target or principal tool[89], e.g. the use of someone's identity to harm that person's reputation, provide a false name to let someone else in for a criminal offense. With regard to criminal activities, this is the most important category. It has four subcategories:
    - Unlawful *identity delegation*: when somebody provides his identity to another person, e.g. gives his or her professional fuel card to a friend so that he can fill up his car. This type of crime is conducted with consent of the original identity bearer;
    - Unlawful *identity exchange*: when two persons switch identity, e.g. somebody visits an inmate in prison and they swap places. This also

---

85 An individual can be unjustly identified but also unjustly *not* identified. This mismatch can both be intentional and unintentional, lawful and unlawful (*ibid.* 6). We will only focus on the unlawful cases.

86 Cf. FIDIS D.5.2b, 56.

87 Deletion without that goal would amount to *data interference* or *data forgery*.

88 If it is not the original identity bearer who claims to have lost his identity card, this would amount to unlawful identity change or identity fraud (*cf. infra*). KOOPS et. al. give as an example of unlawful identity restoration a physician who loses his licence, nonetheless reassumes his practice. This usually involves roles rather than identifiers.

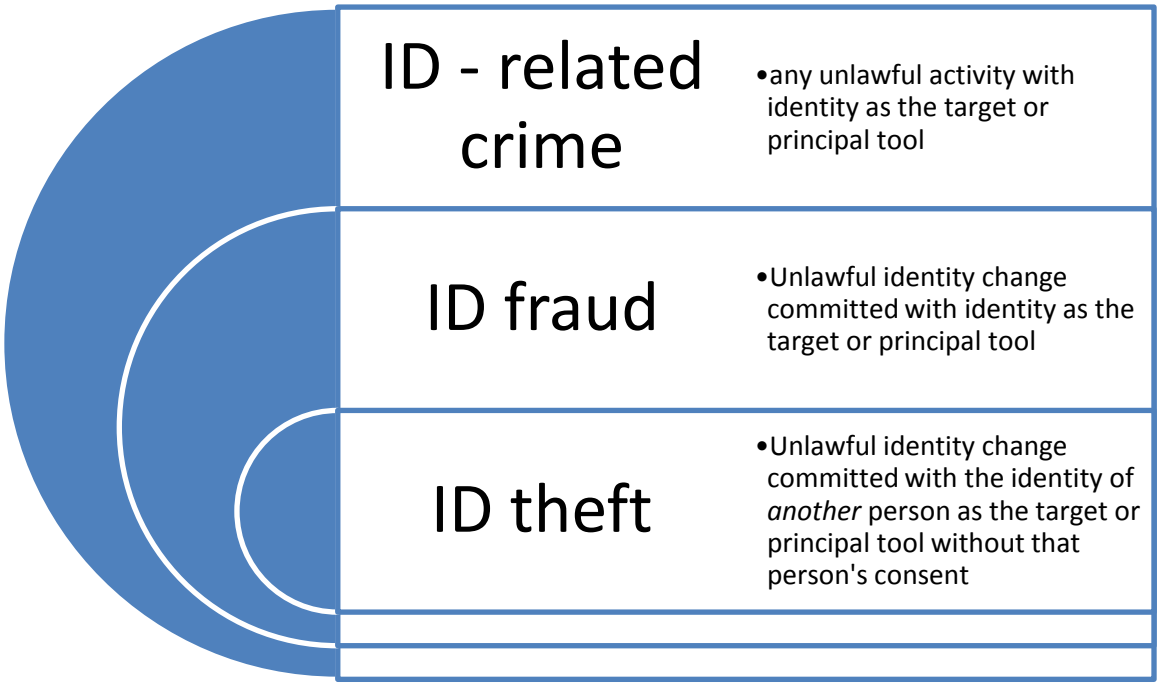
89 B.J. KOOPS and R. LEENES, 'ID theft, ID Fraud and/or ID-related crime. Definitions matter', *Datenschutz und Datensicherheit* 2006, Vol. 30, no. 9, 553-556.

happens with mutual consent of the persons whose identities have been exchanged;

- Unlawful *identity creation*: somebody creates a fictitious identity, e.g. using a fake profile to lure someone into false beliefs. In this situation, there is no abuse of the identity of another person;
- Unlawful *identity takeover* (or *identity usurpation* or **identity theft**): somebody takes over the identity of another person. Here the identity of that other person is *being compromised*, e.g. somebody pretends to be his twin brother to let him in for a criminal offence, someone forges a credit card using someone else's 'stolen' credit card data, someone uses another person's mail account to send spam, …

In the first two categories of identity fraud, the original identity bearer contributes to the abuse or at least condones it. In the third category the identity of another person is not at stake. The last category is really the key point of interest of our research: the fraud or any other unlawful activity where the *identity of another person* is used as a target or principal tool without that person's consent. Please note that a fictitious identity can also be created with identification information of different existing persons. In that case we have multiple cases of identity theft. This type of behaviour thus falls under the fourth category.

To resume, identity theft must be understood as a subcategory of the broader concept of identity fraud. We can represent the different types of abuse of identity in the following scheme:



IDENTITY FRAUD AS A TWO-PHASED PROCESS. – The ways to *target* or obtain identification information (the *modi operandi*) differ. The perpetrators can get hold of it through physical methods, by clever social engineering and through outsider and insider attacks on IT-systems.[90] The motivation to obtain and further use that information can also be very diverse. Identity fraud can revolve around the use of another person's or a fictitious identity to commit other crimes, such as terrorism, embezzlement, credit card fraud, money laundering, drug trafficking, traffic offences, human trafficking, distribution of illegal content, social security fraud etc. The perpetrator uses the identification information *as a tool* to hide his or her own identity and to avoid legal consequences, for example a wanted person uses a false licence plate. Sometimes identity fraud, especially identity 'theft', aims to harm the bearer of the identity. In this case, that person is the *target*, not the identification information as such, e.g. creating an embarrassing Facebook profile in someone else's name to harm that person ('cyberbullying').

The only correlation between these acts seems to be that they can relate to one or more phases in the commission of identity fraud.[91] Identity fraud is often described as a two-

---

90 See for detailed studies on the *modi operandi* B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 11; Verizon 2014 Data Breach Investigations Report which contains a very comprehensive study on the types of attacks.

91 M. GERCKE, 'Internet-related identity theft. A discussion paper', 19-20, www.coe.int/cybercrime.

stage process: the creation of a false identity and its use for a specific purpose.[92] The initial phase involves the gathering of identification information and the creation of the false identity. This can be done by means of unauthorised access to IT-systems containing identification information and the copying of such information (outsider threat), through the abuse of authorised access to IT-systems or illegal disclosure to unauthorised third parties (insider threat), but also through theft or copying of physical identity documents,… This phase also includes interaction with the identification information, like possessing, transferring, processing or selling of identification information, e.g. falsification of identity documents, falsification of number plates, data protection breaches, … In a second phase, the perpetrator *continues* the fraud by using this false identity in some unlawful way (e.g. in the context of human trafficking, money laundering, terrorism,…).[93]

ACCURATELY DEMARCATING IDENTITY FRAUD. – On the basis of a thorough comparative analysis of multiple definitions in several countries, DE VRIES *et al*. have developed a working definition of the concept of identity fraud. They define it as '*obtaining, taking, possessing or creating false means of identification intentionally (and) (unlawfully or without permission) and to use them to commit unlawful behaviour or to have the intention to do so*.' False means of identification are those that do not truthfully identify the person who uses it.
Identity fraud is a specific form of fraud. Two elements are constituent for identity fraud: the falsehood and the deceit. Identity fraud can be qualified as a form of falsehood in identification means for the purpose of deceit in some form.[94] Deceit is thus the goal or result. On the basis of their analysis, they draw the following conclusions.[95]

- First, it is irrelevant whether the false means of identification refer to an existing, deceased or totally fictitious person. *False* means of identification are those that do not truthfully identify the person who uses them. What matters is the pretence of *another* identity, in other words: the alteration of the truth. In the identification

---

92 U.R.M.Th. DE VRIES, H. TIGHELAAR, M. VAN DER LINDEN and A.M. HOL, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid, Universiteit Utrecht 2007, 199.

93 B.J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 11.

94 U.R.M.Th. DE VRIES, H. TIGCHELAAR, M. VAN DER LINDEN en A.M. HOL, *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, 2007, 16.

95 *Ibid.* 16 – 20.

context, it does not always matter *who* a person is, as long as it is the 'right' person.[96] The manipulation of *another person's* identity is therefore not essential. When someone else's means of identification are indeed compromised, this qualifies as identity *theft*, a specific subcategory of the broader concept of identity fraud. Identity theft expresses that there is a (primary) victim of a falsehood in respect of his or her means of identification. Identity fraud emphasizes more the element of deceit, or violation of public confidence (*cf. infra*).

- Secondly, identity fraud is the obtaining and (ab)using of some *means* of identification. Being untruthful about one's identity without (ab)using any means of identification does not amount to identity *fraud*. As we have seen above, means of identification can take the form of intangibles, such as a name, credit card data, biometric data, or tangibles, such as a passport or birth certificate. *Naming* a particular type of means of identification is not necessary to demarcate identity fraud. Means of identification can refer to documents, data or any other data carrier. These means are however the object of the fraud and their different forms can be relevant for policy development, such as the elaboration of countermeasures.
- Thirdly, the meaning of 'identity' is very context-bound. Most of the time it refers to a civil, bureaucratic identity. As we have seen above, we understand identity as the set of elements that allow a person to be qualified as a 'legal subject' to whom the government or other parties can attribute specific acts in a reliable way. This indeed refers to a bureaucratic identity.
- Fourthly, identity fraud is a two-phased criminal process. A distinction can be made between actions which relate to the obtaining, taking, possessing, creating or handing over of identification means on the one hand (the initial phase) and actions existing in using them for unlawful purposes (the subsequent phase). In the initial phase the means of identification can be targeted in various ways, e.g. through forging, stealing, unlawfully accessing a computer system etc. Some acts in this initial phase may however not be unlawful as such, e.g. shoulder surfing or dumpster diving. The means of identification can thus also be lawfully obtained, for instance from public sources.[97] In that case, it is the subsequent use of that

---

96 J. GRIJPINK, 'Identiteitsfraude als uitdaging voor de rechtstaat', *Privacy en Informatie* 2003, 148 – 153.

97 For instance taking someone's picture (legal) to subsequently use it for a fake social media profile (illegal).

information to create a false identity which makes the behaviour unlawful. DE VRIES *et al.* conclude that referring to actions contributes to demarcating identity fraud. Yet, the *ways* of obtaining, taking, possessing or creating, for instance through forging, stealing, hacking etc., are however not decisive. Most of the time, these particular type of actions are indeed criminalised through a range of offences. This is however not necessary, what matters is the unlawfulness of the subsequent use. In other words, *what happens afterwards* with the identification means is constituent for identity fraud. This also seems to emphasize the importance of a specific intent in the criminalisation of the initial phase of identity fraud and the requirement of some harmful result or risk of such harmful result (*cf. infra*).

- This relates to the fifth conclusion, that the carrying out of the *subsequent* behaviour or even attempting to carry it out is the very essence of identity fraud. The mere possession of identification means therefore does not suffice. Identity fraud revolves around the manipulation of the identification process.
- Lastly, it does not matter whether the fraud takes place vis-à-vis a private party (horizontal relationship) or a public authority (vertical relationship). Indeed, in both relationships, similar identification means can be used, especially since secondary identities are often derived from primary identities.

In short, the essential elements of identity fraud are: 1) the use of *false* means of identification (the element of falsehood) and 2) the *two-phased* criminal process, in particular the abuse in the subsequent phase (the element of deceit).

The fictitious identity can indeed be used for a variety of types of unlawful behaviour (financial fraud, money laundering, human trafficking…). In our opinion these subsequent 'result acts' should, however, not serve to demarcate the phenomenon of identity fraud. That should be considered as a separate 'intermediary act'. Otherwise, identity fraud as a phenomenon would become excessively context-dependant. We can compare this to forgery offences, where the forging and subsequent use of the forged object are usually criminalised in general, regardless of the specific context in which the use took place. Forgery is a so-called 'intermediary offence': behaviour that facilitates other crimes ('result offences') but that is also criminalised as a separate offence. We believe that this also indicates the importance of a specific intent requirement for the subsequent phase of the unlawful use of the means of identification.

2.2 Legal interests at stake

RATIO LEGIS AS OUR REFERENCE POINT. – Detecting the legal interests at stake is the second step in further demarcating the phenomenon and analysing the criminalisation. We have seen that the *modi operandi* and the concrete motives can be very diverse, reason why they are difficult to use to detect loopholes in existing law. Instead of focussing on possible ways of committing identity fraud, we will use the *ratio legis* of the criminalisation as our reference point. With *ratio legis* we mean the aim and purpose of the criminalisation, which at the same time justifies and limits the criminalisation of specific behaviour. The *ratio legis* can therefore be a guideline for policy makers, as well as an interpretative tool for the Courts.[98] In German Criminal Law, this purpose of a criminalisation is indicated as the (subsidiary) protection of a legal interest or *Rechtsgut*.[99] This is more or less comparable to the *harm principle* in common law.[100]

2.2.1 Legal interests in the initial phase

INFORMATION PRIVACY. – As identification information is linked to individuals and often reveals information about their personal life, privacy immediately pops up as the logical legal interest to in need of protection (art. 8 ECHR and art. 7 EU Charter). The concept of privacy is very hard to define and demarcate. In general it is often described as '*the right to be let alone*'. It encompasses various aspects, such as the right to personal life, physical and psychological integrity, communication privacy and information privacy. Especially information privacy is important in this context. It refers to the right of an individual to exercise a substantial degree of control over personal information and its use, including the collection and circulation thereof.[101] In *Goodwin*, for instance, the ECtHR stated that '*protection is given to the personal sphere of each individual, <u>including the right to establish</u>*

---

98 M.D. DUBBER, 'Theories of Crime and Punishment in German Criminal Law', *Am. J. Comp. L.* 2005, Vol. 53, 695.

99 C. ROXIN, *Strafrecht. Allgemeiner Teil. 1 : Grundlagen, der Aufbau der Verbrechenslehre*, München, Beck, 2006, 16.

100 N. PERŠAK, *Criminalising Harmful Conduct: The Harm Principle, Its Limits and Continental Counterparts*, Dordrecht, Springer, 2007 104. K. SEELMAN, 'Rechtsgutskonzept, 'Harm principle' und Anerkennungsmodell als Strafwürdigkeitskriterien' in R. HEFENDEHL, A. VON HIRSCH en W. WOHLERS, *Die Rechtsgutstheorie: Legimitationsbasis des Strafrechts oder dogmatisches Glasperlenspiel?*, Baden-Baden, Nomos Verlagsgesellschaft, 2003, 262.

101 E. KINDT, *Privacy and Data Protection Issues of Biometric Applications: a Comparative Legal Analysis*, Springer, Dordrecht, 2013, 214.

details of their identity as individual human beings'.[102] 'Personal information' refers to aspects of someone's private life, hence *intimate* information (e.g. sex life, health), but can also include information and data about unique human characteristics which allows someone to be identified by others, such as biometric data.[103] The notion of private life or personal sphere is determined from case to case and its scope depends on the specific facts and circumstances of the case. What we retain is that the ECtHR has recognised the *right to identity* as an aspect of private life in several cases, also in interaction with others and in a public context. From the case law, we can conclude that this right also protects the individual from (*improper) identification*.[104]

In addition to article 8 ECHR, each identifier can qualify as the legal concept of 'personal data' insofar as they relate to an identified or identifiable individual. Data relates to an individual, if it refers to the identity, characteristics or behaviour of an individual, or if such information is used to determine or influence the way in which that person is treated or evaluated.[105] It is not required that the data can lead to a direct identification or that the individual is easily identifiable (e.g. the full name of an individual). It suffices that the data may indirectly lead to an identification through a combination of the different elements. The processing of personal data is regulated by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter 'the Data Protection Directive').[106] This legal framework regulates the relationship between the original identity bearer and the controller of the personal

---

102 ECtHR 11 July 2002, *Christine Goodwin v. United Kingdom*, §90.

103 ECtHR 15 January 2009, *Reklos and Davourlis v. Greece*; ECtHR 4 December 2008, *S. and Marper v. united Kingdom*; E. KINDT, *Privacy and Data Protection Issues of Biometric Applications: a Comparative Legal Analysis*, Springer, Dordrecht, 2013, 243.

104 E. KINDT, *Privacy and Data Protection Issues of Biometric Applications: a Comparative Legal Analysis*, Springer, Dordrecht, 2013, 256.

105 Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data', WP 136, 20 June 2007, 10, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

106 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31 – 50. The Privacy Directive will be replaced by the General Data Protection Regulation and shall apply from 25 May 2018. (articles 94 and 99 Regulation No 2016/679 of the European Parliament and 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 95/46EC (General Data Protection Regulation), OJ 2016 L 119, 1.) This Regulation will establish a modern and harmonised data protection framework across the EU.

identification information. It determines the principles under which personal data, including identification information, may be lawfully collected and processed.[107] The non-respect of these obligations result in infringements of substantial privacy rights, which include offences such as the illegal processing, disclosure, dissemination, access to and storage of the personal data.[108]

It is worth stressing that data protection law starts from the assumption that *every type* of personal data is worth protecting, regardless of the context.[109] As such it differs from the right to privacy (art. 8 ECHR), the protection of which is often context-dependent and based on an assessment of the reasonableness of the expectation of privacy.[110] Data protection law acknowledges that certain types of personal data are more sensitive than others, such as racial or medical data, and therefore grants this special category of personal data specific protection.

Since the implementation of the Charter of Fundamental Rights of the European Union, data protection is embedded as an autonomous fundamental right (art. 8 EU Charter), in addition to the fundamental right to privacy (art. 7 EU Charter and art. 8 ECHR). Article 8 EU Charter sets the conditions and limits of data processing. An important consequence is that even if there are no specific privacy risks in the sense of article 7 EU Charter and article 8 ECHR, the personal data are still protected as a fundamental right and its processing is only allowed under the conditions of article 8 EU Charter.[111]

Insofar as the processing of this personal data is conducted in the electronic communications sector, they will also fall under the specific protection of electronic communications. The processing of personal data in the electronic communications sector is specifically regulated by Directive 2002/58/EC (hereafter 'e-Privacy Directive').[112] This

---

107 FIDIS D5.2b., 27.

108 M. CHAWKI and M.S. ABDEL WAHAB, 'Identity Theft in Cyberspace: Issues and Solutions', *Lex Elektronica* 2006, Vol. 11, n° 1, 23.

109 P. DE HERT, 'Systeemverantwoordelijkheid voor de informatiemaatschappij' in *De Staat van Informatie*, Amsterdam, Amsterdam University Press, 2011, 54.

110 This however does not mean that the reasonable expectation to privacy is a conclusive factor. A person subject under criminal proceedings for instance still has a right to privacy.

111 Art. 8.2 states that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access to data which has been collected concerning him or her, and the right to have it rectified.

112 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, Official Journal of the European Union, OJ L 201, 23.07.2002, 37 – 47 (amended by

Directive supplements the Data Protection Directive and is specifically aimed at protecting the fundamental rights of natural persons and in particular their right to privacy and the confidentiality of the communication, as well as protecting the legitimate interests of legal persons in the context of the electronic communications sector.[113]

It goes without saying that fraudulent collection and use result in violations of these Directives. The Directives oblige Member States to impose penalties on breaches of data protection legislation. Most forms of identity theft will thus constitute violation of data protection law.

PRIVACY AND DATA PROTECTION *VERSUS* PROPERTY. – The usual use of the notions 'fraud' or 'theft' seems to imply a need to protect property as a legal interest when somebody appropriates someone else's identification information. This is however anything but obvious. Identification information used to be linked to a physical item. As such, it was primarily based on matter: one could identify oneself by means of a physical identity card, a paper birth certificate… Nowadays, identification information can be stored and represented in various forms, either physically or digitally.

The taking away of physical objects containing identification information obviously results in a loss of property. The original identity bearers are deprived of their physical identity card, passport, credit card, etc. The protection of property will be a relevant legal interest at stake in the initial phase.

Yet, the victim does not lose the identification information represented by these physical documents. He or she can, for example, report the theft or loss and receive a new identification document, containing the same identification information. The identification information itself is *intangible* and suitable for *multiple use and storage* ('multiplicity'). These two specific characteristics diminish the suitability of traditional property offences such as theft. The traditional concept of property seems unfit for intangible objects which by nature cannot exclusively belong to one person.[114] The exclusive character of

---

the so-called 'Cookies Directive, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, 111).

113 Recital (12) .

114 Or a group of persons in case of joint ownership.

ownership is indeed intrinsically connected to the tangible and unique character of physical objects. Property offences are based on this materialistic concept of property. Applying them to cases of identity theft or fraud, where the original identity bearer does not necessarily lose his identity, requires a brave yet – in view of the sacrosanct legality principle in criminal law - questionable interpretation of the concept of property and the ways it can be affected.[115]

This does not mean that the law does not confer any rights upon intangible goods, inclusive property rights. This is exactly the case for intellectual property rights and privacy rights. Law can construe its own concepts to regulate relationships. Criminal law is even more unique as its conceptual autonomy of criminal law implies that Courts are not necessarily bound by the meaning given to legal concepts in other fields of law.

For information as a concept, the shift towards commercialisation is increasingly turning it into an economically valuable good.[116] For instance, the law confers (intellectual) property rights on databases containing personal consumer information to the collectors of that information. In doing so, it creates an important incentive for entrepreneurs to collect this information and to monitor their consumers. At the same time, those consumers retain a privacy right, not a property right, over that information. The law tries to find a balance between these two rights. European data protection law therefore confers certain obligations to the data controllers so that the privacy of the data subject is guaranteed.

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF IT-SYSTEMS AND DATA. – The same reasoning applies to digital identification information. Just as the information it represents, computer data are an intangible good. In order to avoid difficult legal discussions about the application of property offences, specific cybercrime legislation was introduced. Specific cybercrime legislation tries to fill in the gap left by property offences. Cyber-offences aim to protect the confidentiality, the integrity and the availability of computer systems and computer data ('CIA'- offences): illegal access to a computer system, illegal interception, data interference, etc. In doing so, they also grant an *indirect* protection to the personal data stored in or transferred through the IT-systems. They thus create a 'formal sphere of

---

115 R. VERSTRAETEN, 'Diefstal van computergegevens: revolutie in het strafrecht?', *RW* 1985-86, 227.

116 M. CHAWKI and M.S. ABDEL WAHAB, 'Identity Theft in Cyberspace: Issues and Solutions', *Lex Elektronica* 2006, Vol. 11, n° 1, 11-12.

secrecy' for the computer data and the information it represents.[117] Here we see a correspondence between CIA and information privacy. The Cybercrime Convention of the Council of Europe[118] and the EU Directive on Cyber-attacks aim to approximate the criminal laws of states in this area. As identity theft often exploits weaknesses of IT-systems in order to collect identification means, these cybercrime offences will play an important role in the criminalisation of identity theft.

2.2.2 Legal interests at stake in the subsequent phase

AUTHENTICITY IDENTIFICATION INFORMATION. – The legal interests mentioned above do not cover the actual function of the identification information in the process of identification (the 'IT-personalised' key, *cf. supra*). They mainly come in hand in the initial phase where they (directly or indirectly) protect identification information as the target. They are less relevant in the subsequent phase, the actual use of the identification information as a tool to get access to certain services (e.g. to pay, to get access to e-mails, to social security services…). The subsequent phase may indeed constitute the initial phase of another identity theft, if the perpetrator abuses the identity of another person (intermediate target) to obtain identification information of a third person (actual target).[119]

As already mentioned, the construction of an identity has undergone several evolutions which has some repercussions for the practical identification process. Identification used to be primarily based on official (paper) identity documents issued by states. Therefore, countermeasures are usually focused on the prevention of (identity) document forgery by implementing more security measures (e.g. biometrics, chips, codes, holograms…). Although this remains an important strategy, the digitisation of the identification process also comes with new risks and threats (*cf. supra*). Nowadays identity fraud does not only contain abuse of a *physical* identity document, but can be committed in various ways (*cf. supra*). This 'e-aspect' may not be ignored. The criminal law needs to be adapted to new technological evolutions which allow a more secure identification process, but *at the same*

---

117 M. CHAWKI and M.S. ABDEL WAHAB, 'Identity Theft in Cyberspace: Issues and Solutions', *Lex Elektronica* 2006, Vol. 11, n° 1, 25.

118 Convention on Cybercrime, Budapest 23 November 2001, ETS No 185.

119 F.i. the use of somebody's login and password to hack into an IT-system in order to obtain identification information of other persons, or the abuse of the social media profile of someone to send a request to the actual target, who is the friend or colleague of the first person.

time lead to an easier abuse of the identity and, what is more, make it more difficult to restore the identity.[120]

The very essence of identity fraud is that someone deliberately pretends to be somebody he or she is not. The perpetrator pretends that the other identity is his or her own, thereby misleading the identity verifier (human or machine). In case of identity fraud, two legal interests need protection. First, we must protect the *authenticity* of the identification information as a proof of an identity match, in other words trust in the information as a reliable identification tool. Identity fraud actually comes down to an alteration of the truth (deceit). The legal interest at stake therefore resembles the legal interest behind forgery offences. Typical for document forgery is that there is a violation of the confidence that society necessarily grants to certain types of documents.[121] These documents play an important role in society, reason why society must be able to count on their reliability. That reliability is called 'public confidence'. It is violated through the alteration of the truth in the document. With regard to identity fraud, the truth can be altered by means of manipulation of identity *documents or data*, but also by merely pretending to be someone else, using his or her identification information (e.g. look-alike fraud). Society however necessarily depends on the reliability of that identification information during the identification process (*cf. supra*). Next to this abstract, general *ratio legis*, the forgery offences also have a concrete, specific *ratio legis*, namely protecting the private interests of the victim who has been deceived by the false use of the 'stolen' identity (the secondary victim, *cf. supra*).[122] As set out above, this is the (natural or legal) person who is defrauded or otherwise harmed by the identity 'thief' because the secondary victim relies on the false identification means to provide services. The identity thief thus gains access to certain services or activities without right. The damages caused can vary from financial damage to moral damage, depending on the specific context. For instance when the impersonation is committed to commit social security fraud, the secondary victim (the social security agency) suffers (at least) financial harm. When the impersonation aims to hide criminal behaviour, e.g. avoidance of speeding tickets, the damage of the secondary victim is also primarily financial (the non-payment of fines). When the identification means are abused

---

120 S. REVEL, 'Précision sur la notion d'usurpation d'identité ou l'inexistence de l'ubiquité', *AJ Pénal* 2010, 218.

121 S. Van DYCK, *Valsheid in geschriften en gebruik van valse stukken*, Antwerp – Oxford, Intersentia, 2007, 27.

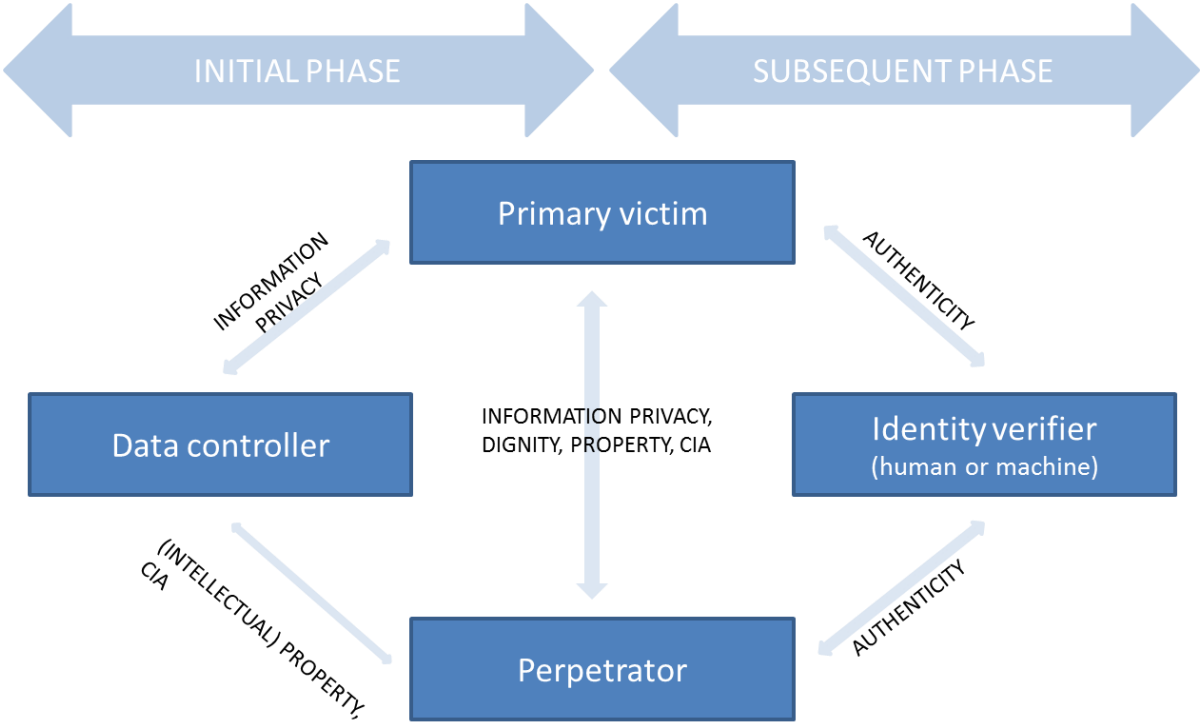
122 Compare it with counterfeiting money: when money is forged, the primary victim will be the state issuing the legal tender, the secondary victim the seller who gets paid with fake banknotes and is unable to use them for his or her payments.

in the context of human trafficking, e.g. to obtain asylum, the damage is non-pecuniary (the obtainment of an unlawful advantage).

DAMAGE TO ORIGINAL IDENTITY BEARER: PRIVACY AND DIGNITY. – Above we identified the potential damage caused by the abuse of someone else's identification information. It is clear that the private life of the original identity bearers and their dignity is again at stake when their means of identification are subsequently used against their will and can cause a very specific type of harm (*cf. supra*). As already mentioned 'identifiers' are part of someone's identity and thus one's personal life. When these identifiers are used against one's will, this abuse may violate the personal life and may also affect one's dignity, for instance when that person is blacklisted, confronted with numerous claims etc. This legal interest related to the primary victim in the *subsequent* phase is what sets identity theft apart from other types of forgery, where normally only the secondary victim suffers harm by the deceit. The impact of the identity theft on the privacy of the primary victim in the subsequent phase is the reason why identity theft asks for a specific approach.

3 Different strategies to criminalise

SCHEME. – The following scheme visualises the principal legal interests to be protected in the context of identity theft[123]:



DIFFERENT STRATEGIES TO CRIMINALISE. – One way to analyse the criminalisation is to examine whether the two phases are sufficiently covered by the current substantive criminal law framework. It will not take long to conclude that criminal law in general deals with different facets of the obtaining, creation and use of false means of identification. It can be a constitutive element of a particular offence. In Belgium and France, for instance, false identification means can be qualified as a fraudulent means, which is a constitutive element of the general offence of fraud ('*escroquerie*').[124]

It can also be criminalised through a range of existing offences which do not specifically address identity theft. The most relevant existing criminal law provisions in this context seem to be: 1) forgery offences (sometimes specifically of a travel document or

---

123 The secondary victim is not included in this scheme as our focus lies on the primary victim.

124 Article 313-1 French CC and art. 496 Belgian CC.

passport[125]), 2) data protection offences, 3) impersonation (the usurpation of a name, status, qualification, …), 4) cybercrime offences (IT forgery and IT Fraud, illegal access, illegal interception and data and system interference) and 5) the general fraud offence. All these different offences and their suitability for identity theft situations were already analysed in detail in other recent studies.[126] They reveal that the application of the different existing criminal law provisions depends very much on the focus. The Council of Europe for instance has not yet developed a comprehensive strategy towards identity theft or identity fraud. We do find a Guidance Note with regard to identity theft and phishing in relation to fraud.[127] While personally identifiable information of a real or fictitious person may be misused for a range of illegal acts, the Guidance Note only focuses on identity theft in relation to fraud. This entails the misappropriation of the identity of another person, without their knowledge or consent, in order to use it to obtain goods and services in that person's name. The Guidance Note examines how different articles of the Cybercrime Convention apply to identity theft in relation to fraud and involving computer systems, such as illegal access, illegal interception, computer related forgery, etc. It concludes that identity theft (including phishing and similar conduct) is generally used for the preparation of further criminal acts such as computer related fraud. Even if identity theft is not criminalised as a separate act, law enforcement agencies will be able to prosecute the subsequent offences.

Another approach is to adopt a 'specific' identity theft offence. It is interesting to examine whether one single specific legal provision addressing identity theft could contribute to the restoration of the compromised identity of the primary victim. For this, we will take a closer look at France, where new identity theft legislation was introduced in 2011 ('LOPPSI 2').[128]

---

125 E.g. art. 198 Belgian CC.

126 RAND Study, M. GERCKE, 'Internet-related identity theft. A discussion paper', 1-32, www.coe.int/cybercrime, S. TOSZA, 'Online social networks and violations committed using I.T. Identity fraud and theft of virtual property' (AIDP Global Report), *Revue Internationale de droit penal* 2013, Vol. 84, n. 1, 115-139.

127 T-CY Guidance Note #4 'Identity theft and phishing in relation to fraud' of 5 June 2013, https://www.coe.int/TCY. Cf. also M. GERCKE, 'Internet-related identity theft. A discussion paper', 1-32, www.coe.int/cybercrime.

128 La Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure ('LOPPSI 2').

FRANCE: NEW SPECIFIC OFFENCE. – Article 226-4-1 French Criminal Code (French CC), inserted in 2011, criminalises '*l' usurpation d' identité ou usage de données permettant d'identifier un tiers*'. This is the act of taking over or using another person's identity to disturb the peace of that person or another person or to affect his honour.[129]

Before introducing this 'specific' legislation, acts of identity 'theft' were (principally) criminalised through[130]:

- The use of a false name in a public act or '*usage d'un faux nom dans un acte public*' (art. 433-19 French CC)
- The usurpation of a civil status or '*usurpation d'état civil*' (art. 434-23 French CC).

So, even before 2011, identity theft was already criminalised to a large extent. These offences however did not seem to cover the entire phenomenon. Instead of modifying existing criminal law, France decided to introduce this new type of identity theft.

FALSE NAME IN PUBLIC ACT[131]. – Although the act described by article 433-19 French CC very much resembles the act of forgery ('faux'), the offense is nevertheless placed in a section XI entitled 'The damage to the civil status of persons' alongside bigamy, celebration of religious marriage before the civil marriage, breach of freedom of the funeral and the absence of a declaration of birth. The article therefore only envisages the taking ('prendre') of (a part of) a name other than the one assigned by the civil status or the changing ('changer'), alteration ('altérer') or modification ('modifier') of (a part of) the name assigned by the civil status in a public act. 'Name' has a broad meaning, it refers to family name, the surname, the prefix. The offence only criminalises the use of the false name in an authentic or public act or administrative document destined for the public authorities. However, the use of a false name in a non-administrative document can qualify as forgery in private writings (art. 441-1 French CC).

The offence does not require a specific intent. The knowledge that the used name is not legally one's own and the will to invoke it are sufficient. Therefore, even the use of a pseudonym in public acts is envisaged.

---

129 *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération.*

130 C. LACROIX, *Usurpation d'identité*, 2012, www.dalloz.fr. Other relevant criminal law provisions were among others: article 781 French Criminal Procedure Code (the usurpation of a name to obtain criminal records or '*usurpation de nom et casier judiciaire*') and art. 225-7 French Traffic Code (the taking of another person's name which could lead to a condemnation).

131 C. LACROIX, *Usurpation d'identité*, 2012, n° 11-25, www.dalloz.fr.

USURPATION OF CIVIL STATUS – Article 434-23 French Criminal Code (French CC) criminalises '*Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales*'. The perpetrator takes over the name of another person to commit crimes. This can lead to criminal prosecution of the victim for the crimes committed by the identity 'thief'. Only the usurpation of the name of an existing and living person is envisaged. The question was raised whether an IP-address or e-mail address could also fall under the scope of the offence. This would require a very broad interpretation of the notion 'name', which conflicts with the legality principle.[132] It seems that only when an e-mail address contains the name of another person, this can constitute the offence of article 434-23 French CC.[133] The usurpation is limited to cases where the victim risks criminal prosecutions for the 'result crime', the crime that gave rise to the usurpation. This means that the constitutive elements of the 'result crime' must also be reunited. [134]

USURPATION OF IDENTITY. – The problem with article 434-23 French CC is that it is sometimes very hard to prove that the constitutive elements of the result crime are met and that the victim actually risked criminal prosecution.[135] Next to that, as we have seen above, there are also other motives of identity 'theft'. The identity of another person is for example sometimes used to defame the primary victim.[136] Exactly for that reason, France introduced in 2011 a new article 226-4-1 French CC called '*usurpation d' identité*'. This is the act of taking over or using another person's identity information to disturb the peace of that person or another person or to affect his honour.[137] The intent to disturb the peace

---

132 C. LACROIX, *Usurpation d'identité*, 2012, n° 31, www.dalloz.fr.

133 Crim. 20 janvier 2009, n° 08-83.255, CCE n° 6n juin 2009, comm. 59, obs. Lepage

134 Crim. 29 March 2006, n° 05-85.857, *Bull. Crim.* N° 94, D. 2006, AJ 1443, obs. Manara, *AJ pénal* 2006, 263, obs. Royer, *Dr. Pénal* 2006. Comm. 82, obs. Véron ; Crim. 30 mai 2007, n° 06-84.365, *Bull. crim*. N° 145.

135 E.g. when the credit card of the primary victim is being used to pay for goods, this does not constitute the offence of fraud towards the vendor (the secondary victim).

136 *Cf.* the Belgian case of the creation of a fake Facebook profile in order to defame the victim. Corr. Dendermonde 8 April 2013, *Computerr.* 2013/195.

137 *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération.*

or to affect the honour of the impersonated victim constitutes the moral element (*mens rea*) of the offence (the specific intent).

This new offence was placed in the section of crimes committed against the right to privacy. It is interesting to see the shift from identity theft as an offence that affects the criminal justice system (an 'obstruction of justice' – offence), such as article 434-23 French CC[138], to a new form of an infringement of the right to privacy.[139] This explains the strong connection with other crimes protecting this legal interest through the special intent. '*Porter atteinte à la à son honneur ou considération*' ressembles closely the wording of defamation; whereas '*en vue de troubler la tranquillité de la victime*' brings it into the sphere of article 222-16 French CC (harassment via telephone).[140] The offence envisages the identity or identification information of another person (*cf.* article 434-23 French CC). This includes the name, surname, online pseudonym, password, IP address[141], etc. Originally, the offence was limited to online identity usurpation. In the end, this restriction was dropped.

OVERVIEW. –

Offence	Criminal act	Object	Form	Intent	Specificities	Legal interest
433-19	- taking - changing - altering - modifying	A name not one's own	Paper or digital form seems irrelevant	Intentional	Only public documents	Civil status / public order
434-23	Unspecified (orally, in writings…)	Another one's name	Offline and online	intentional	Only when this can lead to criminal prosecutions	Obstruction of justice

138 C. LACROIX, *Usurpation d'identité*, 2012, n. 28, www.dalloz.fr.

139 S. REVEL, 'Précision sur la notion d'usurpation d'identité ou l'inexistence de l'ubiquité', *AJ Pénal* 2010, 221.

140 C. LACROIX, *Usurpation d'identité*, 2012, n. 59, www.dalloz.fr.

141 TGI Paris, 24 June 2009, RG n° 08/03317. C. LACROIX, *Usurpation d'identité*, 2012, n. 58, www.dalloz.fr.

226-4-1	Unspecified (usurpation or making use)	Another one's identity or identification information	Offline and online	Specific	Only when motive was to harm other person	Privacy

OTHER RELEVANT CRIMINAL LAW PROVISIONS. – Besides being an autonomous offence, identity theft was also often brought in connection to the offences of fraud (escroquerie) or embezzlement (abus de confiance). It was regarded, for example, as the constitutive element of the use of false name, a false quality or fraudulent manoeuvres required for 'escroquerie'.

France also added a paragraph to its hacking offence (art. 323-1 French CC) in 2012, introducing the illegal access to an IT system which contains personal information as an aggravating circumstance, thereby transposing Directive 2013/40/EU into its domestic legal system.[142]

Finally, as France created two new police databases containing personal information, one with digital fingerprints (FNAED) and one with DNA (FNAEG), a specific offence was created in this context. Article 706-56, II, paragraph 4 French Criminal Procedure Code (French CPC) criminalises manipulations to forge the results of a genetic analyses.[143] The manipulation must take place by replacing one's own biological material by another one's. This specific offence relates to the general 'obstruction of justice'- offence by altering or forging evidence (art. 434-4 French CP).

EVALUATION – The way in which identity theft is autonomously criminalised can differ significantly depending on the focus and the existing legal framework. France, for instance, introduced an autonomous identity theft offence, the usurpation of another one's identity in order to disturb the peace of that person or another person or to affect his dignity. This provision only criminalises one particular aspect of identity theft, namely the 'stealing' of one's identity with the purpose to harm that specific person ('personal attack'). So although France has adopted 'specific' identity theft legislation, its approach remains fragmented. The 'specific' identity theft offence of article 226-4-1 France CC was introduced to fill the

142 M. SEGONDS, 'Loi relative à la protection de l'identité', *RSC* 2012, 905.

143 It more precisely criminalises (the attempt) to commit manoeuvres to substitute one's own biological material by another one's, with or without his consent.

gaps left by pre-existing offences, thereby criminalising the usurpation of another one's identity to violate his right to privacy. The other criminal law provisions still cover the other aspects of identity theft, for instance the usurpation of somebody else's identity to commit other crimes.

Because of this ad-hoc approach, some relevant legal questions were unfortunately not touched upon, such as the broadening of the scope of the already existing offences (for instance from usurpation of *name* to usurpation of *identity* or *identification information*) and more generally, a coherent and equal protection of identity online and offline, the right to anonymity and the right to use pseudonyms, the required moral element in this context, etc.

4 Evaluation

LEGITIMACY. – The legal interests in need of protection in the initial phase very much depend upon the specific context and on the *modi operandi*, e.g.:

- When the identification information is stored digitally, it is important to protect the integrity of the system and the data against insider and outsider attacks (CIA);
- When the physical e-ID is stolen, the legal interest of property is also at stake.

This variety of legal interests in the initial phase explains why we need to rely on very different criminal law provisions to counter the phenomenon, why the approach to criminalise is so differentiated and why finding legal loopholes is not obvious. At the same time, it explains why the phenomenon is already to a large extent covered by existing criminal law provisions, such as cybercrime, data protection law, forgery and 'classic' property offences.

The real challenge seems to be the protection of the legal interests in the subsequent phase: the authenticity of identification information in an offline and online context and the privacy and dignity of the primary victim in the identification process.

As we have seen above, identity has become a key to unlock many doors. A trustworthy identification process – assessing the link between a person, the identity information and a certain claim (i.e. a money transfer) – based on reliable identification information has become ever so important but at the same time ever so difficult in our information society where human-to-human-transactions are increasingly replaced by human-to-machine-transactions (*cf. supra*).[144] Because of its important societal role, the authenticity of the identification information is worth considering protecting through specific criminal law.[145] A second reason is that perpetrators profit from this new role and new vulnerabilities to alter the truth in a way (by pretending to be someone else) which can cause dramatic consequences for the primary victim. Victims can suffer from these crimes in special ways, for instance, by being blacklisted.[146] **Protecting one's identification information therefore is not only relevant because of** its **societal importance but also because of the** specific **harm identity**

---

144 B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 1-2.

145 S. REVEL, 'Précision sur la notion d'usurpation d'identité ou l'inexistence de l'ubiquité', *AJ Pénal* 2010, 218.

146 B.-J. KOOPS, R. LEENES, M. MEINTS, N. VAN DER MEULEN en D.-O. JAQUET-CHIFFELLE, „A typology of identity-related crime. Conceptual, technical and legal issues', *Information, Communication & Society* 2009, 9.

theft can cause to the primary victim. Because of these specific legal interests in the subsequent phase, it seems legitimate to criminalise identity theft as an autonomous offence, free from the used *modi operandi* in the initial phase, free from the motive of the perpetrator and more focused on the elements of falsehood and deceit and on the harm the identity theft may cause to the primary victim (in other words: the harmful consequences of the offence with regard to the primary victim).

EFFICIENT CRIMINALISATION. – Most studies conclude that existing criminal law provisions suffice to cope with the phenomenon. Sometimes a legal vacuum is detected, as in France, where parliament decided to fill the specific lacuna by introducing a new offence, rather than altering the existing ones. One should indeed bear in mind that criminal law is the ultimate resort and over-criminalisation should be avoided. We should not criminalise behaviour that is already sufficiently criminalised through other offences (subsidiarity principle). On the other hand, the case law of the ECtHR suggest that *efficiency* will also be part of the considerations on criminalisation.[147] For example, victims have to fall back on various criminal law provisions and are not recognised as victims of the identity theft *as such*. Consequently, primary victims are deprived of an adequate criminal law instrument to obtain redress and can only rely on secondary crimes committed by means of the 'stolen' identification information. The legal protection of primary victims will thus very much depend on the specific circumstances of the case. A disparate legal framework also complicates the international cooperation so indispensable in these cases.

Furthermore, those who claim that the result offences such as fraud, money laundering, human trafficking etc. are sufficient to tackle identity theft, deny the important fact that identity theft is a type of offence that should be tackled in an early stage. Like document or data forgery, it is a type of behaviour that facilitates other offences, but might merit criminalisation as a separate (preparatory) act. One should also realise that identity theft can cause a very specific type of harm, which should not be seen as a mere 'indirect effect'[148] but on the contrary, as one of the key issues, namely the difficulty to restore the compromised identity of the primary victim. It affects the primary victim's dignity and personal life, a legal interest which is not (sufficiently) covered by the preparatory offences (theft, hacking, etc.) nor the result offences (fraud, human trafficking …).

---

147 ECtHR 4 December 2003, *M.C. v. Bulgaria,* no. 39272/98.

148 OECD Policy Guidance on Online Identity Theft, 6, http://www.oecd.org/sti/consumer/40879136.pdf.

Finally, some studies stress the importance of statistical information in order to detect trends and developments.[149] Identity theft however, will often be the *modi operandi* or the motive rather than the offence and will as such not be registered as such. The official police database only allows registrations of existing (preparatory or result) offences, without knowing if the infringement was in fact committed to obtain or with the abuse of identification information. As a consequence, no statistical data are available.

The French approach of autonomously criminalising identity theft is a step in the right direction, as it takes into account the interests of the primary victim: the crime must be committed *with the purpose* to harm the primary victim. However, we believe a better approach would be to criminalise identity theft in a more comprehensive way. We have seen that the disturbance of the peace or the violation of one's dignity is not always the purpose of identity theft but the (potential) consequence. The motives of identity theft can vary significantly so that it seems more appropriate to implement these harmful consequences as the constitutive (potential) result of the crime, rather than the specific intent.

TOLERATED ACTS OF IDENTITY THEFT. – This however does not mean that the offence of identity theft should not require a specific intent, quite the contrary. We believe that in order to avoid over-criminalisation, a criminal provision with regard to identity theft should require the intention to obtain an illicit advantage for oneself or another or to harm somebody. One must bear in mind that the use of a false identity can sometimes be justified. Using another identity, for instance the use of a pseudonym, can be a means to safeguard freedom of speech, as well as privacy and private communication. Anonymity also protects people from unwanted or unwarranted control by public or private entities, from screening of social networking sites by marketing companies, from fraudsters and would-be intruders and from censorship and control by authoritarian regimes. Therefore, 'honest people' might also feel that the best way to protect their real identity is sometimes the use of a pseudonym. Criminal law should not encompass all such behaviour and therefore a specific intent should be required.[150] Another way to exclude such behaviour, is to depend on the concept of 'necessity' developed by doctrine and accepted by case law in order to justify certain criminal acts. Sometimes the offender is torn between the violation of the

---

149 *Ibid*. 6

150 S. TOSZA, 'Online social networks and violations committed using I.T. Identity fraud and theft of virtual property' (AIDP Global Report), *Revue Internationale de droit penal* 2013, Vol. 84, n. 1, 137.

law and the need to protect a legal interest which is deemed more important or at least equally important than the legal interest protected by the offence.[151] The violation of the latter could be justified when this violation was the ultimate remedy to protect the other, higher or equally important legal interest, for instance the use of a fictitious identity by undercover agents or refugees.

BUT…NO OVERRELIANCE ON SUBSTANTIVE CRIMINAL LAW. – Of course an autonomous criminalisation of identity theft will not make society more 'fraud-proof'. Criminal law is not and cannot be the best way *to prevent* identity theft. It can only play a role in the aftermath of it, as the legal basis to start criminal investigations, to acknowledge the suffering of the primary victims and to give them a stepping stone in the legal process of recovery of their compromised identity.

In considering strategies to tackle identity theft, we must also bear in mind that one does not necessarily need to get hold of someone's *primary* identity to commit identity theft. Somebody can easily pretend to be someone else using photographs or other personal information, especially in the online context. Identity theft is thus no longer limited to specific situations, documents or procedures but has become a much broader type of crime. The problem therefore is not so much the quality of the document itself but the quality of the identity check, the process of identification, verification and authorization.[152] This identity check relies too much on the integrity of the primary identity document. Especially in a digitised environment, the automation and standardisation brings extra risks when we blindly trust on technology.[153] The real answer in combatting identity theft, and identity fraud in general, is to make the identity check less predictable and uniform. By reducing the utility of the primary identity for non-authorised persons, its might become less appetising to predators. Tackling identity theft, and more in general identity fraud, demands a more differentiated approach, such as a regime under which the different identification information are independently controlled from each other and where this information can be compared.[154] A sort of 'compartmentalisation' of the identification information in order to make the identity check more complex and varied, and thus less predictable.

---

151 *Cf.* ECtHR 24 Mai 2011, *Mikkelsen and Christensen v. Denmark,* no. 22918/08.

152 J.H.A.M. GRIJPINK, 'Identiteitsfraude en overheid' in *What's in a name? Identiteitsfraude en –diefstal*, Maklu, Antwerpen/Apeldoorn, 2012, 18.

153 Ibid., 25.

154 Ibid., 29.

III Criminal law responses in the aftermath of identity 'theft': how to restore the compromised identity?

1 The road to restoration: a Via Dolorosa

FOCUS. – This chapter is limited to the issue of identity theft because this specific form of identity fraud comes with several unresolved problems as to the aftermath of the crime. As said, we start from the assumption that identity theft can never be completely prevented. We try to detect defaults in dealing with the aftermath of identity theft and to make suggestions for improvement to prevent *further* damage and bring restoration for the victim.[155]

ROMET V. THE NETHERLANDS[156]. – Once an identity is compromised, the primary victim faces enormous difficulties to 'clean up the mess'. The case of *Romet v. the Netherlands* before the European Court of Human Rights (ECtHR) is a perfect example of the Via Dolorosa victims of identity theft have to cross when they want to restore the damages and recover their 'stolen' identity.

Romet alleged a violation of article 8 of the European Convention in Human Rights (ECHR). In November 1995, Romet had reported to the police that his driving licence had been stolen two months earlier. For financial reasons, he only applied for a new driving licence at the beginning of 1997. It was issued to him shortly thereafter, on 14 March 1997. In the period between his reporting of the theft and the issuance of the new licence, no less than 1.737 motor vehicles had been registered on his name.[157] They had been registered upon presentation of the stolen driving licence.

As a result, Romet received large numbers of tax assessments, faced many prosecutions on the basis of the Motor Liability Insurance Act and was fined by the public prosecutor for traffic offences committed with the cars. When he refused to pay, he was detained for failure to comply with these fines and he ended up paying for the offences he had not committed. Furthermore, he was held liable for damage caused by uninsured vehicles

---

155 N. VAN DER MEULEN en B.-J. KOOPS, 'Van preventie naar risicoacceptatie en herstel voor slachtoffers in Nederlands beleid tegen identiteitsfraude', *NJB* 2012, 5.

156 ECtHR 14 February 2012, nr. 7094/06, *Romet/The Netherlands.*

157 During the period of 19 months, this is an average of 91 times a month or 3 times a day.

registered in his name and even his welfare benefits were stopped as his financial means were considered to be sufficient in view of the number of vehicles he apparently could effort.

In 1996, Romet made several unsuccessful attempts to rectify the situation. He asked the Agency to annul all the vehicle registrations in his name and bar the one relating to his own car. He also wrote several complaints to the public prosecutor. In February 2004, he lodged an appeal against the refusal of the Public Prosecution Service to prosecute those responsible for the vehicle registrations in his name. The Court of Appeal stated that although the police could have acted more effectively in this case, by then it was too late to conduct any viable investigation. The Court however noted that a complete remission in a single administrative act of all the administrative sanctions could come in hand. No such remission took place.

In January 2004 Romet once more requested the Agency to annul all the malicious registrations with retroactive effect. Three months later, the Agency partially granted the request and annulled 240 registrations as of that date. The Agency refused to annul the registration retroactively, stating that this would be detrimental to the reliability of the motor vehicle registration system. Romet objected to that, arguing that the system was already flawed by the malicious registrations and that the refusal would have enormous financial consequences for him. Moreover, in 1996, the Agency had offered to annul the stolen driving licence on condition that Romet would apply for a new one, condition he was unable to meet at that time for financial reasons. The Agency dismissed Romet's objection, claiming that annulment with retroactive effect would lead to legal uncertainty and to interference of the Agency with competencies of other authorities, such as the Public Prosecution Service and the Tax and Customs Administration. Such decision could affect the legality of decisions of the other services based on the content of the motor vehicle registration system. Romet appealed against that decision to the Court. He reasoned that the requirement to have to apply for a new driving licence in order to stop new registrations in the name of the stolen driving licence was unjust and discriminatory.[158] The Court disregarded his arguments and held against Romet that he had waited more than seven years before starting proceedings. Again, Romet appealed to the Council of State. He indicated that his rights under article 8 ECHR were being violated due to the unlawful

---

158 In 2006, a new Act provided that the driving licence would cease to be valid when it is reported missing. This Act also introduced a new model of driving licence. It includes a number of security features to counter misuse.

registrations and that the motor vehicle registration system was flawed in that it allowed such large-scale fraud to occur so easily (breach of data protection law). He also claimed the deprivation of his liberty based on the malicious registrations violated article 5 ECHR and article 9 International Covenant on Civil and Political Rights (ICCPR). The council of State brushed these arguments aside. It reasoned that it could not be found that the refusal to grant the annulment with retroactive effect was not reasonable since '*the purity of the vehicle register and legal certainty of the registration of vehicles justify such a policy.*'
As to the asserted breach of data protection law, the Council stated that '*it cannot be deduced from the fact that the guideline includes a right of correction that the processor of those personal data is obliged to do so* sua sponte *and unasked and might not make the desired correction dependent on a request to that effect.*' With regard to article 5 ECHR, the Council also disagreed, stating that these provisions contain an exception to these rights in order to secure the fulfilment of an obligation prescribed by law. Moreover, the Council noted that Romet had been deprived of his liberty because he had not taken the necessary measures to correct the wrongful registrations.

Romet took his case to the ECtHR, alleging among others a violation of the articles 6.2, 8 and 41 ECHR.
The main arguments of the Dutch government were that:

- the interference had been in accordance with the law at the relevant time and it was Romet who had delayed matters;
- it was the responsibility of the holder of an official document to guard against abuse. Romet could reasonably have been expected to ask for a replacement of the driving license to be issued before but he remained passive for several months while the cars were being registered in his name;

Romet argued that the interference did violate article 8 ECRM because the procedure in the Dutch Road Traffic Act to apply for a new licence was not the only way to prevent such fraud. In addition, the malicious registrations were incompatible with article 7 of the European Data Protection Directive because they had been made without his unambiguous consent. Therefore it had not been his fault: the government had been negligent.

The ECtHR did not delve into the question whether Romet had been negligent or not. It stated in a few sentences that from the very moment Romet reported his driving licence as being stolen, the domestic authorities were no longer entitled to be unaware that whoever might have Romet's driving license in his or her possession was someone other than

Romet. Therefore, '*swift administrative action to deprive a driving licence its usefulness as an identity document was possible and practicable*.'[159] The government should have responded immediately after Romet reported the theft, based on its positive obligation under article 8 of the Convention.[160]

The alleged violation of article 6.2 ECHR was related to the detention and various fines which, according to Romet, were solely based on presumptions flowing from the registrations of vehicles in his name. The ECtHR stated that the defence argument that the traffic offences had been committed in his name by other persons was available to Romet before the trial Court so that he was not left without means of defence.[161]
Romet finally claimed compensation of the damages. The ECtHR decided that Romet had suffered non-pecuniary damage and awarded him 9.000 EUR.[162]

INVESTIGATION AND EFFECTIVE REMEDIES AS A POSITIVE STATE DUTY. – The main problem in the *Romet* case was not a lacuna in the criminalisation of identity theft, but the lack of appropriate measures to end the crime. The extent and the impact of the identity theft was completely underestimated. Romet was therefore continuously confronted with the harmful consequences of the theft of his identity. It raises the question to what extent states are under an obligation to put an end to the identity theft.

On the basis of the positive state duty doctrine developed by the ECtHR, states have a positive duty to *effectively protect* their citizens from violations of their human rights, even in a horizontal relationship.[163] The ECtHR also applies this doctrine in criminal law, especially in the context of article 8 ECHR – violations. This means that Member States should not only make the impugned act punishable, but also provide for a consistent comprehensive procedure to bring the offender to the Court and to restore the illegal situation. These last two positive state obligations are strongly intertwined and are the tailpiece of an adequate criminal law framework to tackle identity theft. In our information

---

159 ECtHR 14 February 2012, nr. 7094/06, *Romet/The Netherlands,* §43.

160 *Ibid*, §37-43.

161 *Ibid*, §49-53.

162 *Ibid*, §67.

163 ECtHR 26 March 1985, no. 8978/80, X and Y/The Netherlands.

society, states however cannot do this alone. The 'electronic highway', where numerous forms of communication and services are interrelated and interconnected through the sharing of common transmission media and carriers, has altered the procedural powers and investigative techniques.[164] Once identification information is put online, it is *de facto* (technically) beyond the control of the intended user (the original identity bearer). It is in the hands of third parties, in particular service providers. They hold the data and thus *de facto* control the technical environment. That is why many traditional investigative measures do not longer work. Governments have to elaborate a legal framework that obliges third parties, in particular service providers, to cooperate with law enforcement.[165] DE HERT calls it 'system accountability': the responsibility of the government for the proper societal use of ICT.[166] This is necessary in our postmodern and digital era where the traditional governmental powers to regulate and enforce are threatened by the complex and global technological processes. The fact that many European states lost their monopoly on telecommunication channels adds to the need for private cooperation duties. Especially when human rights are at stake, cooperation cannot remain voluntary but demands enforceable legal rules (duties to cooperate). Moreover privacy legislation can restrict the possibilities of 'voluntary' cooperation.[167] 'Forced' means that the law prescribes how the norm addressee is supposed to act, there is no choice. This duty to cooperate with law enforcement can be enforced through either an administrative or a criminal legal framework. The choice between these two is often a matter of national policy. However, sometimes the ECtHR will demand that states should use criminal law (*cf. infra*).

We can distinguish three types of duties to cooperate: active, reactive and proactive duties.[168] 'Active' means spontaneously, at one's own initiative. In that case, there is no prior injunction, the duty originates directly from the legal provision. 'Reactive' means that the duty will only be activated *after* an injunction (e.g. a Court order). The initiative

---

164 Explanatory Note, 132.

165 ECtHR 2 December 2008, no. 2872/02, *K.U. v. Finland*, §49.

166 P. DE HERT, 'Systeemverantwoordelijkheid voor de informatiemaatschappij' in *De Staat van Informatie*, Amsterdam, Amsterdam University Press, 2011, 43.

167 For example the CJEU decided in the *Tele2 Sverige* case, that states can no longer pose a general data retention duty on ISPs because this would breach articles 7 and 8 of the EU Charter. Therefore ISPs might no longer possess the information requested by State authorities. (see *Supra* III.3.3.2)

168 E.C. MAC GILLAVRY, *Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven*, Nijmegen, Wolf Legal Publishers, 2004, 87 e.v.

therefore does not lie upon the norm addressee. Without such injunction, there is no duty to cooperate. Sometimes, the norm addressee will have to take certain measures to support an active or reactive obligation to cooperate. These are the so-called 'proactive' duties. They make sure that an active or reactive duty can be executed when necessary.
In case of identity theft, the following measures should be considered:

- Reporting mechanisms and notification duties for the data controller;
- The identification of the perpetrator and the retention and preservation of data to assist law enforcement;
- The blocking of access to and the rendering inaccessible of the illegal content, and/or the deletion of illegal content;
- The restoration of the harmful consequences (re-acquiring and resetting the compromised identity).

BALANCING. – Most of these procedural measures also touch upon *negative* obligations of states, derived from the right to privacy and freedom of expression. In terms of articles 8 and 10 ECHR, each infringement by a public authority must be in accordance with the law and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Not only victims of identity theft but also internet providers and users should be protected against disproportionate state interference.
This raises the difficult question of balancing conflicting fundamental human rights. On the one hand, the state must protect the rights of the victim of the identity theft, such as the right to privacy and data protection. As we have seen above, identity theft often threatens the physical and mental welfare of the victim.[169] On the other hand, such protection will clash with other fundamental rights, such as the right to privacy of other internet users, their right to freedom of information and the freedom of internet service providers to conduct business and their freedom of expression (*cf. infra*). In K.U. v. Finland, the ECtHR held that:

> '*Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate*

169 ECtHR 2 December 2008, no. 2872/02, *K.U. v. Finland;* ECtHR 14 February 2012, nr. 7094/06, Romet/The Netherlands.

> *imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context.*'[170]

Special notice should also be given to jurisdictional issues concerning these criminal law measures. In the following chapters, we will pay specific attention to their enforcement in an online context as this creates new challenges. Perpetrators can easily hide their identity online by using pseudonyms or false identities and profit from the ubiquitous nature of the internet to disseminate harmful or illegal content on large scale. Online content respects neither national rules nor boundaries. This complicates efforts to find an appropriate balance between the different human rights at stake and the fight against the distribution of illegal content. In its Action Plan for a safer use of the Internet in 1998, the European Commission for instance stated that '*harmful content needs to be treated differently from illegal content*'.[171] Yet what is harmful or offensive in one country may be deemed illegal in another and vice versa.[172]

As we will see further, it will not always be easy to strike the right balance between these rights. This is partly due to the complex international legal framework.

---

170 ECtHR 2 December 2008, no. 2872/02, *K.U. v. Finland*, § 49.

171 Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, December 1998.

172 Y. AKDENIZ, 'To block or not to block: European approaches to content regulation, and implications for freedom of expression', *Computer Law & Security Review* 2010, 26, 262.

2 Complex international legal framework

COUNCIL OF EUROPE. – Already in 1995 the Council of Europe adopted a set of principles in order to respond adequately to the new challenges raised by new technologies. The Committee of Ministers adopted Recommendation (95)13 of 11 September 1995 Concerning Problems of Criminal Procedural Law Connected with Information Technology[173] to ensure that investigating authorities possess appropriate and effective powers to investigate computer-related crimes. In 1996, a Committee of Experts was set up to further reflect on necessary steps in the fight against cybercrime. They recommended to adopt a binding international instrument, which resulted in the signature of the Convention on Cybercrime on 23 November 2001.[174] This Convention is the first and only international treaty on cybercrime. Next to substantive criminal law provisions, it contains procedural provisions, such as the expedited preservation (art. 16 and 17), production order (art. 18), search and seizure of stored computer data (art. 19), real-time collection of traffic data (art. 20) and interception of content data (art. 21).

In 2008, the 'Guidelines for the cooperation between law enforcement and Internet Service Providers' were adopted by a working group set up by the Council of Europe.[175] These Guidelines aim to streamline the interaction between law enforcement authorities and ISPs with regard to cybercrime. They explicitly encourage internet service providers to cooperate with law enforcement agencies in order to minimise the abuse of their services for criminal activity.

EUROPEAN UNION. – The European Union has adopted several instruments which may play an important role in ending and restoring identity theft:

- Data protection Directive[176]

---

173 Council of Europe Committee of Ministers, Recommendation (95)13 of 11 September 1995 Concerning Problems of Criminal Procedural Law Connected with Information Technology (Hereafter: Recommendation (95)13).

174 Council of Europe, *Convention on Cybercrime*, Budapest, 23 November 2001, ETS no. 185.

175 http://www.coe.int/en/web/cybercrime/lea-/-isp-cooperation

176 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31. This Directive will be repealed and replaced by the General Data Protection Regulation with effect from 25 May 2018 (articles 94 and 99 GDPR).

- Framework Directive[177]
- e-Privacy Directive[178]
- e-Commerce Directive[179]
- Data retention Directive[180]
- Cyber-attack Directive[181]
- General Data Protection Regulation (hereafter GDPR)[182]

Each of these Directives has its own scope and its own framework. As we will see further, sometimes there will be an overlap which further complicates matters even more.

---

177 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive 2009/140/EC and Regulation 544/2009.

178 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, OJ 2002 L 201 , 37. (amended by the Cookies Directive 2009/136/EC).

179 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive), OJ 2000 L 178, 1.

180 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105, 54. The Court of Justice declared this directive invalid in joined Cases C‑293/12 and C‑594/12 (Cases *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, EU:C:2014:238 (hereafter *Digital Rights Ireland*) *See further.*

181 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ 2013 L 218, 8.

182 Regulation No 2016/679 of the European Parliament and 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 95/46EC (General Data Protection Regulation), OJ 2016 L 119, 1.

3 Concrete procedural mechanisms

3.1 Reporting mechanisms and data breach notification laws

3.1.1 In general

FIRST STEP IN SWIFT RESPONSE. – Identity theft cases can at the same time qualify as a criminal offence, as well as violations of the right to privacy and data protection of the primary victim. Identity theft can thus be reported as a crime and as a violation of data protection law (*cf. supra*). A recent study on identity theft concluded: '*The establishment of a single EU-level reporting site might be a worthwhile avenue for exploration, as would the use at the national level of harmonised reporting forms/questions, which would further facilitate cross-border investigations*'.[183]

The reporting of a data breach by the data controller is the first step in the fight against identity theft. Reporting mechanisms would also support the more systematic collection of statistical data.[184]

Many breaches, however, remain undetected and if detected, are not reported to authorities or potential (primary) victims.[185] In the summer of 2011, for instance, DigiNotar, a Dutch digital certificate authority experienced a security breach which led to its bankruptcy and which allowed the attackers to generate fake PKI certificates.[186] These fake certificates were used to wiretap online communications in Iran. DigiNotar did not immediately report the incident to its customers or government authorities, which put the security and privacy of millions of citizens at risk.[187] This case shows that companies who deliver important digital society services, should quickly inform the relevant parties (users involved, corporate customers involved, government authorities) about significant

---

183 RAND Study, p. 117

184 Cf. Task 7.4. EKSISTENZ Project concerning the legal possibilities and implications of reporting an identity theft attempt.

185 M. DEKKER, C. KARSBERG en B. DASKALA, 'Cyber Incident Reporting in the EU: An Overview of Security Articles in EU Legislation', ENISA 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu.

186 http://www.enisa.europa.eu/media/news-items/operation-black-tulip

187 In the Press it was said that Iranian activists have died as a consequence of the delayed reporting about the attack.

security incidents. Immediate reporting of the incident and a swift response would have limited the impact considerably.[188]

The issue with regard to these reporting mechanisms is therefore that primary victims often do not know that their personal data has been compromised because their data are in the hands of other parties. Fearful of reputational damages, these companies will not be so eager to voluntarily inform the primary victims of identity theft that their data has been compromised and that they are a potential victim of identity theft. That is why security and data breach notification duties are becoming increasingly popular with European legislators.[189] In that case, the societal harm caused by the security and/or data breach outweighs the companies' interest to keep the incident secret and these companies are legally obliged to inform the authorities and/or (potential) victims about the data security incident. The goal is to create transparency about these incidents and to limit their impact. Another reason for the increasing EU attention to mandatory incident reporting is that national incidents can have a cross-border impact. So, in order to improve security across the EU, common rules are needed. Furthermore, service providers often operate across EU countries and it would cumbersome for them to adapt their systems to different national legislation.[190]

The EU has already developed legislation with the objective to have a consistent and harmonised legal framework. We will first examine the different data breach notifications and will then evaluate whether this framework is indeed consistent.

3.1.2 Legal framework

E-PRIVACY DIRECTIVE. –The e-Privacy Directive, as amended in 2009,[191] is the first legal instrument containing a data breach notification duty for data holders. As soon as the

---

188 Cf. the audit report of Fox-IT on the incident: http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

189 H. GRAUX, 'Data Breach Notifications – New Rules', time.lex newsletter 2013, www.timelex.eu. See for a non-exhaustive but clear overview M. DEKKER, C. KARSBERG en B. DASKALA, 'Cyber Incident Reporting in the EU: An Overview of Security Articles in EU Legislation', ENISA 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu.

190 M. DEKKER, C. KARSBERG en B. DASKALA, 'Cyber Incident Reporting in the EU: An Overview of Security Articles in EU Legislation', ENISA 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu.

191 Directive 2009/136/EC OF the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of

provider of publicly available electronic communications services becomes aware that a data breach has occurred, it should notify the breach to the *competent national authority.*[192] Next to that, the individuals *whose data and privacy could be adversely affected* by the breach should be notified without delay in order to allow them to take the necessary precautions.[193] The notification should also include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned. [194]

SCOPE. - This duty is however limited in scope. First of all it is limited to the telecommunications sector, and more particular to publicly available electronic communication services. This rules out a large amount of companies who also hold personal data and where the risks of identity theft are equally high. For instance, in June 2012 millions of hashed passwords of LinkedIn were disclosed on public hacker forums, urging millions of users to change their passwords because their personal data could be at risk.[195] This type of data breach at the time was not covered by incident reporting legislation. However this situation would now fall under the recently adopted General Data Protection regulation[196] that introduced a more general notification duty (*cf. infra*). Secondly, under the e-Privacy Directive the providers are not obliged to report to the individual if the provider has demonstrated to the satisfaction of the competent authority that it has implemented *appropriate technological protection measures*, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it (article 4.3).

---

personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ 2009, L 337, 11.

192 Article 4 (3) e-Privacy directive. In some countries this is the Telecom regulator, in other countries it is the data protection authority or another agency.

193 Article 4 (3) e-Privacy directive.

194 Article 4 (3) e-Privacy directive.

195 http://www.pcworld.com/article/257045/6_5m_linkedin_passwords_posted_online_after_apparent_hack.html

196 Articles 33 and 34 GDPR.

DETAILS NOTIFICATION. - Next to the limited scope, it also remained unclear when telecommunications service providers were required to notify breaches, nor was there a harmonised list of information to be provided. The EU Member States were free to interpret the rules themselves. This led to legal uncertainty and could even result in competitive distortion. Regulation No 611/2013 of 24 June 2013 therefore harmonised this matter.[197] It sets out the conditions under which data supervisors and (potential) victims must be informed and within which time-periods after the incident, and provides a basic template for such notifications (in the form of an Annex specifying the information to be communicated). The notification to the competent national authority must take place *no later than 24 hours* after the detection of the personal data breach, where feasible. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under the Regulation. [198]

The Regulation also clarifies in which situations a personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual. This shall be assessed by taking account of, in particular, the following circumstances[199]:

- the nature and content of the personal data concerned, in particular where the data concerns financial information, special categories of data referred to in Article 8(1) of Directive 95/46/EC, as well as location data, internet log files, web browsing histories, e-mail data, and itemised call lists;
- the likely consequences of the personal data breach for the subscriber or individual concerned, in particular where the breach could result in *identity theft or fraud*, physical harm, psychological distress, humiliation or damage to reputation; and
- the circumstances of the personal data breach, in particular where the data has been stolen or when the provider knows that the data are in the possession of an unauthorised third party.

---

197 Commission Regulation No 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, 2. (Hereafter: Regulation No 611/2013).

198 Article 2 Regulation No 611/2013.

199 Article 3 (2) Regulation No 611/2013

The Regulation also specifies when data are considered unintelligible. This is when the data are encrypted or hashed and the key used to decrypt or hash the data has not been compromised in any security breach, nor generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key.[200]
The Regulation entered into force on 25 August 2013. Unlike directives, Regulations are directly applicable across the EU, meaning that all providers of publicly available electronic communications services must immediately observe the new rules in the Regulation in cases of data breaches.[201]

THE E-PRIVACY REGULATION. – On January tenth 2017 the Commission proposed a Regulation concerning the respect for private life and the protection of personal data in electronic communications (hereafter e-Privacy Regulation).[202] This Regulation will repeal the e-Privacy Directive. The Regulation has several aims, including ensuring consistency and coherency with the new General Data Protection Regulation (see *infra).*[203] In this regard the notification duty under the e-Privacy Directive is not adopted in the new Regulation. Instead only the notification duty under the GDPR will be applicable to publicly available electronic communication services (see *infra* III. 3.1.3).

FRAMEWORK DIRECTIVE. - In 2009, another notification duty was implemented in article 13a of Directive 2002/21 on a common regulatory framework for electronic communications networks and services (Framework Directive).[204] This article states that providers of public communications networks or publicly available electronic communications services shall notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.
When necessary, for instance in case of cross-border incidents, the national regulatory authority shall inform the national regulatory authorities in other Member States and the

---

200 Article 4 (2) Regulation No 611/2013.

201 H. GRAUX, 'Data Breach Notifications – New Rules', time.lex newsletter 2013, www.timelex.eu

202 European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 10 January 2017.

203 European Commission, Digital Single Market - Proposal for an e-Privacy Regulation, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

204 Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive 2009/140/EC and Regulation 544/2009.

European Network and Information Security Agency (ENISA). It may also inform the public or require the providers to do so, where it determines that disclosure of the breach is in the public interest.

EIDAS REGULATION. [205] - Article 19.2 of the eIDAS Regulation of 2014 also contains a notification duty for trust service providers. It is similar to article 13a Framework Directive. 'Trust service' means any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.

Trust service providers must, without undue delay but in any event within 24 hours after having become aware of it, notify the competent supervisory body and other relevant bodies[206] of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Where the breach of security or loss of integrity is *likely to adversely affect a natural or legal person to whom the trusted service has been provided*, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.

E-COMMERCE DIRECTIVE. – Another duty to notify breaches is 'hidden' in article 15 of the e-Commerce directive: '*Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service (…)*'. Identity theft or fraud qualifies in most Member States as an illegal activity (*cf. supra*). This obligation

---

205 Regulation No 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 *OJ L 257, 28.8.2014, p. 73–114*

206 such as the competent national body for information security or the data protection authority

was introduced to compensate the system of limited liability of these ISPs (*cf. infra*). In exchange for that exemption, these ISPs are obliged to inform the competent authorities to allow them to take the necessary measures, such as the rendering inaccessible of the offending information (*cf. infra*).

Belgium, for instance, has implemented such an obligation to inform in the law transposing the e-Commerce Directive into its national legal framework.**207** This duty to inform is enforced through the imposition of a criminal fine of 26 to 25.000 euro in case of non-compliance.

Of course, these providers will sometimes also process personal data themselves. In that case there can be an overlap between the e-Commerce Directive and the Directives regulating the processing of personal data and the question arises how these overlapping Directives relate to each other.

The e-Commerce Directive emphasises that the protection of personal data is solely governed by the Data Protection Directive and e-Privacy Directive. The relationship between the different Directives is handled by article 1(5)b of the e-Commerce Directive. That article suggests that the liability exemptions provided in the e-Commerce Directive should not be applied in cases concerning the liability of 'data controllers', as this is a matter regulated by the Data protection Directive and the e-Privacy Directive.[208] It should therefore be examined whether an ISP acts as a 'neutral' internet intermediary, falling under the scope of the e-Commerce Directive, or as a 'data controller', falling under the scope of the Data Protection Directive. Recital (47) of the Data Protection Directive states that providers of electronic telecommunications or electronic mail services may be considered controllers '*in respect of the processing of the additional personal data necessary for the operation of the service*' but will generally not be considered controllers '*in respect of the personal data contained in the message*'.

GENERAL DATA PROTECTION REGULATION[209]. – The General Data Protection Regulation of 27 April 2016 introduces an obligation for controllers and processors to notify personal data breaches. The Regulation will replace the Data Protection Directive and shall apply from

---

207 Artikel XII.20 §2 and article XV.118 Belgian code of economic law

208 Search engines after Google Spain, 61.

209 Articles 33 and 34 Regulation No 2016/679 of the European Parliament and 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 95/46EC (General Data Protection Regulation), OJ 2016 L 119, 1.

25 May 2018 onwards. A controller under this Regulation is 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.[210] A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[211] The question can be raised what is meant by 'a breach of security'.[212] Do organisational security measures result under it or only technical security measures covering IT security? If we go for a broad interpretation the unauthorised disclosure by employees who were authorised to access the data concerned, but misused their access rights would fall under 'breach of security'.[213]

NOTIFICATION TO THE SUPERVISORY AUTHORITY. Article 33 of the Regulation contains the obligation of the controller to notify a personal data breach to the supervisory authority competent, not later than 72 hours after having become aware of it. There is no notification duty if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Recital 75 of the Regulation clarifies that the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, and includes among other things identity theft or fraud. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. The notification shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to

---

210 Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (article 4 (7) General Data Protection Regulation)

211 Article 4 (12) General Data Protection Regulation.

212 W. KUAN HON, E. KOSTA, C. MILLARD and D. STEFANATOU, 'Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation', Queen Mary University of London, School of Law Legal Studies research Paper No 172/2014, http://ssrn.com/abstract=2405971, 37.

213 *Ibid.*

be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[214] The processor shall notify the controller without undue delay after becoming aware of a personal data breach.[215]

COMMUNICATION TO THE DATA SUBJECT.- Article 34 of the Regulation obliges the controller to communicate the personal data breach to the data subject when the personal data breach is likely to result in a *high* risk to the rights and freedoms of natural persons. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the name and contact details of the data protection officer or other contact point where more information can be obtained, the likely consequences of the personal data breach, the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[216] According to article 34 (3) there will be no communication duty if any of the following conditions are met: '(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.' The supervisory authority may inform the data subject if the controller has not already done so.[217]

If controllers or processors neglect their notification duties under the regulation, administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, can be imposed.[218]

---

214 Article 33 (3) GDPR.

215 Article 33 (2) GDPR.

216 Article 34 (2) GDPR.

217 Article 34 (4) GDPR.

218 Art 83 (4) a GDPR.

3.1.3 Evaluation: a complex patchwork of notification duties

OVERVIEW. – Under the Data Protection Directive there was no general obligation on controllers to notify data breaches either to data protection authorities or to the affected data subjects.[219] However, as we have seen, some sector-specific notification duties were put in place. Until the enforcement of the General Data Protection Regulation, in the context of personal data breaches,[220] only providers of publicly available electronic communications services and trust services are required to notify incidents at a national and EU level. With the introduction of the GDPR there will exist a duty for all controllers to notify personal data breaches that put the rights and freedoms of natural persons at risk. The notification duties as described in the different EU instruments are summarised in the Annex to this report.

EFFECTIVENESS OF NOTIFICATION DUTIES.- The question remains if these notification duties are effective. A significant degree of uncertainty remains on certain key issues, such as who must be informed, which information must be provided and its level of detail, which safeguards should surround the disclosure, how to co-ordinate EU wide responses and exactly which companies will be subject to the incident reporting. Practical guidance is thus very much needed to enhance legal certainty.

In an evaluation and review of the e-Privacy Directive, a study prepared for the European Commission by Deloitte, the effectiveness of article 4 e-Privacy Directive is scrutinized. One of the key findings is that there are 'practical difficulties when it comes to the application of personal data breach notifications: confusion for businesses about which authority to contact, confusion based on the duplication with the GDPR, few breaches are notified hinting towards a low level of compliance, enforcement powers of authorities not always appropriate'[221]

---

219 HUNTON and WILLIAMS, The EU General Data Protection Regulation, A guide for in-house lawyers, 2016, https://information.hunton.com/23/1139/landing-pages/eu-gdpr-guide---registration-page-thank-you.asp.

220 The recently-adopted Cyber Security Directive also implements a notification duty for security breaches. This mandatory incident reporting is applicable to market operators responsible for critical infrastructures, like energy, water, health, finance and transport. The main *ratio* of this incident reporting is not the protection of personal data but national security and economic stability. We have therefore left it out of the overview.

221 DELOITTE, 'Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector', A study prepared for the European Commission, 2017, 115.

A PATCHWORK OF NOTIFICATION DUTIES. - The co-existing of different notification regimes creates (too) many reporting obligations. This leads to additional and unjustified burdens for businesses and confusion over the competency related to breaches. In some cases the same incidents are reported to different authorities causing duplications.[222]
The GDPR lies a notification duty on all 'data controllers', and thus overlaps with all the other notification duties under EU law. However it still remains relevant to know when these other duties apply, since they all differ[223] and the GDPR normally will function as *lex generalis.* Meaning that it can be overruled by more specific notification duties in other EU instruments qualifying as *lex specialis.*[224] For example under the eIDAS Regulation trust service providers must notify within 24 hours. This *lex specialis* will override the 72 hours term in the GDPR. [225]

The EU Commission took this concern into account and did not include a separate data notification duty in its proposal for the e-Privacy Regulation, replacing the e-Privacy Directive. From May 2018 onwards providers of publicly available electronic communications services thus will no longer have a separate notifications duty under the e-Privacy Regulation next to their duty under the GDPR. If we compare the GDPR with the e-Privacy Directive we can conclude that the obligations under the GDPR are more limited. Under the e-Privacy Directive telecom providers must notify all personal data breaches within 24 hours to the DPA. The GDPR, on the other hand, foresees in a timeframe of 72 hours and only requires notification where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons. According to ENISA, the notification duty for telecom service providers will therefore be made more efficient and less costly.[226]

---

222 *Ibid,* 116, 119.

223 For a schematic overview see the annex.

224 Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector, 115-116.

225 Article 33 GDPR.

226 The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. This view tends to be confirmed by businesses interviewed in relation to the evaluation of the e-Privacy Directive. (Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector, 113.)

THE GDPR TOO LENIENT? On the other hand, according to DE HERT and PAPAKONSTANTINOU, the data breach notification duty under the GDPR might be too flexible.[227] As discussed above, the GDPR follows a three level approach. If the personal data breach is 'unlikely to result in a risk for the rights and freedoms of individuals' controllers have no notification duty at all. If there is a risk, they need to notify the competent Data Protection Authority (DPA). If this risk is 'high' they also need to notify the data subject.[228] However even at this stage controllers can avoid notifying the individual by taking *ex post* measures (see article 34 (3) GDPR). Therefore 'in practice very few notifications are expected to indeed reach the public in a meaningful format'.[229] It is noteworthy that the initial proposal by the Commission foresaw in a broader notification duty. As in the e-Privacy Directive, all personal data breaches had to be notified to the DPA and the data subject had to be notified when the breach was likely to adversely affect the protection of the personal data or privacy of the data subject.[230] However, controllers are very reluctant swiftly to communicate data breaches to individuals, because this would incur substantial costs and reputational damage.[231] This explains why notification duties in the discussed EU instruments are layered. In first instance controllers are only obliged to inform the supervisory authorities and only in second instance the individuals concerned.[232]

---

227 P. DE HERT and V. PAPAKONSTANTINOU, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?', *Computer law & Security Review* 2016, (179) 191-192.

228 P. DE HERT and V. PAPAKONSTANTINOU, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?', *Computer law & Security Review* 2016, (179) 191-192.

229 P. DE HERT and V. PAPAKONSTANTINOU, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?', *Computer law & Security Review* 2016, (179) 191-192.

230 Article 31 and 32 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11, 25 January 2012.

231 P. DE HERT and V. PAPAKONSTANTINOU, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review* 2012, (130) 139-140.

232 P. DE HERT and V. PAPAKONSTANTINOU, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review* 2012, (130) 139-140.

FEW BREACHES NOTIFIED. – From a study prepared for the EU Commission by Deloitte it appears that the numbers of breach notifications in many Member States are very low or even inexistent. Some authorities explained that the lack of criteria made it difficult to determine which breaches need to be notified. Correspondingly, some authorities responding to Deloitte's online survey indicated that businesses in some cases fail to report personal data breaches.[233]

PRACTICAL IMPLEMENTATION AND ENFORCEMENT. - Finally, effective enforcement and a sanctions mechanism are important to ensure the objectives are achieved. Here the question surges whether notification duties should be enforced through administrative sanctions or criminal sanctions. In 2009, the Article 29 Working Party recommended to give the national data protection authorities more power, including the power to impose financial sanctions on controllers and processors.[234] However, it was pointed out during a workshop which the Commission held with competent Member State authorities, that not all competent authorities have the power to enact penalties in case of violations of article 4.[235]

In Belgium there is a legislative proposal pending, which extends the telecom data breach notification duty to all sectors (to the extent that they process personal data). The idea is to enforce it through administrative sanctions as 1) current breaches are quasi never prosecuted in reality, 2) administrative authorities can respond more quickly (and thus more effectively) and 3) the criminal sanctions are low in relation to the market value of personal data, thereby creating little deterrent effect.[236] The GDPR also opted for administrative sanctions. High fines apply when a data controller neglects his notification duties (*supra*, article 83 (4) a GDPR). As we will see further on, there are specific jurisdictional issues which hinder enforceability.

---

233 Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector, 116.

234 Article 29 Data Protection Working Party, 'The Future of Privacy', 02356/09/EN WP 168, 1 December 2009, lemma 84, § 90.

235 Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector, 114; referring to the European Commission (April 19, 2016). Meeting with Competent National Authorities on the review of the e-Privacy Directive. Minutes, p. 4.

236 *Parl. St.* Kamer 54-0416/001.

EXCESSIVE BURDEN? - Enhancing legal certainty and enforcement is however not the only concern. Notification duties go hand in hand with different costs.[237] Concerns further raise whether such mandatory incident reporting will hinder business growth and competition. Such reporting requirements could indeed impose significant administrative burdens and cause reputational risks for businesses, particularly for SMEs, which may not have the resources required to meet these standards. Article 13a Framework Directive and article 19.2 eIDAS Regulation both state that the public must be informed when the security incident has an impact on public interest. It remains unclear *when* this is the case and *which information* should be disclosed. This is however of great importance to the undertakings who can suffer economic losses and reputational damages when this information would unnecessarily be publicly revealed. One might even argue that the information that does not fall under the scope of the notification duty qualifies as confidential business information and is *as such* worth protecting against illegal disclosure. So there is a very fine line in this case between information that *must* be disclosed and information that *may not* be disclosed. This issue should be clarified. These reporting requirements may also not hinder a quick and effective response to the incident. Emergency response should remain the prior concern.[238] Hence, a careful balance between stimulating better exchange of information and adding unnecessary burdens to businesses should be struck. There are also some other concerns. Disclosing of information in order to protect the privacy rights of the victim may also pose new threats to privacy rights when that disclosure is not regulated in an adequate way, f.i. more information than necessary is disclosed, the disclosure is not surrounded with the necessary security requirements etc. This issue should also be addressed.

---

237 A division can be made between two general cost elements: (1) Notification costs, including the: Creation of contact databases; Determination of all regulatory requirements, Engagement of outside experts, Postal expenditures, email bounce-backs and inbound communication set-up; and (2) Post data breach response costs, including: Help desk activities, Inbound communications, Special investigative activities, Remediation, Legal expenditures, Product discounts, Identity protection services and Regulatory interventions. (Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector, 116.

238 M. DEKKER, C. KARSBERG en B. DASKALA, 'Cyber Incident Reporting in the EU: An Overview of Security Articles in EU Legislation', ENISA 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu.

3.2 Identifying the identity 'thief'

3.2.1 In general

ANONYMITY IN CYBERSPACE. – The enactment of a criminal offence has limited deterrent effect if there are no means to identify the actual offenders and to bring them to justice.[239] The internet offers users more possibilities to protect their real identity than many other channels of communication do. Such a protection is not always a bad thing. As already explained, in cyberspace anonymity is a means to safeguard freedom of speech, as well as privacy and private communication (*supra* III. 4). But neither of these two fundamental rights is an absolute one. In some situations and under some conditions, states may intervene (Article 8.2 and 10.2 ECHR). This is definitely justified to detect crime, to collect evidence or to identify and prosecute the perpetrators. States may therefore, within the limits set by their national legislations and by the texts protecting fundamental rights and freedoms, uncover the identity of criminal suspects on the internet.

These days, much of the information which is of interest to the criminal investigation is not held by the government, but by private entities with relevant technical knowhow and access to the information. Most service providers however do not execute effective or reliable identity controls. Yet, they do dispose of a large amount of data that might help to retrieve someone's real identity. A lot of this 'identification data' will be useful in a criminal investigation in order to identify the perpetrator. The challenge is how to enable the service providers to hand over this information to law enforcement.

3.2.2 Legal basis for identification orders

COUNCIL OF EUROPE. – Different initiatives by the Council of Europe introduce recommendations to identify perpetrators. Recommendation (95)13 already recommended states to impose specific obligations on service providers which offer telecommunication services either through public or private networks to identify their users when ordered by the competent investigating authority.[240] Article 18 Cybercrime Convention further obliges the Member States to adopt legislative and other measures to order a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or

---

239 ECHR, 2 December 2008, *K.U./Finland*, no. 2872/02, 46.

240 Point 12 Recommendation (95)13.

control. Subscriber information means, among others, the subscriber's identity, his address, telephone number etc.[241] On the basis of this article, Member States can thus impose a duty to disclose the identity of the user of an ICT-application to law enforcement, when ordered to do so by a competent authority. Such orders should help investigators to link telephone numbers, email-addresses and IP addresses to specific users.
These type of orders were, among others, deemed necessary as service providers are at the same time obliged to ensure the confidentiality of the identification data, among others by data protection law and other secrecy obligations. Most of these obligations are enforced by the threat of criminal sanctions. Therefore, in order to prevent contractual and criminal liability, they can only disclose the information when they are legally obliged to do so.[242]

DATA RETENTION DIRECTIVE. – No European instrument directly deals with the obligation to hand over identification data. The recently annulled Data Retention Directive was based on the principle that data should be available for the purpose of investigation, detection and the prosecution of serious crimes in relation to the use of ICT. It thereto imposed an obligation to retain certain categories of identification, location and traffic data for a period between six months and two years in order to ensure their availability, upon request, for law enforcement agencies. How these law enforcement agencies access the data, is a matter of national procedure. On the 8th of April 2014, in the *Digital Rights Ireland* case, the CJEU declared the Directive invalid.[243] The Court ruled that the principle of data retention serves, under clear and precise conditions, a legitimate and general interest, namely the fight against serious crime and the protection of public security. The Directive however disproportionally infringed the rights of privacy and data protection and should have provided more safeguards to protect these fundamental rights. As a result of the invalidity, data could only be retained under EU law on the basis of article 15 (1) e-Privacy Directive.

DATA RETENTION AND THE E-PRIVACY DIRECTIVE. - Article 15 (1) of the e-Privacy Directive allows Member States to create national rules which restrict the rights and obligations provided for under the general rules where it is '*necessary, appropriate and proportionate*'

---

241 Article 18 (3) Cybercrime Convention.

242 There is still no decision on whether this requires a court order. One might argue that there is less of an infringement to privacy with regard to identification data than with regard to content data, so that in case of disclosure of identification data, an order of the public prosecutor suffices.

243 Judgement of 8 April 2014, Digital Rights Ireland and Seitlinger and Others, C-293/12 and C-594/12, EU:C:2014:238 (hereafter *Digital Rights Ireland*).

to do so for the purposes of safeguarding national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences. Article 15 (1) further states: '*To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph*.' In the *Tele2 Sverige* case[244] the question was raised whether a general obligation to retain traffic and location data is allowed in light of the *Digital Rights Ireland case*, Article 15(1) of e-Privacy Directive and Articles 7, 8 and 52(1) of the EU Charter.[245] And if so, whether such general data retention obligation must be accompanied by all the safeguards laid down by the Court in paragraphs 60 to 68 of *Digital Rights Ireland* in connection with access to the data, the period of retention and the protection and security of the data.

On the 21st of December 2016 the Court ruled that '*article 15 (1) e-Privacy Directive read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.*'[246] Furthermore, the Court stated that national legislation governing the protection and security of traffic and location of data should only allow the competent national authorities access to the retained data, in the context of fighting crime, if the following requirements are met: the objective must be the fighting of serious crime, there must be a prior review by a Court or independent administrative authority and the data must be retained within the EU.[247]

---

244 Judgement of 21 december 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Joined Cases C-203/15 and C-698/15, EU:C:2016:970 (hereafter *Tele2 Sverige)*; Opinion of Advocate General SAUGMANDSGAARD ØE of 19 July 2016, Tele2 Sverige AB, C-203/15 and C-698/15, EU:C:2016:572, paragraphs 67-68.

245 Article 7 EU Charter contains the right to respect for private and family life, article 8 EU Charter the right to protection of personal Data. Article 52 (1) EU Charter sets out the conditions under which limitations can be made to the rights and freedoms in the Charter.

246 '*The retention of data must meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected*.' Judgement of 21 december 2016, Tele2 Sverige AB, C-203/15, EU:C:2016:970, § 110-112.

247 Judgement of 21 December 2016, Tele2 Sverige AB, C-203/15, EU:C:2016:970.

PERPLEXITY. - The judgement is a real stumbling block for the investigation of crimes. Especially the requirement of 'serious crime'[248] is problematic in the fight against ID theft. Not every type of ID theft will qualify as a serious crime. The Court states that '*the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest*'.[249] In the case of cybercrime not only serious crimes depend on modern investigation techniques. A single person can commit a variety of e-crimes without any accomplice or terroristic motive with only the help of a computer. Furthermore, even if the requirement of a serious crime is met, only data retention for the future is possible. In many cases this will be too little, too late. A runaway teenager case (not serious) can become a murder case (serious) if the body is found months later. Localisation or communication data from the period of disappearance would be very important for the murder investigation, but will no longer be available.

DATA RETENTION AND THE ECTHR. - In the case of *Figueiredo Teixeira v. Andorra*[250] before the ECtHR, Mr Teixeira complained that the storage of data relating to his telephone communications amounted to an unjustified interference with his right to respect for his private life under article 8 of the ECHR.[251] Mr Teixeira, who was suspected of the serious offence of drug trafficking, was arrested on 5 December 2011.[252] The judge responsible for the criminal investigation asked Andorra Telecom to hand over a list of incoming and outgoing calls from two telephone numbers pertaining to Mr Figueiredo Teixeira over the period from 15 August to 4 December 2011, and to inform him of the identities of subscribers holding the numbers set out in the list.[253]

The ECtHR decided unanimously that article 8 ECHR had not been violated. It stated that the interference was prescribed by law and emphasised that the Andorran procedure

---

248 *Ibid,* §102.

249 The ECJ adds that the seriousness of the crime 'cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 51)' (Judgement of 21 December 2016, Tele2 Sverige AB, C-203/15, EU:C:2016:970, §103.)

250 ECHR, 8 November 2016, *Figueiredo Teixeira/Andorra,* no. 72384/14.

251 *Ibid*, §29.

252 *Ibid*, §5.

253 *Ibid*, §6.

provides a wide range of safeguards against arbitrary actions. These included the involvement of a judge to grant prior authorisation for the measure, exclusively applicable to very serious offences; a statutory time-limit on the measure; and finally, the fact that the applicant could at any time contest the lawfulness of evidence gathered during proceedings.[254] The impugned interference had a legitimate aim, that is the prevention of crime as foreseen in article 8. Furthermore the measure was deemed proportional by the Court.[255] From this judgement it seems to appear that the compulsory storage of personal data by a telecom company as such is not a problem under the Convention. The communication of this data however, has to meet certain conditions and safeguards to be in accordance with the right to privacy. This is the main difference between this case and the *Tele2 Sverige* case of the CJEU.[256] The assessment of a breach of the right to privacy[257] is similar but according to the CJEU takes place in an earlier stage, namely at the time of the retention of the data, whereas the ECtHR only verifies if the subsequent use, the communication of data to the authorities, meets the necessary safeguards.

NATIONAL DATA RETENTION LAWS RENDERED INVALID? - In 2015 the Belgian Constitutional Court, relying on the judgement of the CJEU in *Digital Rights Ireland,* annulled the Belgian data retention law[258] that partially implemented the Data Retention Directive in Belgian law.[259] Recently (May 2016) Belgium adopted a new Data Retention law.[260] Just as with the annulled legislation, a general retention duty for telecom and internet providers is introduced. However, in the reformed law extra privacy guarantees are built in. For example, data should only be retained for 12 months and there is no longer a possibility to

---

254 *Ibid*, §38-47.

255 *Ibid* §48-52.

256 And perhaps this is also the difference between the *Digital Rights Ireland* case, as read by the data retention optimists, and the *Tele2 Sverige* case.

257 Under the EU Charter the Respect to privacy and the Protection of personal data are two separate rights (respectively article 7 and article 8 EU Charter). However, it is noteworthy that in the *Tele2 Sverige* Case the CJEU seems to assess them together.

258 Wet van 30 juli 2013 houdende wijziging van de artikelen 2,126 en 145 van de wet van 13 juni 2005 betreffende elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering, *B.S.* 23 augustus 2013.

259 Belgian Constitutional Court 11 juni 2015, nr. 84/2015.

260 Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016, (Act of 29 May 2016 concerning the gathering and retention of data in the sector of electronic communications)

prolong the retention period.[261] The security of the stored data is also enhanced by, among other things, a duty to make the stored data illegible for unauthorised persons.[262] Against the background of the *Tele2* judgement this legislation is more than likely to face a new annulment by the Belgian Constitutional Court since it still imposes general data retention and only restricts the access to it is .[263] Not only Belgium, but all EU-countries with a general data retention duty will need to adapt their national legislation to bring it in line with the CJEU judgement. This will certainly be the case for Sweden and the UK, whose legislations led to the preliminary questions in the *Tele2* case.

3.2.3 Case law with regard to identification orders

ECHR LIMITS TO ANONYMITY. – In the case of the European Court of Human Rights *K.U. v. Finland,*[264] a Finnish service provider refused to divulge the identity of the holder of an IP address to the victim of an identity theft,[265] regarding itself bound by the confidentiality of telecommunications. At that time, there was no Finnish legal provision authorising the service provider to disclose telecommunications identification information. The disclosure of this information would have breached professional secrecy, in this case qualified as 'malicious misrepresentation'.

The Finnish government argued that it was a private individual who interfered with K.U.'s private life and that according to Finnish legislation, a service provider has an obligation to verify the identity of the sender before publishing a defamatory announcement on its

---

261 Article 126, § 3 Wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005. (Act of 13 June 2005 concerning electronic communications.)

262 Article 126, § 4 Wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005.

263 S. ROYER and C. CONINGS, 'Ook hervormde dataretentiewet staat onder druk' , De Juristenkrant 2017, nr 341, 1.

264 ECtHR 2 December 2008, no. 2872/02, *K.U. v. Finland.*

265 An unidentified person placed an advertisement on an internet dating site in the name of the then twelve year-old boy K.U. The advertisement mentioned personal information, such as his age, year of birth, a detailed description of his physical characteristics and a link to his personal website which showed his picture and his telephone number. It claimed that he was looking for an intimate relationship with a boy of his age or older 'to show him the way'. K.U. found out about the advertisement after receiving an e-mail from a man, offering to meet him and then 'see what you want'.

website.[266] Failure to identify is a criminal offence which has sufficient deterrent effect and the government had thus taken the necessary measures to ensure the protection of private life.[267]

On the basis of a violation of article 8 ECRM, the ECtHR required Finland to ensure access to communication data in order to identify the perpetrator who had violated another individual's right to private life and to enable effective criminal prosecution. As telecommunication data are qualified as personal data and also fall under the protection of article 8 ECHR[268], the ECtHR thus had to balance these two types of privacy. The ECtHR is very clear: it is necessary to disclose communication data to law enforcement in order to ensure an effective and efficient protection of private life. As such the Court contributes to the difficult balancing exercise between on the one hand the confidentiality of communication data, guaranteeing as well the 'formal sphere' of the right to privacy (art. 8 ECRM) as the right to freedom of information (art. 10 ECRM), and on the other hand the 'substantive' right to privacy.

ASSURE AUTHORISED ACCESS, EXCLUDE UNAUTHORISED ACCESS – The ECtHR thus obliges Member States to assure effective protection of private life in a digital context and thereto requires effective means of identifying perpetrators in that context. A duty to verify, sanctioned with a criminal penalty in case of non-compliance, apparently was not sufficient. Law enforcement must be enabled to access data in order to identify the perpetrator of a serious violation of private life.

In the same year, the ECtHR decided in *I. v. Finland*, that the respect for private life under article 8 ECHR, holds a positive obligation for the state to provide for effective information security measures to exclude the possibility of unauthorised access to data.[269] In this case, the Court had to assess the security measures of a public hospital with regard to the IT-system storing medical data.[270] The Court found that the lack of keeping records of

---

266 ECtHR 2 December 2008, no. 2872/02, *K.U. v. Finland,* §§ 19, 37 and 39; T. PÖYSTI,'Judgement in the case of K.U. v. Finland*', Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 36.

267 *Ibid.*

268 ECtHR 3 April 2007, no. 62617/00, *Copland v. the United Kingdom*, paragraphs 41-44.

269 ECtHR 17 July 2008, no. 20511/03, *I. v. Finland*, paragraph 37.

270 ECtHR 17 July 2008, no. 20511/03, *I. v. Finland*.

personnel who had access to the records, constituted a lack of effective security measure in order to protect the private life.[271]

Both judgements make clear that an effective protection of private life must be included in the IT infrastructure, such as the keeping of records and the enabling of access to identification data to law enforcement.[272] Deterrence thus not results (only) from the criminalisation of certain behaviour, but also depends on the risk of being caught, in this case the risk of being identified.

On the basis of this case law, one might argue that this also demands technical measures which provide for the reliable identification and authentication of users of electronic communication services. Such technical measure enables that only authorised persons access the identification data and that unauthorised access is made more difficult.[273] Here the Project's technology might provide as a handy tool in the fight against ID Fraud and other misuse of personal data.

One could also argue that effective protection of private life indirectly implies the recording and retention of this identification data for law enforcement purposes, which brings us

---

271 ECtHR 17 July 2008, no. 20511/03, *I. v. Finland*, paragraphs 44-49.

272 T. PÖYSTI,'Judgement in the case of K.U. v. Finland'*, Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 34.

273 In this context the question rises if law enforcement cans also oblige private parties to decrypt. In the United States this question was at the center of the discussion in the *U.S.* v. *Apple* case concerning the decryption of an iPhone in a terrorism investigation concerning the San Bernardino Shooting. The FBI had requested Apple to develop new software to break into an iPhone recovered during the investigation. Apple refused this because this would leave the door open for sophisticated hackers and cybercriminals. Encryption of data of course can be an important tool to prevent ID theft. Data that are protected with encryption are more difficult to hack and in case of strong encryption hacking can even made impossible. At the same time, decryption also hinders the gathering of information necessary for the investigation and prevention of crimes, including ID theft. (T. COOK, 'A Message to Our Customers', 16 February 2016, http://www.apple.com/customer-letter/; M. FINNEMORE, D. B. HOLLIS, "Constructing norms for global cybersecurity", Am. J. Int'l L. 2016, 425-479; N. GIBBS and L. GROSSMAN, "Apple CEO Tim Cook on his fight with the FBI and why he won't back down", TIME, 17 March 2016, http://time.com/4261796/tim-cook-transcript/)
The Dutch government made an assessment of the pros and cons of encryption and came to the conclusion that, for now, it is not desirable to take restrictive measures concerning the development, availability and use of encryption in The Netherlands. (NEDERLANDS MINISTERIE VAN VEILIGHEID EN JUSTITIE, 'Kabinetsstandpunt Encryptie', 4 January 2016, file:///C:/Users/u0110896/Downloads/tk-kabinetsstandpunt-encryptie.pdf.)
The British government on the other hand wants to ban end-to-end decryption, requiring mandatory back doors in the encryption technology. This appears from leaked documents in hands of the Open Rights Group. (https://www.openrightsgroup.org/assets/files/pdfs/home_office/ANNEX_A_Draft_Investigatory_Powers_(Technical%20Capability)_Regulations.pdf; I. KOTTASOVA and S. BURK, 'U.K. government wants access to WhatsApp messages', CNN Money, 27 March 2017, http://money.cnn.com/2017/03/27/technology/whatsapp-encryption-london-attack/)

back to the controversial domain of data retention.[274] The practical effectiveness of identification namely depends to a large extent on the legal obligation to store and retain this data. On the basis of K.U. v. Finland, we could argue that in order to protect essential aspects and values of private life, States have a positive obligation under the ECHR guarantee some storage and retention of identification data and to provide access to it in criminal investigations.[275] Again, the right balance should be struck between various competing rights and claims and this assessment might be different in case it concerns children or other vulnerable persons. The outcome of this assessment might be different in other cases, as is demonstrated by the CJEU judgement *Promusicae*.[276]

3.2.4 Conclusion

NEED FOR IDENTIFICATION ORDERS. – On the basis of K.U. v. Finland, we can conclude that States should implement a legal procedure where a judicial authority may order, under certain conditions, the release of information required to identify an internet user provided that there are reasonable grounds to believe that he or she has committed a criminal offence. It should be noted that the ECtHR paid specific attention to the fact that in this case a minor was the subject of an advertisement of a sexual nature. This created a stronger positive obligation to protect fundamental rights, even in a horizontal relationship.[277] The ECtHR is indeed particularly strict when it comes to the protection of the physical and emotional welfare of children because of their vulnerability.[278]

---

274 See Cases *Digital Rights Ireland and Seitlinger and Others*, C-293/12 and C-594/12, EU:C:2014:238; Opinion of Advocate General SAUGMANDSGAARD ØE of 19 July 2016, Tele2 Sverige AB C-203/15 and C-698/15, EU:C:2016:572 as discussed above.

275 T. PÖYSTI,'Judgement in the case of K.U. v. Finland*', Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 44.

276 In this case the CJEU had to decide whether Promusicae, a Spanish association of audiovisual producers, could oblige an internet access provider to hand over identification data for the purpose of identifying a user suspected of copyright infringement. The CJEU thus had to balance the right to privacy and data protection of internet users and the right to property (intellectual property) of copyright holders in a civil proceeding. It decided that any personal data collected pursuant to the Data Retention Directive could not be used in civil lawsuits, unless a national provision that strikes a fair balance between the various fundamental rules, allowed for it. Judgement of 29 January Promusicae C-275/06, EU:C:2008:54; E. WERKERS EN F. COUDERT, 'In The Aftermath of the Promusicae Case: How to Strike the Balance?', *Int J Law Info Tech* 2010, 50-71; P. VAN EECKE, « Online service providers and liability: a plea for a balanced approach », *Common Market Law Review* 2011, (1454) 1493.

277 T. PÖYSTI,'Judgement in the case of K.U. v. Finland*', Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 37.

278 Cf. ECtHR 26 March 1985, no. 8978/80, X and Y/The Netherlands.

Nonetheless, the ECtHR provides some essential elements concerning the positive obligations in the context of article 8 ECHR violations and unfair processing of personal information. The right to private life and the right to informational self-determination, which is the core of the data protection law, complement each other in defining the elements of protection in the context of electronic communications and IT systems. The storing and retention must not only be seen as a threat to fundamental human rights such as the right to private life; sometimes it is required to protect those very same rights.[279] The judgement of K.U. v. Finland is very important as it makes it clear that weak or even non-existent user identification and authentication may easily create problems with regard to an effective protection of fundamental human rights, in particular private life. Personal data legislation, such as data protection laws, should not stand in the way of an effective protection but might on the contrary be used to address this weakness. These laws should arrange proper identification and authentication in electronic transactions when elements of personal integrity and identity are at stake. With 'proper' we mean that they should make identification and authentication possible while at the same time surround these processes with the necessary guarantees with regard to competing fundamental human rights and freedoms at stake, such as the right to privacy of other users and their right to freedom of expression. These rights are not absolute and are sometimes overridden by other interests. The ECtHR calls for a balanced approach and emphasises the role of the legislator therein.[280] It accepts that Member States have a certain margin of appreciation and that positive obligations should not create a disproportionate burden to other concerned private persons, such as internet service providers. It also accepts that implementing legislation and criminal policy in the changing social and technological modern society is difficult and that different circumstances apply in different Member States. The standards are however defined from the perspective of the protection of fundamental human rights and freedoms. The ECtHR for instance considered that although Finland had legal provisions regulating the issue, it failed to meet its positive obligation to provide practical and effective protection because its legislation did not enable the authorities to identify and prosecute the person who had committed the criminal offence that violated the applicant's private life. Therefore the ECtHR actually imposes a positive duty upon States to follow societal and technological developments in order to ensure that

---

279 T. PÖYSTI,'Judgement in the case of K.U. v. Finland*', Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 44.

280 *Ibid, 39.*

the legislation in force can provide effective protection. This means that they must actively and systematically manage the risks to fundamental human rights.[281] The Court extended its principle of practical effectiveness to the effectiveness of criminal investigations and stated that these require access to identification data in order to identify the perpetrator. In that perspective, the protection of private life and identity can be achieved by attempting to provide for proof of identity and authentication in IT-systems and at the same time implementing the necessary safeguards to protect this personal data during that identification process, for instance by obligating internet service providers who store the data to provide for the proper security of their IT and archive systems.[282] In *I. v. Finland,* for example, the ECtHR decided that article 8 ECHR had been breached because the IT system did not record who had been obtaining access to and consulting confidential files and access was not restricted only to staff members who were responsible for the treatment of these files. This implies that the ECtHR requires (technical) secure IT systems, which can only be accessed by authorised persons and which should be subject to effective audits.[283] This also means that IT systems which make it impossible or very difficult to detect the identity of the user, such as TOR, should be critically assessed. [284] Such applications can indeed enhance the freedom of expression and protect the right to anonymity, yet these rights are not absolute and can (at least in most Western countries) be sufficiently protected by restricting the access by the competent governmental authorities to that data. In that way, the right balance can be struck.

IDENTIFICATION HINDERED BY CJEU CASE LAW. - According to the Court of Justice of the European Union, a general data retention obligation contravenes the right for private and family life and the right to the protection of personal data (*supra Tele2* case). The rationale behind this case law cannot be reconciled with the positive obligation of Member States in the light of the ECtHR case law. Member States' duty under the ECHR to make identification possible might in many situations, be rendered practically impossible by the CJEU's ban on general data retention. One can hope that the CJEU would adjust its – very principled, yet not very practical – position to the more nuanced position taken by the ECtHR, thus defusing a potential conflict on fundamental (human) rights standards in a fundamental

---

281 Ibid., 41-42.

282 ECtHR 17 July 2008, no. 20511/03, *I. v. Finland.*

283 Added value Eksistenz

284 T. PÖYSTI,'Judgement in the case of K.U. v. Finland*', Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 44-45.

policy area. Once an identity is stolen it is important that we can identify the identity thief, in order to stop the crime and to make a claim for damages by the victim possible.

3.3 Blocking, rendering inaccessible and erasing of personal data

3.3.1 In general

POLICY CONCERNING BLOCKING MEASURES. – The potential harm and negative consequences of identity theft often result from the widespread and continuous availability of the compromising information online. In order to end the crime or to prevent further damage, the compromising data can be rendered inaccessible, either by the *blocking of access* to or by *deleting* compromising online content. Both measures could provide an effective remedy to end the identity theft and to limit further damages. Because of the difficulties to identify the perpetrator and to locate the compromising data (*cf. infra*), law enforcement often has to turn to internet intermediaries to block access to or to take offending information offline. Especially blocking of access to illegal content through internet access providers seems to be the new trend as state authorities' requests to remove or take down the illegal content are rejected or simply ignored by hosting or content providers outside their jurisdiction (yet *cf. infra* Google Spain).

EU-RELUCTANCE. - The blocking or deletion of online data appears to be a major issue. Regardless of possible technical difficulties (e.g. easy to circumvent), this measure also poses legal problems as it remains uncertain under which conditions such a measure is compatible with EU law. Blocking measures clearly affect fundamental human rights such as the right to privacy, the right to freedom of expression, the right to property, the EU right to provide services in any Member State[285] and the right to conduct a business.[286] Therefore, they can only be imposed by law, subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society the triple 'proportionality check' of article 8.2. and 10.2 ECRM, *cf. infra*). The main issue seems to be the potential collateral blocking of legal content. Next to these restrictions, the e-Commerce Directive stipulates that a general monitoring obligation cannot be imposed on ISPs, which may also impose limits to the legal possibilities of internet blocking.[287] This

---

285 Article 15 (2) Charter of Fundamental Rights.

286 Article 16 Charter of Fundamental Rights. See also the Opinion of AG CRUZ VILLALÓN, Case C-134/12, UPC Telekabel, EU:C:2013:781, §95.

287 Article 15.1 e-Commerce Directive.

however has not stopped the issuance of blocking orders in practice, which has led to various cases at the ECtHR and the CJEU (*cf. infra*).
Because of efficiency and legal concerns, the EU remains reserved in its policy towards the blocking and deletion of online illegal content and does not encourage it.

EXCEPTIONS. - An exception is the EU's policy with regard to combating the sexual abuse, sexual exploitation of children and child pornography.[288] The EU also shows itself more flexible towards blocking of online data, and which is of great importance with regard to identity theft, is in the context of the processing of inaccurate, incomplete or no longer up-to-date personal data. In the context of data protection law, the rectification, blocking or erasure of data is even recognized as a right of the data subject (*cf. infra*). Yet in general, the blocking of access is not a requirement under EU law. The 2005 Framework decision on Attacks against Information Systems[289] for example did not address this issue, nor does the Directive 2013/40/EU which has replaced the Framework Decision.[290] In several policy documents concerning cybercrime, the European Commission expresses its concerns towards internet blocking because of the direct economic impact of the measure for ISPs and internet users and its ineffectiveness as in most cases blocked websites simply reappear under another name outside the EU's jurisdiction.[291] This is exactly what happened in the fight against the illegal website the *Pirate Bay*, which we will discuss further on, and which gives some food for thought with regard to internet blocking. First we will examine the current legal possibilities of internet blocking.

3.3.2 Legal basis for blocking data

ERASURE OR BLOCKING OF PERSONAL DATA BY THE 'DATA CONTROLLER'. – When the identification information is linked to the wrong person as a consequence of identity theft, it is of great importance to rectify this situation as soon as possible. Keeping this in mind, we will take

---

288 Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, *OJ* L 013 20.01.2004, 44.

289 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

290 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

291 Cf. overview given by Y. AKDENIZ, 'To block or not to block: European approaches to content regulation, and implications for freedom of expression', *Computer Law & Security Review* 2010, 26, 262., 263.

a look at the EU instruments and the case law of both the CJEU and the ECtHR on the blocking and erasure of data.

EU DATA PROTECTION LEGISLATION. - Because the matter of identity theft is related to personal data and the right to data protection of the victim, the principles set out by the Data Protection Directive and responsibilities of data controllers with regard to the processing of personal data will apply. The conditions for the processing of personal data are defined in articles 6 and 7 of the Data Protection Directive.[292] The data controller[293] has the task of ensuring that personal data are processed '*fairly and lawfully*'[294], that they are '*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*'[295], that they are '*adequate, relevant and not excessive in relation to the purposes for which they are collected and/ or further processed*',[296] that they are '*accurate and, where necessary, kept up to date*',[297] and finally, that they are '*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed*'.[298] The CJEU concluded in *Google Spain* that in this context, the controller must take every reasonable step to ensure that data which do not meet the requirements of that provision are erased or rectified.[299] The General Data Protection Regulation sets out the same, yet slightly differently phrased, principles for the processing of personal data. Each principle now carries its official name, in parenthesis,

---

292 And in articles 5, 6, 7 and 8 General Data Protection Regulation that will apply from 25 May 2018 *(supra).*

293 Defined in article 4 (7) General Data Protection Regulation. See also Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of 'controller' and 'processor'', WP 169, 16 February 2010; B. VAN ALSENOY, 'Allocating responsibility among controllers, processors, and 'everything in between': the definition of actors and roles in Directive 95/46', *Computer, Law & Security Review* 2012, Vol. 28, 25-43.

294 Article 6 (1) a Data Protection Directive, see also article 5 (1) a GDPR.

295 Article 6 (1) b Data Protection Directive, see also article 5 (1) b GDPR.

296 Article 6 (1) c Data Protection Directive, see also article 5 (1) c GDPR.

297 Article 6 (1) d Data Protection Directive, see also article 5 (1) d GDPR.

298 Article 6 (1) e Data Protection Directive, see also article 5 (1) e GDPR. Article 5 of the General Data Protection Regulation adds another responsibility for the controller, namely that the personal data are 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'. The regulation shall apply from 25 May 2018 (*Supra).*

299 Judgment of 13 May 2014, Google Spain C-131/12, EU:C:2014:317, paragraph 72.

after being laid down in the Regulation's text: '*lawfulness, fairness and transparency*', '*purpose limitation*', '*data minimisation*', '*accuracy*', '*storage limitation*'[300] The Regulation also adds some principles. In subparagraph a) the transparency principle[301] and under f) the appropriate security of the personal data is added as a condition for processing ('*integrity and confidentiality*' principle).[302] Under the GDPR the controller shall be responsible for and must be able to demonstrate compliance with, all these principles.[303] Furthermore, when the processing of data is based on consent, the data subject will be able to withdraw his or her consent at any time.[304] Article 5 of the Data Protection Directive set out the lawful grounds for processing: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, public interest, and overriding interest of the controller. They remain largely the same under article 6 GDPR.[305]

RECTIFICATION, ERASURE OR BLOCKING OF DATA. - Article 12(b) of the Data Protection Directive provides that Member States are to guarantee every *data subject* the right to obtain from the controller, as appropriate, the *rectification, erasure or blocking* of data, the processing of which does not comply with the provisions of the directive, in particular because of the incomplete or inaccurate nature of the data.[306] Subject to the exceptions permitted under article 13 of the Data Protection Directive, all processing of personal data must comply, first, with the principles relating to data quality set out in article 6 of the Directive and, secondly, with one of the criteria for making data processing legitimate listed in article 7

---

300 P. DE HERT and V. PAPAKONSTANTINOU, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?', *Computer law & Security Review* 2016, (179) 185.

301 Article 5 (1) a GDPR.

302 Article 5, f GDPR: 'Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').'

303 Article 5(2) GDPR.

304 Article 7 (3) GDPR: The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

305 For a comparison between both articles see P. DE HERT and V. PAPAKONSTANTINOU, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?', *Computer law & Security Review* 2016, (179) 186.

306 The GDPR sets out these rights in more detail in articles 16 (right to rectification), 17 (right to erasure) and 18 (right to restriction of processing) of the GDPR.

of the Directive. Deletion or blocking will therefore be useful in the case where the data have been obtained or are being used unlawfully. Article 14 further grants the data subject a right to object to the processing of his or her data.[307] The data subject must have compelling legitimate grounds relating to his or her particular situation in order to object. This will normally be the case in the context of identity theft. For valid claims, the data controller must fully erase the data, inform the requester of the outcome and communicate the erasure request to any downstream recipients who got the data from the controller.[308] This mechanism thus aims to guarantee a real 'cleaning up'.

REQUEST TO THE DATA CONTROLLER -These rights are to be exercised vis-à-vis the data controller. The data subject may address his or her request directly to the controller who must then duly examine its merits and, as the case may be, end the processing of the data in question (*cf. infra*, Google Spain). Each supervisory authority has investigative powers and effective powers of intervention enabling it to order the blocking, erasure or destruction of data or to impose a temporary or definitive ban on such processing (art. 28 (3) and (4)).
This procedure thus construes a form of 'notice and take down' in the data protection framework.[309]

PRINCIPLES SET OUT IN GOOGLE SPAIN. – In the case *Google Spain*, the CJEU had to examine to what extent the operator of a search engine is obliged to erase data under the Data Protection Directive on request of individuals whose name is used as a search query. It stated that a search engine can be a data controller and can be obliged to erase or block personal data when the processing of that data is incompatible with the Directive.[310] This may result from the fact that such data are inaccurate, inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific purposes.[311] The Court, referring to article 6 (1) c to e, therefore

---

307 Cf article 21 GDPR.

308 Article 12 (c) Data Protection Directive.

309 D. KELLER, 'A Right to be forgotten for hosting services?', CIS 30 April 2015, http://cyberlaw.stanford.edu/blog/2015/04/right-be-forgotten-hosting-services.

310 Judgement of 13 May 2014, Google Spain, C-131/12, EU:C:2014:317, §92.

311 *Ibid*.

states that even initially lawful processing of accurate data may, in the course of time, become incompatible with the Directive where those data are no longer necessary in the light of the purposes for which they were collected or processed.[312] That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.[313]

However, inasmuch as the measure could, depending on the information at issue, have effects upon the economic interest of the operator or the search engine and the legitimate interest of internet users potentially interested in having access to that information, a fair balance should be sought in particular between those interests and the data subject's fundamental rights under articles 7 and 8 of the Charter.[314] Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, the interests of operators of search engines and internet users, that balance may however depend, in specific cases, *on the nature* of the information in question, *its sensitivity* for the data subject's private life and on *the interest of the public in having that information*, an interest which may vary, in particular, according to the role played by the data subject in public life.[315] The CJEU therefore, again, underlines the importance of balancing between opposing rights and interests. It however seems to favour the privacy interests of the individual.

THE 'RIGHT TO BE FORGOTTEN' IN THE GDPR. – Article 17 of the GDPR foresees in a right to erasure, also known as 'the right to be forgotten'. This article partly draws from the *Google Spain* judgement.[316]

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. The controller has to erase where one of the following grounds apply: (a) the personal data are no longer necessary for the purpose collected or processed,[317] (b) the data subject withdraws consent and no legal grounds for processing remain; (c) the data subject objects to the processing pursuant to Article 21(1)

---

312 *Ibid,* §93.

313 *Ibid,* §94.

314 *Ibid,* §99. The CJEU did not assess the compatibility of the measure with the e-Commerce directive (cf. infra).

315 Judgement of 13 May 2014, *Google Spain,* C-131/12, EU:C:2014:317, § 81 Cf. also case law of ECtHR

316 M. KRZYSZTOFEK, ''The Right to be Forgotten' on a swing', *EBLR* 2016, (865) 867.

317 This approach was at the core of the *Google Spain* case (see supra).

and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services directly to a child, under the consent to data processing.[318]

Option (a) corresponds with the prohibition in article 5 (1) e of the GDPR and article 6 (1) e of the Directive to keep personal data in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed. Option (c) refers to article 21 GDPR that contains the 'Right to object'.[319] With regard to option (d), lawful processing is specified in article 6 of the GDPR and article 7 of the Directive.
In case of ID theft a claim to erase data can be made under article 17 (1) d.

INFORM OTHER CONTROLLERS. - Following paragraph 2 of article 17 a data controller that has an obligation to erase data under article 17 (1) must also take reasonable steps to inform other controllers of the data subject's request to erase all links to, or copy or replication of, those personal data. 'Reasonable' is to be considered in the light of the available technology and the cost of implementation.[320] Once data is published on the Internet it is available to an unlimited and unspecifiable pool of recipients and further controllers.[321] It is impossible to find all such data and their respective further controllers. Therefore the

---

318 For a detailed explanation of all of these grouds see: M. KRZYSZTOFEK, ''The Right to be Forgotten' on a swing', *EBLR* 2016, (865) 868-871.

319 Paragraph 1 of this article reads as follows: 'The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Paragraph 2 states: 'Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.'

320 Article 17 (2) GDPR, see also recital 66 of the GDPR.

321 M. K KRZYSZTOFEK, 'The Right to be Forgotten' on a swing', *EBLR* 2016, (865) 871.

GDPR thrives for a practicable effectiveness of the 'right to be forgotten'.[322] The controller only has a duty to inform and should not take legal steps against further controllers if they disregard the notification of an erasure of data.[323]

EXEMPTIONS TO THE RIGHT OF ERASURE. - Paragraph 3 states exemptions to the right to erasure. In short, there shall be no obligation to erase if processing is necessary a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health; (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or; (e) for the establishment, exercise or defence of legal claims.

TOO MANY RESPONSIBILITIES DATA CONTROLLER? - It is up to the data controllers, often private companies, to scrutinize the erasure request. In theory, data controllers should only comply if the request is legitimate. Yet, as there are no specific guidelines in the Data protection Directive nor in the new regulation to investigate complaints, that entity is left with little direction on how to assess the data subject's claim. The CJEU set out some directions in *Google Spain*. However, it remains to be seen whether these are sufficient (*cf. infra*). The notion of 'data controller' is furthermore very broad and also envisages SMEs all over Europe and beyond. Are all these data controllers capable of dealing with this complex issue? It remains unclear how the data controllers handle concrete complaints in practice. Do they for instance react to any request in any language? Which and whose legal interests do they have to take into account? If they also take their own interests into account (f.i. costs etc.) they become judge in their own case. Critics fear that in order to avoid risks and costs, data controllers will simply comply with any request and that this will lead to over-removal of legal online content.[324] This leads us to the more fundamental

---

322 *Ibid*.

323 On the evolving concept of the right to be forgotten at successive stages of work on the GDPR see M. KRZYSZTOFEK, 'The Right to be Forgotten' on a swing', *EBLR* 2016, 871-872.

324 D. KELLER, 'THE GDPR's Notice and Takedown Rules: Bad News for Free Expression, But Not Beyond Repair', The Center for Internet and Society, Stanford Law School, http://cyberlaw.stanford.edu/blog/2015/10/gdpr%E2%80%99s-notice-and-takedown-rules-bad-news-free-expression-not-beyond-repair

question: is it up to private companies to balance these fundamental rights? Article 18 GDPR furthermore states that the data controller must restrict public access to the disputed data, before assessing its validity. In a case of identity theft, this is of course an important tool to end the offence as soon as possible. Critics however warn that such automatic removal is '*a tool begging for use by bad actors with short-term issues*.'[325] In the context of identity theft, one might think about the example of somebody who pretends to be someone else in order to request for removal. This brings us to a specific point of interest in the context of identity theft, notably the concern that the requester is actually the individual whose personal data are at stake. It remains an open question how the data controller in some cases will be able to verify the identity of the data subject.

IDENTIFYING THE SUBJECT. - From article 11 (2) GDPR follows that a data subject cannot exercise its rights under articles 15 to 20, including the right to rectification and the right to erasure, if the controller is not in a position to identify the data subject. Article 12 (6) states that the controller may request the provision of additional information necessary to confirm the identity of the data subject.[326] If we would accept the idea that a data controller should decide upon erasure requests, we should also give that entity the necessary tools to verify the identity of the claimer without evidentially creating new threats to privacy. Technology in order to protect privacy might help. Again the Project tool can prove to be of great value here, since identification through the tool gives more safeguards regarding one's true identity.

NOTICE AND TAKE DOWN BY INTERNET INTERMEDIARIES. – Internet intermediaries play a pivotal role in the distribution of online information, by providing access to online information (internet access providers) or by storing and making the online information available (internet host providers).[327] Because they provide the necessary technical means to

---

325 *Ibid.*

326 Article 12 (6) GDPR.

327 Online intermediaries provide the platforms or act to intermediate between two or more communicators on the internet for the purpose of sending, receiving, sharing or downloading information. Definition formulated by M. A. ARAROMI. (M. A. ARAROMI, 'Determining the liabilities of internet service providers in cyber defamation: a comparative study', *C.T.L.R.* 2016, (123) 123.)

Online intermediaries can be divided into three groups: connectivity intermediaries (e.g. ISPs) navigating intermediaries (e.g. Google) and commercial and social network providers (e.g. Facebook, Twitter etc.) (K.N. ASARI and N. I. NAWANG, 'A Comparative Legal Analysis of Online

transmit, access and store the online information, the question arises to what extent these services also come with certain responsibilities, for example in the case of storage of or access to *illegal* information. Unlike 'traditional' publishers and broadcasters, internet intermediaries do not (and may not) actively control the information they store, transmit or render accessible. This is to avoid private censorship and enhance freedom of speech. As a consequence, they do not face the same responsibilities.[328] This liability issue of intermediary ISPs who provide services of mere conduit, caching and/or hosting is handled by the e-Commerce Directive.[329] Article 12 (mere conduit), article 13 (caching) and article 14 (hosting) state that the providers of these services are not liable for the information they transfer, store or render accessible as long as they are 'neutral'. This means that activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of, nor control over the information which is stored.[330]

LIMITS TO BLOCKING ORDERS.– Article 15.1 e-Commerce Directive forbids Member States to impose a general obligation on service providers under article 12-14 to monitor the information which they transmit or store. They cannot create a general obligation actively to seek facts or circumstances indicating illegal activity either. ISPs do not have to act as internet watch dogs. However, Member States can oblige ISPs promptly to inform the competent public authorities of alleged illegal activities or information provided by recipients of theirs services. Member States can also compel ISPs to comply with the request of competent authorities to provide information enabling the identification of recipients of their services with whom they have storage agreements.[331] Recital 47 explicitly bars Member States from imposing a monitoring obligation on service providers only with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national

---

Defamation in Malaysia, Singapore and the United Kingdom', *International Journal of Cyber-Security and Digital Forensics* 2015, (123) 322.)

328 Search engines after Google Spain, 58.

329 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce), OJ 2000 L 178, p. 1.

330 Cf. Recitals (42) and (44) e-commerce Directive; Judgement of 23 March 2010, *Google France,* joined case C-236/08, C-237/08 and C-238/08, EU:C:2008:389.

331 Article 15 (2) e-Commerce Directive.

authorities in accordance with national legislation, i.e. the interception of electronic communication in specific criminal proceedings.
So in essence, ISPs may be obliged to block access to a website or remove illegal information in order end an infringement and to prevent further infringements unless this leads to a general monitoring obligation. Measures to end as well as measures to prevent infringements are allowed according to CJEU case law.[332] However, it is thus prohibited to impose an obligation to monitor actively all the data of each customer in order to prevent any future infringement. Such an obligation would also be disproportionate.[333]

SCOPE OF THE BLOCKING ORDER. - The e-Commerce Directive does not deal with the actual issuance of blocking orders. It only states that its limited liability regime '*shall not affect the possibility for a Court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement*'[334] Recital 46 adds to this that '*the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression*'[335] With regard to internet host providers, article 14.3 of the e-Commerce Directive explicitly states that this includes the removal of illegal information or the disabling of access to it. [336]

END OF NEUTRALITY. - The neutrality of service providers ends as soon as they actually take note of illegal activities committed with their services, for instance through notification by a user, a victim or law enforcement agencies. In order to benefit further from the exemption of liability, the internet host provider has to act expeditiously to remove the information concerned or to disable access to it.[337] The e-Commerce Directive only

---

332 Cf.Judgement of 27 March 2014, *UPC Telekabel,* C-314/12, EU:C:2014:192, § 37; Judgement of 24 November 2011, *Scarlet Extended,* C-70/10, EU:C:2011:771, § 31 and Judgement of 12 July 2011, *L'Oréal and Others*, C-324/09, EU:C:2011:474, § 131.

333 Judgement of 12 July 2011, *L'Oréal and Others*, C-324/09, EU:C:2011:474, § 139. This case was related to intellectual property – rights infringements.

334 Article 12 (2), 13 (2) and 14 (3) e-Commerce Directive.

335 Recital 46; A. KUCZERAWY, 'Intermediary liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative', ICRI Working Paper 21/2015, 6.

336 Cf. articles 12.3, 13.3 and 14.3 and Recitals (45) and (47) of the directive. The removal or disabling is only provided for hosting services. Recital (45) however seems to apply to all three services.

337 Article, 14 (1) b and recital (46) e-Commerce Directive.

introduces this principle for intermediaries who *store* the information and not for the providers of mere conduit and caching (see *infra).*

According to Belgian law, for instance, as soon as the internet host provider has knowledge of unlawful activities, it immediately has to inform the public prosecutor, who can take the necessary measures on the basis of article 39*bis* Belgian Criminal Procedure Code, the procedural measure of digital seizure (*cf. infra*). While awaiting of the decision of the public prosecutor, the internet host provider can only take the necessary steps to render the information (temporarily) inaccessible. This automatic temporary blocking by the intermediary seems useful in cases of flagrant illegal activities, such as child pornography, terrorism etc. Yet in other, less obvious cases, it remains risky to put the removal of data in the hands of a private party, even if it is only temporarily (*cf. supra*). Much will depend on the required level of the 'knowledge standard' and whether this can actually set a bar for removal.[338] It is thus of utmost importance to give the intermediary the necessary tools in order to verify the identity of the requester without creating new privacy risks (*cf. supra*).
In Belgium it is thus the public prosecutor who has to determine the legitimacy of the request. This brings us to the question of the legal basis of internet blocking in criminal procedures.

BLOCKING ORDERS IN CRIMINAL PROCEDURES. – Internet blocking or a notice and take down measure in order to end a crime and/or to avoid further damage were not a common feature in a 'classic' criminal procedure, which focused on evidence gathering and prosecution (the process of establishing 'the truth').[339] It is therefore not evident that 'classic' investigative measures, such as seizure, cover this specific measure. Two international legal instruments indirectly deal with this matter: Recommendation (95)13 and the Cybercrime Convention.

---

338 D. KELLER argues that the knowledge standard can set a much higher bar for removal than in the Data Protection Regulation where the data controller prior to assessing the validity, temporarily suspends or restricts the data so that it is no longer available. (D. KELLER, 'THE GDPR's Notice and Takedown Rules: Bad News for Free Expression, But Not Beyond Repair', The Center for Internet and Society, Stanford Law School, http://cyberlaw.stanford.edu/blog/2015/10/gdpr%E2%80%99s-notice-and-takedown-rules-bad-news-free-expression-not-beyond-repair)

339 B.-J. KOOPS, 'Tijd voor computercriminaliteit III', *NJB* 2010, 1982.

Recommendation (95)13 states that: '*Criminal procedural laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general against search and seizure should be equally applicable in case of search in computer systems and in case of seizure of data therein*.'[340] Recommendation (95)13 further states that '*Subject to legal privileges or protection, most legal systems permit investigating authorities to order persons to hand over objects under their control that are required to serve as evidence. In a parallel fashion, provisions should be made for the power to order persons to submit any specified data under their control in a computer system in the form required by the investigating authority*'.[341]

According to article 19 Cybercrime Convention, each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or *similarly secure* computer data. Article 19 applies to stored computer data.[342] To secure the data means to maintain its integrity, to make sure that the data remains unchanged during the time of criminal proceedings. The term is included to reflect other means by which the control over or the taking away of intangible data is executed, such as the power *to render inaccessible or remove those computer data in the accessed computer system* (art. 19 §3 d).[343] The rendering inaccessible can include the technologically denying anyone access to that data. This can be useful when harm is involved, such as the spreading of a virus, or when the content of the data is illegal.[344]

The aim of a seizure usually is that the suspect is temporarily deprived of the control over the data, but it can be returned following the outcome of the criminal investigation. To seize or similarly secure data normally has two functions: 1) to gather evidence, such as by copying the data, or 2) to confiscate data, such as by copying the data and subsequently rendering the original version of the data inaccessible or by removing it.[345] The term 'removal' is intended to express the idea that while the data are removed or rendered

---

340 Recommendation (95)3, under I. Search and Seizure, point 2.

341 Recommendation (95)3, under III. Obligations to co-operate with the investigating authorities, point 9.

342 Explanatory Report to the Convention on Cybercrime, § 190

343 *Ibid,* § 197.

344 *Ibid,* § 198.

345 Explanatory Report to the Convention on Cybercrime, § 199.

inaccessible, it is not destroyed, but continues to exist. The rendering inaccessible of data can include encrypting the data or otherwise technologically *denying anyone access to that data*. This measure could usefully be applied in situations where danger or social harm is involved, such as virus programs or instructions on how to make viruses or bombs, or where the data or their content are illegal, such as child pornography.[346] This might also be useful in the case of identity theft, f.i. when 'stolen' personal data, such as passwords, are exchanged online or when somebody is defamed by someone abusing someone else's identity. So 'blocking' is not just seen as an investigative measure in order to gather evidence but also to prevent further harm.

Article 19, § 4 introduces a specific duty to cooperate. It contains a coercive measure to facilitate the search and seizure of computer data. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted. This provision therefore allows law enforcement to compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure.[347] This power is not only of benefit to the investigating authorities. Without such co-operation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that would be denied access to data during this time. A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data.[348]

In a recent criminal law case against intellectual property infringements, the procedural measure of digital seizure has been accepted as the legal basis to block access to a website: *the Belgian Pirate Bay* Case. This case illustrates the relationship between blocking orders issued by law enforcement and the principles set out in the e-Commerce Directive.

---

346 *Ibid*, § 198.

347 *Ibid*, §200.

348 *Ibid, §*§ 200 and 201.

EXAMPLE: THE BELGIAN PIRATE BAY CASE.[349] – In the Belgian case against The Pirate Bay, the Court of Cassation accepted the blocking of access to a website by Internet Access Providers as a form of digital seizure ('databeslag/'saisie des données).[350] The legal basis was article 39*bis* Belgian Criminal Procedure Code (Belgian CPC), which is inspired by Recommendation 95(14) and article 19 Cybercrime Convention. In this case, the Belgian Anti-Piracy Federation had submitted an official complaint to the investigating judge for intellectual property offences via the Swedish website 'The Pirate Bay'. On the basis of article 39bis Belgian CPC, the investigating judge ordered all the Belgian operators and Internet Access Providers to block access to the content hosted by the server connected to 'thepiratebay.org', and more precisely to make use of '*all the possible technical measures*', including at least the blocking of all the domain names that refer to the server connected to the main domain name 'thepiratebay.org'.[351]

As a consequence, the ISPs were obliged to check whether a domain name referred to the illegal website 'thepiratebay.org' and if it did, to block access to this domain name. The ISPs however lodged an appeal against this 'blocking order'. They argued that 1) art. 39*bis* Belgian CPC did not provide a legal basis for this type of order and 2) such order would imply a general monitoring duty which is incompatible with article 15 e-Commerce Directive and the jurisprudence of the European Court of Justice (*cf. infra*).

In regard to the first argument, the ISPs held that the purpose of the coercive measure of a seizure, and therefore also digital seizure, is to obtain criminal evidence and to make sure that law enforcement takes control over the data for the duration of the criminal

---

349 Cass. 22 oktober 2013, AR P.13.0550.N/1; Cf. R. SCHOEFS, 'Strijd tegen The Pirate Bay over andere boeg gegooid: databeslag toegestaan', *T. Strafr.* 2014, 136.

350 Cf. also the Italian Pirate Bay case where the Italian Supreme Court also accepted this (case of 29 September 2009, nr. 49437/09)

351 In 2009 he Pirate Bay (TPB) was already convicted in Sweden by the Stockholm District Court. Four members were found guilty of assistance to infringe copyright and sentenced to jail time and significant fines. In 2010 the appeal court shortened the prison sentences, but increased damages. The confiscation of their services by Swedish authorities resulted in a three day outage. (Stockholm District Court (*Tingsritten*)17 April 2009, case no. B 13301-06, for an unofficial English translation: http://www.ifpi.org/content/library/Pirate-Bay-verdict-English-translation.pdf; Court of Appeal (*Hovr-tten*) 26 November 2010, case no. B 4041-09.; S. LARSSON, 'Metaphors, law and digital phenomena: the Swedish pirate bay court case', *International Journal of Law and Information Technology* Vol. 21 2013, 354-379.) However the Pirate Bay was never shut down permanently due to its complex distributed server structure. Since 2012, they have moved all their servers to various cloud providers. This makes them even harder to trace. Moving to the cloud lets TPB move from country to country, crossing borders seamlessly without downtime. All the servers don't even have to be hosted with the same provider, or even on the same continent. (S. EETEZADI and P. KOKX, 'Why hasn't anyone shut down The Pirate Bay permanently?', *Quora*, https://www.quora.com/Why-hasnt-anyone-shut-down-The-Pirate-Bay-permanently)

proceedings. The aim of seizure is temporarily to deprive the suspect of the data. According to the ISPs, seizure could not be used as the legal basis to compel internet access providers to block access to an illegal website, because it does not prevent the suspect from accessing the illegal content he or she hosts on the main server. Seizure is not intended to end an infringement or to protect the interests of the victim.

The Court of Cassation did not follow the argumentation of the ISPs. It stated that article 39*bis* Belgian CPC provides a valid legal basis for the blocking of access to a website to end behaviour that seems to constitute a crime and to protect the interests of the victim. In order to do so, the investigating judge can order internet access providers to block access to the illegal website. It is not necessary that the host himself can no longer consult that data.[352]

Regarding the second argument, the Court stated that the fact that the ISPs were ordered to take all the possible technical measures to block the access to the website, does not establish a general monitoring duty as they were not ordered to monitor the content or to actively seek facts or circumstances indicating illegal activity.

CLEAR LEGAL BASIS? - If one would follow the reasoning of the Belgian Supreme Court, the blocking of access to a website in order to end a crime and to prevent further damages could take the form of a seizure as a criminal procedure measure. An important consequence is that the *ratione personae* scope of blocking orders could be extended to *any person*, not only 'data controllers' or internet hosting providers. It is however doubtful whether the Belgian article with regard to digital seizure provides a clear enough legal basis in the light of articles 8.2 and 10.2 ECHR (*cf. infra*). Criminal seizure is furthermore a temporary measure. It remains unclear what will happen with this measure once the criminal judge has to decide on the merits of the case.[353]

Better would be to introduce a clear specific legal basis for this measure. The Netherlands is currently debating about the implementation of a 'notice and take down' in criminal procedures which would apply to all providers of communication services.[354] The envisaged article 125p of the Dutch Criminal Procedure Code would clearly state that they

---

352 Cass. 22 oktober 2013, AR P.13.0550.N/1, §12.

353 Since there is currently no legal basis for definite internet blocking as far as we know of. On 9 July 2015, the (Criminal) Court of first Instance acquitted all the suspects. It however remained silent about the blocking measure. The case is now pending before the Antwerp Court of Appeal.

354 Article 125p Dutch Criminal Procedure Code in the Proposal for a Law on Computer Crime III.

can be ordered immediately to take all the reasonable measures to render certain data inaccessible in order to end a crime or to prevent new crimes. This legal proposal however does not address certain issues, such as providers located abroad (*cf. infra*), the freedom to conduct business or the risk of censorship. Under the Dutch proposal the blocking can only be ordered by a judge at the request of the public prosecutor and not by the victim or the administration.[355] Internet blocking may touches upon different fundamental human rights so that a European initiative, which clearly demarcates the limits of this type of measure thereby taking into account European legal standards and policy, seems appropriate. Both the ECtHR and CJEU have already dealt with issues of internet blocking.

3.3.3 Principles on the basis of the case law of the CJEU and the ECHR

DELICATE BALANCING OF RIGHTS. – The general principles of blocking orders directed at ISPs were further elaborated in the case law of the CJEU. Until now, legal questions of intermediary responsibility have mainly been touched upon in the (non-criminal law) context of intellectual property rights, where there are different interests at stake than in the context of identity theft. These cases nonetheless shed some light on the Court's view on the limits of blocking orders.

FILTERING MECHANISM. - In *Scarlet Extended,* the CJEU had to check whether a filtering mechanism was compatible with article 15 of the e-Commerce Directive and with the fundamental human rights in the Charter.[356] Sabam, a management company which represents authors, composers and editors of musical works, brought proceedings against Scarlet, an internet access provider. It claimed that Scarlet was best placed to end copyright infringements committed by its users by blocking or making it impossible for its users to send or receive copyright infringing files. In order to do so, Scarlet would first have to identify files containing copyright infringements. Thereto it had to filter any communication of data passing through its network, in order to detect or, if preferred, to isolate those indicating an infringement of copyright.[357] Scarlet therefore claimed that such obligation would impose a general obligation to monitor as such system would necessarily require general surveillance of all the communications passing through its

---

355 Article 125p, 4 Dutch Criminal Procedure Code in the Proposal for a Law on Computer Crime III.

356 Judgement of 24 November 2011, *Scarlet Extended,* C-70/10, EU:C:2011:771.

357 Conclusion of Advocate General CRUZ VILLALÓN of 14 April 2011, *Scarlet Extended,* C-70/10, EU:C:2011:255, §46.

network. This would also be in breach of European data protection law and the secrecy of communications.

The CJEU ruled that an order to implement a system for filtering 1) *all electronic communications* passing via the ISP which 2) applies indiscriminately to *all its customers*, 3) as a preventive measure, 4) exclusively at its expenses and 5) *for an unlimited period*, in order to detect on its network intellectual property infringements with the view of blocking the transfer of such IP infringing files is indeed not compatible with article 15 e-Commerce Directive. The Court also examined the order in the light of the requirements stemming from the protection of the applicable fundamental rights. It found that such system would violate fundamental human rights, as it disproportionately protects the fundamental right to property, including the intellectual property rights, to the detriment of the protection of other fundamental human rights, such as the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information (articles 16, 8 and 11 of the Charter).
Although this case only relates to the permissibility of a *filtering* mechanism in the light of article 15 e-Commerce Directive and fundamental human rights, it does make clear that any system that imposes obligations on ISPs must strike a fair balance between the applicable human rights. To that extent, the CJEU valued the fact that the monitoring 1) would require the installation of a complicated, costly, permanent computer system at the own expenses of the ISPs, 2) would lead to the systematic analysis of all content and the collection and identification of IP addresses which are protected personal data and 3) might not distinguish adequately between lawful and unlawful content and could lead to the blocking of lawful communications. Therefore the filtering mechanism was a disproportionate measure.

NO SPECIFICATION REQUIRED. – In *UPC Telekabel*[358] the CJEU examined whether an order in general terms (thus without ordering specific measures) to block access to a website infringing copyright is compatible with EU law, in particular with the necessary balance between the parties' fundamental rights. The Court had to interpret among others Article 8 (3) Directive 2001/29.[359] This article states that Member States must ensure that holders

358 Judgement of 27 March 2014, *UPC Telekabel,* C-314/12, EU:C:2014:192.

359 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, OJ 2001 L 167, p. 10.

of IP rights can apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right. These measures are aimed not only at bringing to an end to such infringements of copyright and related rights, but also at preventing them.[360] Such preventive effect presupposes that it does not have to be proven that the ISP's customers actually access illegal content.

The Court underlined that the specific conditions to be met and the procedure to be followed for such injunctions are a matter of national law.**[361]** When transposing a directive Member States must however ensure that they rely on an interpretation of the Directive which '*allows a fair balance to be struck between the applicable fundamental rights protected by the European Union legal order*'.**[362]** So the national law must be interpreted in conformity with the Directive and the fundamental human rights and other general principles of EU law, such as the principle of proportionality.

The applicable fundamental rights were intellectual property on the one hand, and the freedom to conduct business and the freedom of information and the other.[363] The CJEU first ruled that a blocking order in general terms indeed restricts the freedom to conduct business as it obliges ISPs to take measures which may represent a significant cost, have a considerable impact on the organisation of its activities or require difficult and complex technical solutions. On the other hand, it does not seem to infringe the *very substance* of that freedom for two reasons:**[364]**

- It leaves it to the ISP to determine the specific measures to be taken so that he can choose measures which are best adapted to his resources and abilities, and to his other obligations and challenges.**[365]** So, perhaps somewhat surprisingly, the CJEU valued the open-ended formulation of the blocking order in a positive way because it left the concrete elaboration to the ISP's appreciation.
- It allows the ISP to avoid liability by proving that it has taken all *reasonable* measures. The effort matters, not the result. The ISP will not be obliged to make

---

360 Judgement of 24 November 2011, *Scarlet Extended,* C-70/10, EU:C:2011:771.

361 Judgement of 27 March 2014, *UPC Telekabel,* C-314/12, EU:C:2014:192, §43.

362 Judgement of 27 March 2014, *UPC Telekabel,* C-314/12, EU:C:2014:192, §46.

363 *Ibid,* §47. In this case, the protection of personal data was not at stake as the blocking order did not required any preliminary monitoring of data.

364 *Ibid*, §50-51.

365 *Ibid, §52.*

unbearable sacrifices, which seems justified as he is not the perpetrator of the IP right infringement.[366] Such general blocking order meets the principle of legality when it is possible for the ISP to maintain before the Court that the measures taken were indeed those which could be expected of him in order to prevent the proscribed result.[367]

In paragraphs 56 to 64, the CJEU elaborates the main principles ensuring that the injunction at issue strikes a fair balance between the applicable rights:

- In order to be in compliance with the fundamental right to freedom of information of internet users, the measures taken must be strictly targeted: they must serve to bring an end to the infringement, but without unnecessarily depriving internet users of the possibility of lawfully accessing information;
- There must be a possibility for a judicial review to check this first condition. The national procedural rules must provide a possibility for internet users to assert their rights before the Court once the implementing measures are known and before the stage of the enforcement proceedings;
- The measures taken do not have to be fully effective, they need not ensure a complete cessation of the infringements. A measure can be for instance fully effective but unreasonable in the light of the above. It suffices that the injunction has the effect of preventing unauthorised access to the illegal content or at least of making it more difficult to achieve and of seriously discouraging internet users form accessing the illegal content.

EFFECTIVENESS OF THE BLOCKING MEASURE. – In the *Brein* case, which is still pending before the CJEU, Stichting Brein demanded Dutch ISPs to block access to The Pirate Bay website. The Dutch Supreme Court asked in a prejudicial question to the CJEU whether EU law allows an injunction against an ISP ordering it to block access for its users to an indexing site of a peer-to-peer network by means of which copyright infringements have been committed, even if the operator of that site does not itself communicate to the public the works made available on that network.[368] This situation differs from *UPC Telekabel*, that

---

366 *Ibid,* §53.

367 *Ibid, §54.*

368 Opinion of the Advocate General SZPUNAR of 8 february 2017, *Stichting Brein,* C-610/15, EU:C:2017:99, §57.

concerned the blocking of access to a website whose operator itself was the originator of the copyright infringement.[369] However, in considering whether a blocking measure complies with fundamental rights Advocate General SZPUNAR invoked the principles as outlined in *UPC Telekabel*.[370] Furthermore, the Advocate General underlined that ISPs cannot escape their obligation to block '*by claiming, according to the circumstances, that the measures are either over-restrictive or ineffective*'.[371] He concluded that '*if a measure that is less restrictive for service providers and constitutes less of an intrusion upon the rights of users were now rejected on the ground that it is not sufficiently effective, internet service providers would ultimately be released de facto from their duty to cooperate in the fight against copyright infringement*.'[372]

In the main proceedings, the ISPs had expressed their doubt about the effectiveness of blocking access to TPB.[373] The Dutch Court of Appeals recognised this inefficiency and ordered the injunction at issue be lifted immediately. However, this judgement was rendered prior to the Court of Justice's ruling in *UPC Telekabel,* where it stated that blocking measures should not be fully effective (*supra*).[374] In *Scarlet Extended* the CJEU rejected the blocking of all internet traffic involving work illegally shared on peer-to-peer networks, because it found it too restrictive for ISPs and because it intruded too far upon the rights of users (*supra).*[375]

LIABILITY ISPS HATE SPEECH. – The Grand Chamber of the ECtHR also faced the balancing of rights in the *Delfi* case . An online news portal (Delfi) was found liable under Estonian law for user generated comments containing hate speech and speech that directly advocated

---

369 *Ibid,* §62.

370 *Ibid, §*71-78.

371 *Ibid,* 83.

372 Opinion of the Advocate General SZPUNAR of 8 february 2017, *Stichting Brein,* C-610/15, EU:C:2017:99, §83.

373 In their view, first, that measure is ineffective since the same works can be found and exchanged on the internet by means other than TPB. Secondly, the blocking of a website address can easily be circumvented by any informed internet user. (*Ibid*, §79.)

374 V. MLYNAR, 'Storm in ISP Safe Harbor Provisions: The Shift From Requiring Passive-Reactive to Active-Preventative Behavior and Back', *Intell. Prop. L. Bull*. 2014, (1) 18.

375 Judgment of 24 November 2011, *Scarlet Extended*, C‑70/10, EU:C:2011:771, § 38 to 52.

acts of violence[376] posted on its online news portal.[377] A balance had to be made between article 8 (the right to protection of reputation as part of the Right to respect for private life) and article 10 (Right to freedom of expression).[378] The Court ruled that the liability of Delfi under Estonian law did not infringe upon the freedom of expression. Although it cannot be concluded from this judgement that Member States have a duty to hold internet intermediaries liable for hate speech posted on their platform, the judgement still raises questions.

First of all, we should point out the limited scope of the arrest. The Court emphasised that '*the present case relates to a large professionally managed internet news portal run on a commercial basis which published news articles of its own and invited its readers to comment on them*.'[379] It further stressed that '*the case does not concern other fora on the Internet where third-party comments can be disseminated, for example (…) a social media platform where the platform provider does not offer any content and where the content provider may be a private person running the website or a blog as a hobby.*'[380]

With regard to the notice-and-take-down system that Delfi foresaw the Court ruled that this could function in many cases as an appropriate tool for balancing the rights and interests of all those involved. However, when dealing with third-party user comments in the form of hate speech and direct threats to the physical integrity of individuals '*the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening Article 10 of the Convention, if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties.*' [381]

---

376 This was not scrutinized by the ECtHR. The Court only refers to the assessment of the Estonian Supreme court and states that 'the remarks were on their face manifestly unlawful'. (EHRM 16 juni 2015, *Delfi/Estland,* nr. 64569/09, §117.)

377 EHRM 16 juni 2015, *Delfi/Estland,* nr. 64569/09.

378 *Ibid*, §110.

379 *Ibid*, §115.

380 *Ibid*, §116.

381 *Ibid*, §159.

Similar issues were at stake in the *Magyar* case[382] of the ECtHR. The only substantial difference was that in that case the Court ruled that the comments posted on the online platforms did not constitute '*clearly unlawful expressions, amounting to hate speech and incitement to violence*'[383] Therefore the balance between article 8 and article 10 shifted and the liability of the online platforms was seen as a breach of article 10 ECHR.

The problem with the ECtHR's case law is that the intermediaries have to decide what is manifestly unlawful and what is not. In an annotation of the *Delfi* case, VANDERSLOOT points out that the ECtHR declared the statements as manifestly unlawful, without elaborating on why they were.[384] It only refers to the assessment by the Estonian Supreme Court.[385] This assessment is however not without concern.[386] By laying the responsibility with the online intermediary to decide what is unlawful and what is not, the ECtHR increases the risk – often underscored by the CJEU – of self-censuring by internet intermediaries.[387] As soon as doubt about the lawfulness of content arises, the intermediary may be inclined to remove the information. If it does not, it runs the risk of being held liable. This is problematic because of its impact on the freedom of expression and the freedom to conduct a business.[388]

Legal scholars are convinced that Delfi qualified as a hosting provider under article 14 (1) e-Commerce Directive and thus could not have a general monitoring duty, since this is prohibited by article 15 of the Directive (*supra)*.[389] However, the ECtHR did not question

---

382 EHRM 2 February 2016, Magyar Tartalomszolgáltatók Egyesülete and Indes.hu zrt/ Hungary, no. 22947/13.

383 *Ibid,* §64.

384 B. VANDERSLOOT, 'Annotatie bij Europees Hof voor de Rechten van de Mens 16 juni 2015 (Delfi AS/Esland)', European Human Rights Cases, 2015, nr. 172.

385 EHRM 16 juni 2015, *Delfi/Estland,* nr. 64569/09, §117.

386 K. DE SCHEPPER, 'De Strafrechtelijke aansprakelijkheid van een internetnieuwsportaal voor zijn lezersreactie: het arrest Delfi in de Belgische strafrechtelijke context', *T.Strafr.* 2016, (282) 284.

387 *Ibid*, (282) 284.

388 M. A. ARAROMI, 'Determining the liabilities of internet service providers in cyber defamation: a comparative study', *C.T.L.R.* 2016, (123) 124.

389 L. BRUNNER, 'The Liability of an Online Intermediary for Third Party Content The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v Estonia', *HRLR* 2016, (163) 168-169; K. JANSSENS and T. DE MEESE, 'De aansprakelijkheid van niewswebsites na de Delfi- en Magyar-arresten van het EHRM: Much Ado About Nothing?', *Computerrecht* 2016, 5-9.

the qualification given by the national Courts which decide that it was a publisher.[390] This is not surprising since it is fixed case law of the Court that it is for the national authorities, notably the Courts, to interpret and apply domestic law.[391] However, if this case had been brought before the CJEU, it would have been more than likely that the Court would have ruled that Estonia breached the e-Commerce Directive by holding Delfi liable.

LIABILITY ISPS ID FRAUD? - The question is whether the ECtHR would take a similar approach in the case of ID fraud. For example could internet intermediaries be held liable for fake profiles abusing the identity of another person on their platforms?
Under EU law this would more than likely not be the case since notification is a requirement under the e-Commerce Directive. Even if an individual notifies the abuse, it remains unclear whether an service provider should remove the notified data. How can the ISP be sure that the individual notifying does not himself act in bad faith and/ or that the notified content is indeed compromised? Holding service providers liable only if the notified content is 'manifestly illegal' can minimise the danger of private censuring and over-blocking by service providers, but only if this standard is strictly interpreted. In case of notification by administrative authorities, the public prosecutor, and when confronted with a judicial order, service providers should act promptly without making their own legality assessment, since the content will already be scrutinized by the notifying authorities. Another possibility would be to create a hotline where complaints of ID-fraud can be made, together with an identification center. This identification center can then assess (in cooperation with law enforcement and authorities best placed to verify identities and identification instruments) the complaint and confirm authentic ID of the complainant. In case of ID fraud, they can send a notice and take down request to the service provider (see *infra* III.5).

CONVENTION-COMPATIBLE LEGAL FRAMEWORK. – In a very interesting and clear concurring opinion in the *Yildirim* case[392] , ECtHR-judge PINTO DE ALBUQUERQUE examined the standards set out in the various documents of the Council of Europe and the case law of the

---

390 EHRM 16 juni 2015, *Delfi/Estonia,* nr. 64569/09, §126-127.

391 *Ibid,* §127. This is fixed case law by the ECHR see, among others: EHRM 7 juni 2012, *Centro Europa 7 S.r.l. and Di Stefano/Italy*, nr. 38433/09, § 140, and EHRM 20 May 1999, *Rekvényi/Hungary*, nr. 25390/94, § 35.

392 ECtHR 18 December 2012, *Yildirim/Turkey*, no. 3111/10.

ECtHR with regard to internet blocking. On the basis of his research, he developed the minimum criteria for Convention-compatible legislation on Internet blocking measures[393]:

1) a definition of the categories of persons and institutions liable to have their publications blocked, such as national or foreign owners of illegal content, websites or platforms, users of these sites or platforms and persons providing hyperlinks to illegal sites or platforms which have endorsed them. For instance, a clear legal definition of a content or a service provider should be provided as their responsibilities are different;
2) a definition of the categories of blocking orders, such as blocking of entire websites, Internet Protocol (IP) addresses, ports, network protocols or types of use, like social networking;
3) a provision on the territorial ambit of the blocking order, which may have region-wide, nationwide, or even worldwide effect;
4) a limit on the duration of the blocking order. Indefinite or indeterminate blocking orders constitute *per se* unnecessary interference. Indefinitely valid blocking orders, or blocking orders which remain valid for a long period are inadmissible forms of prior constraint or pure censorship.
5) an indication of the 'interests', that may justify the blocking order[394];
6) an observance of the criterion of proportionality, which provides for a fair balancing of the competing 'interests' pursued;
7) compliance with the principle of necessity, which enables an assessment to be made as to whether the interference with human rights, such as freedom of expression, adequately advances the 'interests' pursued and goes no further than is necessary to meet the said 'social need'. Less draconian measures should be envisaged, for example by implementing a 'notice and take down' policy prior to the issuance of a blocking order;

---

393 Although he focused on article 10 ECHR, we can extend these criteria to the entire convention. Cf. and compare with the in March 2015 adopted Manila Principles. Manila, an international coalition, launched the 'Manila Principles for Intermediary Liability'. These principles are a roadmap for the global community to protect online freedom of expression and innovation around the world. The framework outlines clear, fair requirements for content removal requests and details how to minimize the damage a takedown can do. The principles are not legally binding. They are a set of global baselines to guide the development and implementation of intermediary liability regimes and practice. For more information and the exact principles see https://www.manilaprinciples.org/principles.

394 In the sense of article 8.2 or 10.2 ECRM.

8) a definition of the authorities competent to issue a reasoned blocking order. The fact that many different authorities may issue blocking orders does not enhance legal certainty. This could lead to different interpretations and applications of the law. Better would be to concentrate this power in the hands of one single authority.
9) a procedure to be followed for the issuance of that order, which includes the examination by the competent authority of the case file supporting the request for a blocking order and the hearing of evidence from the affected person or institution, unless this is impossible or incompatible with the 'interests' pursued;
10) a notification of the blocking order and the grounds for it to the person or institution affected;
11) a judicial appeal procedure against the blocking order.

He further underlined that such a framework must be established through specific legal provisions and that neither the general provisions and clauses governing civil and criminal responsibility nor the e-Commerce Directive constitute a valid basis for ordering Internet blocking. According to the judge, any indiscriminate blocking measure which interferes with lawful content, sites or platforms as a collateral effect can never be justified as it lacks a rational connection between the interference and the social need pursued. He concludes that '*when exceptional circumstances justify the blocking of illegal content, it is necessary to tailor the measure to the content which is illegal avoid targeting person or institutions that are not de jure or de facto responsible for the illegal publication and have not endorsed its content*.'

3.3.4 Evaluation

MANY ISSUES TO BE SOLVED. – Many issues with regard to internet blocking remain to be solved. For instance, who should be ordered to block (scope *ratione personae*)? Different entities have different responsibilities which are sometimes hard to fit together and may even collide. This makes a clear overview necessary of which entity has which responsibility and when (*after* being requested or ordered, and thus reactive, or at its own initiative (proactive))? Another question is the scope *ratione materiae* (what should be blocked)? Different laws create different categories of information (f.i. personal data and non-personal data, identification data, meta data and content data). These different categories make it hard to identify the different responsibilities, the applicable laws and the legal interests to be assessed. In the context of identity theft, 'identification data' may at the same time qualify as personal data and as content data, e.g. when somebody uses

another person's picture for his or her Facebook profile. Should Facebook then block the entire profile or merely the 'stolen' picture? Is it Facebook that has to decide what it should do? In the context of data protection law, it is the data controller which decides, while in the context of the e-Commerce Directive, this depends upon the national procedure.

BLOCKING OR REMOVAL IN THE CONTEXT OF IDENTITY THEFT. – This brings us to the next question: which legal safeguards and procedural checks and balances should surround the measure? Taking the different principles all together, we may assume that a blocking order to terminate the identity theft or prevent further damage, is appropriate provided that the following conditions are met:

- First of all, it must be based on a particularly strict legal framework ensuring both tight control over the scope of the ban and effective judicial review to prevent possible abuse, because it could have significant effects of 'collateral censorship' (*cf.* minimum criteria *supra*)[395];
- Secondly, it may not impose a general obligation to monitor on the intermediary ISP. This condition will only apply in case the ISP provides services of mere conduit, caching and hosting.
- Thirdly, the specific measure has to be proportionate in the sense that it must strike a fair balance between the applicable rights and interests, in particular the right to privacy of the individual on the one hand, and the economic interests of the entity and the right to privacy and freedom of information of internet users on the other hand.[396] The measure should leave the concrete elaboration to the ISP's appreciation.[397] The privacy of the individual seems to override as a general rule the economic interests of the entity as well as the interests of internet users. This however may depend on the nature of the information, its sensitivity and the interest of the general public in the information. In case of stolen identification information, it seems that the privacy of the individual will take the upper hand.

---

395 ECtHR 18 December 2012, *Yildirim/Turkey*, no. 3111/10.

396 Cf. also ECtHR, 20811/10, 11 March 2014, *Akdeniz/Turkey* no. 25165/94 where the Court decided that there was no violation of the right to freedom of information of an internet user who claimed to be affected by a blocking measure of a music sharing website. The Court stated that he had been deprived of only one means of listening to music among many others. In addition, he was not deprived of a major source of communication.

397 Thereby taking the data protection principles into account as the entity qualifies at that moment as a data controller.

- Lastly, the blocking measure has to be effective. It suffices that it has the effect of preventing further damages or at least of making it more difficult to achieve the identity theft and of seriously discouraging internet users from accessing the compromising information.

ENFORCEABILITY THROUGH NOTICE BASED LIABILITY. – In the end, the successfulness of such measure comes down to having an effective form of enforceability. The e-Commerce Directive introduces a very specific type of enforceability. It holds the principle that service providers are not responsible for the information they store, transmit or render accessible as long as they are 'neutral'. This means that activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.[398] As discussed earlier, this neutrality however ends as soon as service providers actually take note of illegal activities committed with the aid of their services. They could find such content through their own activities or they could be notified by a third party (a user, a victim or a public authority, *cf. supra*).[399] In the case the host provider is notified by a private entity, he must assess whether the notification is credible. It however remains unclear how they handle concrete complaints. This makes internet host providers judges in their own case.[400] This '*notice based liability*' actually comes down to making internet host providers responsible for maintaining and keeping illegal information accessible. It thus depends on their own decision whether or not they are exempted from liability. They may, however, lack the knowledge to assess the illegality of the content. This assessment is moreover *per definition* a very delicate issue, regarding the diverging points of view on the right to freedom of speech in different states.[401]

---

398 Recital 42 e-Commerce Directive; CJEU C-236/08, C-237/08 en C-238/08, 23 March 2010 (Google/Vuitton);

399 A. KUCZERAWY, 'Intermediary liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative', ICRI Working Paper 21/2015, 6.

400 Ibid., 6.

401 Tribunal de Grande Instance Paris (Superior Court in Paris), 22 May 2000, *UEJF and Licra/Yahoo! Inc. and Yahoo France*, http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm); C. DUB, 'Yahoo! Inc. v. Licra', *Berkeley Technology Law Journal* 2002, (359) 369-370.

This increases the risk of privatized censorship and over-blocking. Needless to say that this regime also implies potential abuse by fictitious victims.[402]

FRENCH YAHOO! CASE. - A good illustration of the fact that the assessment of the legality of data can be complicated by different views on freedom of speech, is the French Yahoo! Case.[403] The Tribunal de Grande Instance convicted Yahoo for allowing their online auction service to be used for the sale of memorabilia from the Nazi period, contrary to Article R645-1 of the French Criminal Code (Code penal).[404] Therefore the Court ordered Yahoo! to take all possible measures to dissuade and block access in France of web pages stored on Yahoo!'s US-based servers. The French Tribunal, relying on expert reports, concluded that Yahoo! could screen nineteen percent of its users as well as the illegal content by using technologies to identify the geographical origin of users (by their IP addresses) and soliciting users' good faith declarations of their nationality. Other possibilities for the ISP to identify users included the purchaser's delivery address and the language used by their internet browser.[405] Subsequently, Yahoo! successfully sought a declaration in the US (its place of incorporation) that the orders made in France were not enforceable under US law on the basis that the orders would breach in the First Amendment of the United States Constitution, which protects freedom of speech.[406] This judgement does not nullify '*the right of France or any other nation to determine its own laws and social policies.*'[407] A US based Internet company like Yahoo! Still needs to comply with French speech regulations if it wished to do business or maintain a physical presence in

---

402 A. KUCZERAWY, 'Intermediary liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative', ICRI Working Paper 21/2015, 7.

403 For an extensive discussion on the french Yahoo case(s) see E. A. OKONIEWSK, 'The French Challenge to free expression on the internet', *Am. U. Int'l L. Rev.* 2002, 295-339 or C. DUB, 'YAHOO! INC. V. LICRA', *Berkeley Technology Law Journal* 2002, (359) 366-378.

404 Tribunal de Grande Instance Paris (Superior Court in Paris), 22 May 2000, *UEJF and Licra/Yahoo! Inc*. *and Yahoo France*, http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm).

405 J. STRACHAN, 'The Internet of tomorrow: the new-old communications tool of control', *E.I.P.R.* 2004, (123) 134-135; C. DUB, 'Yahoo! Inc. V. Licra', *Berkeley Technology Law Journal* 2002, (359) 366.

406 United States District Court, N.D. California, San Jose Division, *Yahoo! Inc. v. La Ligue contre le racism et l'antisemitsme*, 169 F. Supp. 2d at 1194; D. IRELAND-PIPERA, 'The Future Extraterritorial Criminal Jurisdiction: Does the Long Arm of the Law Undermine the Rule of Law?' *Melb. J. Int'l L.* 2012, (122) 136.

407 United States District Court, N.D. California, San Jose Division, *Yahoo! Inc. v. La Ligue contre le racism et l'antisemitsme*, 169 F. Supp. 2d at 1181, 1186.

France.[408] In an attempt to comply with the French Order, Yahoo! amended its policy to also prohibit individuals from auctioning *'[a]ny item that promotes, glorifies, or is directly associated with groups or individuals known principally for hateful or violent positions or acts, such as Nazis or the Ku Klux Klan.'*[409] It is noteworthy that Yahoo! amended its overall policy and did not employ technical measures to identify French users and then filter out Nazi-related propaganda for them. DUB points out that this would have been difficult to achieve and burdensome.[410] Moreover, '*Conducting business in a country-by-country basis is impractical. Even if a website achieves a reasonable level of compliance with the laws of one country, in the end, scalability issues might require most sites to tailor all their content to fit the laws of the most restrictive country*.'[411]

STORAGE REQUIREMENT. - Strangely enough, the e-Commerce Directive only introduces notice and take down obligations for intermediaries who *store* the information and not for the providers of mere conduit and caching. Although these providers obtain actual knowledge or awareness of illegal activities committed through their services, they cannot be held liable if they are in no way involved with the information transmitted. To enjoy this immunity it is necessary that, among other things, they do not modify the information that they transmit. This requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission. However, if they deliberately collaborate with one of the recipients of their service in order to undertake illegal acts goes, this goes beyond the activities of '*mere conduit*' or '*caching*'. As a result, they cannot benefit from the

---

408 C. DUB, 'YAHOO! INC. V. LICRA', *Berkeley Technology Law Journal* 2002, (359) 374.

DUB notes that 'AS long as U.S.- based websites keep all their assets in the United States, they will be protected

against foreign judgments which impose unconstitutional speech restrictions upon them. As a result of this ruling, U.S.-based websites may move all their assets to the United States, so that foreign courts will not be

able to collect on any money judgments.'

409 United States District Court, N.D. California, San Jose Division, *Yahoo! Inc. v. La Ligue contre le racism et l'antisemitsme*, 169 F. Supp. 2d at 186 ; C. DUB, 'YAHOO! INC. V. LICRA', *Berkeley Technology Law Journal* 2002, (359) 375.

410 C. DUB, 'YAHOO! INC. V. LICRA', *Berkeley Technology Law Journal* 2002, (359) 376-377.

411 *Ibid,* 378.

liability exemptions established for these activities.[412] In that sense, this principle of limited liability does not completely quash the '*normal*' criminal liability principles.

Because of the many legal uncertainties and the lack of specific guidelines, including safeguards, with regard to internet blocking through the notice and take down scheme of the e-Commerce Directive, action was needed at EU level. At the moment of writing, a new European Framework for Notice-and-Action is under development.[413] It should however be clear that private entities, such as internet host providers, should not take over the role of judicial authorities in the assessment of the (il)legality of conduct. As already mentioned, in Belgium internet host providers, after being notified about alleged illegal activity, must immediately contact the public prosecutor's office. It is thus the latter who assesses the illegality of the content and decides what action should be taken. In the meanwhile, the internet host provider can only take provisional action. This is a step in the right direction, but it remains to be seen whether a public prosecutor qualifies as an independent and impartial judicial authority.[414]

OTHER WAYS OF ENFORCEMENT. – To further strengthen the enforcement of blocking orders, lawmakers could consider making the refusal to cooperate after being ordered to block a separate, contempt-offence (*cf. supra*). It will however not be easy to implement such type of enforcement in a digital context (*cf. infra*).

The Netherlands are discussing the introduction of a very peculiar, new type of enforcement in criminal procedure. They link the non-compliance of the notice and take down order to the issuance of a periodic penalty payment (een 'dwangsom'). This would be more efficient than a prosecution for non-compliance.[415] Imposing pecuniary damages

---

412 Recital 43 and 44 e-Commerce Directive.

413 Commission Communication to the European Parliament, The Council, The Economic and Social Committee of Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM(2011) 942 final, http://ec.europa.eu/internal_market/e-commerce/communications/2012/index_en.htm#maincontentSec2.

Insiders even indicate that the European Commission is preparing a proposal for a Notice-and-Action Directive. A. KUCZERAWY, 'Intermediary liability & Freedom of expression: Recent developments in the EU Notice & Action Initiative', ICRI Working Paper 21/2015, 16.

414 The ECtHR has generally refused to consider public prosecutors as an independent and impartial tribunal within the meaning of Article 6 § 1 of the Convention. According to the Court, *'the mere fact that the prosecutors acted as guardians of the public interest cannot be regarded as conferring on them a judicial status of independent and impartial actors'* (ECHR, 15 June2006, *Zlínsat, spol. s r.o., v. Bulgaria*, no. 57785/00, § 78; European Court of Human Rights Research Division, *The role of public prosecutor outside the criminal law field in the case-law of the European Court of Human Rights,* Case-law Reports 2011, 4-5.)

415 B.-J. KOOPS, 'Tijd voor Computercriminaliteit III', *NJB* 2010, 1982.

to enforce compliance indeed seems an effective way to compel somebody to do something, when he or she cannot forced be physically or *manu militari*. It however remains a strange idea for continental lawyers to introduce this enforcement technique from civil procedure in their criminal procedures.

Another specific issue which remains to be solved is the enforceability in cross-border context. As this counts for any type of forced cooperation, we will discuss this in the next chapter.

4 Enforceability of forced ISP cooperation in a cross-border context

4.1 Situation *de lege lata*: limits to cross-border law enforcement

COOPERATION ORDERS. - Criminal investigation is the organised gathering of information with a view to establish offences, to identify their perpetrators and to find evidence. It is thus a specific, targeted and proportional collection of information. Typically, in the course of a criminal investigation, i.e. an exercise of State power, investigators can obtain, by compulsion, information which the holder does not want to disclose. Orders can be used in addition to requests.

All the above criminal procedure measures relate to ordering third parties, in particular internet service providers, to cooperate with law enforcement. Given the international context of identity theft, specific attention should be given to their enforceability in an international context. Because internet service providers are often located abroad, their cooperation in criminal investigation will often require international (public-private) cooperation. The Cybercrime convention, which is currently the only binding international instrument dealing with internet-related criminal investigations, tries to develop a more flexible system of international cooperation. Yet, especially on the point of ISP cooperation, it has proven not to be flexible enough. Procedural measures are only effective if all the States have law enforcement functions which can rapidly act and provide effective international assistance for investigations. Traces however often end at a server providing anonymous services in a third country known for its weak international cooperation. That is why law enforcers try to be creative and find other solutions to obtain similar results. The previously discussed Pirate Bay case is an example of this. Blocking access to websites through local telecom operators is an alternative to notice and take down procedure through internet host providers. These are often not effective because the host providers do not react as they do not feel bound by orders of foreign authorities.[416]

---

416 This could however change as the CJEU recently ordered Google to comply with the Spanish Data Protection Law although they are US based. To the extent that the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and *which orientates its activity towards the inhabitants of that Member State,* the processing of personal data falls within the territorial scope of that Member State. (Judgment of 8 April 2014, *Google Spain,* C-131/12, EU:C:2014:317)

UNILATERAL ORDERS? – The (Belgian[417]) *Yahoo* case is another illustration.[418] The Belgian Criminal Procedure Code (Belgian CPC) imposes a duty to disclose the identity of the user of an ICT-application to law enforcement, when ordered to do so by a prosecutor or judge. Failure to comply is punishable with a criminal fine. This article 46*bis* Belgian Criminal Procedure Code can be seen as the Belgian implementation of article 18 Cybercrime Convention. In a national context enforcing Belgian service providers to cooperate poses little problems. But how can Belgium impose this duty to cooperate on a foreign service provider based in a foreign country who delivers internet services in Belgium? In other words, can a company, that delivers internet services globally but is based in a foreign country, ever be required to respond to a cooperation order issued by authorities from other states?

The Belgian public prosecutor tried to enforce it unilaterally. The Belgian prosecution service initiated criminal prosecution of a US dotcom for failure to respond to production orders for user identification data issued by a Belgian prosecutor. The prosecution is based on the assumption that American company Yahoo! Inc. (hereinafter 'Yahoo') fell under Belgian territorial jurisdiction and therefore no mutual legal assistance from the US authorities was required. This case thus revolves around the territorial scope of a duty imposed upon private operators to cooperate with law enforcement authorities during a criminal investigation. This calls into question the limits of the State's jurisdiction to enforce, which is a sensitive issue.[419] Where the classic *Lotus* judgement was flexible on substantive jurisdiction, a sovereign *claim* to power, it was not flexible on executive jurisdiction, a sovereign *exercise* of power. This jurisdiction '*cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom*

---

417 Not to be confused with the French *Yahoo* case on the offer of French prohibited Nazi memorabilia over the Internet (Tribunal de Grande Instance Paris (Superior Court in Paris), 22 May 2000, *UEJF and Licra/Yahoo! Inc. and Yahoo France*, http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm).

418 This case law is now also codified in article 46*bis* Belgian CPC. (Article 5 Wet van 25 December 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *B.S.* 17 January 2017.)

419 C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 24-25; P. DE HERT, 'Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty is at Stake?' in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 102.

or from a convention'.[420] States can therefore, in theory, only exercise their procedural powers within the national borders. But, where do these borders end in the digital environment? Authorities (just like cybercriminals) can investigate information abroad by digital means without physically having to leave their territory.[421] And, as in the *Yahoo* case, they can request information from a foreign service provider via modern means of communication, under the threat of criminal prosecution if refused. This raises the question of whether, through this, the Belgian prosecutor is exercising jurisdiction outside Belgium. Is he, with a request of this kind, exceeding his Belgian-wide jurisdiction or would this procedure be permissible in the light of international law?

NO UNILATERAL ENFORCEMENT ON ANOTHER STATE'S TERRITORY. – The territorial scope of the criminal procedure law arises, as does substantive criminal law, from the sovereign equality of the States.**[422]** If a State wishes to conduct an investigation on another's territory, it does in theory require permission.[423] This is why States conclude bilateral or multilateral conventions on mutual legal assistance, to obtain evidence located on another State's territory. Any unilateral exercise of authority in another country's territory outside the framework of these conventions is, theoretically, contrary to international law.[424] International law on legal assistance does not prevent States from exchanging information voluntarily. A merely informal request is not, therefore, contrary to international law.

---

420 Permanent Court of International Justice, 7 September 1927, *SS Lotus* (France/Turkey), *PCIJ Collection of Judgements* 1927, Series A, no. 10, 19. C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 9 and 22 et seq.; C. VAN DEN WYNGAERT, *Strafrecht, Strafprocesrecht en Internationaal Strafrecht in hoofdlijnen*, Antwerp, Maklu, 2006, 1215. This is our own underlining.

421 See P.L. BELLIA, 'Chasing Bits across Borders', *The University of Chicago Legal Forum* 2001, 35-101; C. CONINGS and J.J. OERLEMANS, 'Van een netwerk zoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht* 2013, 23 et seq.

422 A. CASSESE, *International Criminal Law*, New York, Oxford University Press, 2008,336.

423 J. WOUTERS, *Internationaal recht in kort bestek*, Antwerp, Intersentia, 2006, 115; T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 231; F. THOMAS, *Internationale rechtshulp in strafzaken* in *Algemene praktische rechtsverzameling*, Antwerp, Kluwer Rechtswetenschappen, 1998, 1 and 55.

424 Unless on the grounds of a permissive rule derived from international practice. Permanent Court of International Justice, 7 September 1927, *SS Lotus* (France/Turkey), *PCIJ Collection of Judgements* 1927, Series A, no. 10, 19. Note that this ban does not generally apply and is not absolutely observed. See T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 231-251.

Neither is fulfilment of that foreign request by a private person, for example.[425] But once the request is no longer informal, but an order, that State is exercising direct authority in another State and this violates the principles of international law.

NON-PHYSICAL BREACHES OF SOVEREIGNTY. - To what extent do criminal investigative measures constitute a breach of another State's sovereignty? In our opinion, these acts include not only coercive measures implemented *physically* in a foreign country, such as interrogation after deprivation of liberty, a house search or a seizure of property, but any action by the detectives or investigators which results in subjecting someone or something in a foreign country to state powers. With modern means of communication, investigators have the ability to investigate data abroad without physically leaving the territory of the State in which it is located. An investigation physically carried out on the territory of one State can, however, have extraterritorial consequences. The question is whether such investigations violate another State's sovereignty and thus requires permission or mutual legal assistance.

CURRENT OBJECT-ORIENTATED APPROACH – In parallel with the gathering of physical evidence, we could say that the gathering of virtual evidence takes place in the country were the data are stored.**[426]** In this view a search at a distance, for virtual data stored abroad requires, in principle, international cooperation. This classical viewpoint is generally accepted in the US**[427]** and in the Council of Europe. While drafting the Cybercrime Convention, many state parties considered that transborder law enforcement access to data or networks, if conducted without the permission of the Member State in question, would breach the

---

425 Even if that would be inconsistent with local law, e.g. a European company discloses information to a US authority in breach of national or EU legislation. But this is not a matter of international law.

426 C. CONINGS notes that: '*It is difficult or impossible to pinpoint the precise location of data. Cloud computing is a major contributing factor to this. The 'cloud' consists of various servers connected to one another through the internet. Data stored in the cloud are continually moved for financial reasons and in order to render optimum use of the storage capacity. Therefore, locating data at a given moment appears to be practically impossible. Moreover, files in a cloud can be split up into small parts, which can be stored at different locations.'* This is one of the reasons why she suggest to move to a subject-orientated approach when determining procedural competence in criminal law. (C. CONINGS, *Locating criminal investigative measures in a virtual environment. Where do searches take place in cyberspace*. B-CCENTRE Legal Research Report 2015, 56.)

427 J. DASKAL, 'The UN-Territoriality of data' , *Yale L. J.* 2015, vol. 125, (326) 371; see also *infra Microsoft* case (United States Court of Appeals, Second Circuit, IN RE: a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation Microsoft Corporation, Appellant, v. United States of America, Appellee, No. 14-2985, 14 July 2016.).

sovereignty of that country and the principles of international law. This is true in particular of data stored on the territory of another State. In this case, all that remains is the traditional path of mutual legal assistance as foreseen in article 31 Cybercrime Convention.[428] Intrusions of this kind are best regulated by international agreements.[429]

Article 20 of the EU Convention on mutual legal assistance in criminal matters[430] and article 32 of the Convention on Cybercrime are examples of international agreements of this kind of non-physical intrusions. They illustrate the broader investigation potential thanks to the use of new communication technologies.[431]

Problems of jurisdiction in criminal investigations had already come up when transborder telephone calls were tapped. For instance, when a Belgian receives calls from abroad, these calls can be subject to a Belgian tapping procedure without the Belgian investigators having to leave the territory and without them having to rely on foreign jurisdiction. These telephone calls are, however, multiterritorial because the audio signals move through both foreign and Belgian telecommunication networks and a Belgian tapping order can apply to foreign subjects. These cases often involve nothing more than a trace that 'moves' to another State without Belgian investigators entering the territory of that State. The breach of the other State's sovereignty is less serious than when the police deliberately cross the border to gather evidence on their own initiative.[432]

The EU Convention on mutual legal assistance in criminal matters contains a specific Regulation on this. Under Article 20, the authorities of one Member State can tap a

---

428 See P.L. BELLIA, 'Chasing Bits across Borders', *The University of Chicago Legal Forum* 2001. See, however, J.L. GOLDSMITH, 'The Internet and the Legitimacy of Remote Cross-Border Searches', *The University of Chicago Legal Forum*, Forthcoming. Available via SSRN: http://ssrn.com/abstract=285732 or http://dx.doi.org/10.2139/ssrn.285732 (posted on 13 October 2001).

429 See also Recommendation R(95)13 concerning problems of criminal procedural law connected with information technology of the Committee of Ministers (of the Council of Europe).

430 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Pb. L.* 12 July 2000, C 197/01. Member States shall take the necessary measures to comply with this Directive by 22 May 2017 (article 36).

431 P. DE HERT, 'Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty is at Stake?' in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 81.

432 B. DE SMET, 'Registratie en lokalisatie van telecommunicatie' in *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak*, 28.

telecommunication address that is used on the territory of another Member State provided that they 1) do not require any technical assistance from that Member State in order to do so and 2) inform the Member State in question either before the tap order, if it is known that the targeted person is on the Member State's territory or, in other cases, immediately after they are aware that the person is located on the territory of the notified Member State. The same rules can be found in article 31 of the European Investigation Order (EIO).[433]

Article 32 of the Convention on Cybercrime regulates the situation in which investigators are able to gain remote access to a foreign network and the data stored therein. The question of whether this was possible unilaterally led to serious discussion during the preliminary negotiations. It was thought by some that the physical location of the computer systems and the data stored there would determine which State had (exclusive) sovereignty. Others were of the opinion that these systems were part of global cyberspace and were therefore freely accessible, not only by citizens, but also by the police and judicial authorities.[434]

Eventually, the Member States reached an agreement on just two issues. These kinds of transborder investigations are possible only when 1) the computer data are open to the public or 2) the investigators have obtained the lawful and voluntary consent of the person who has the lawful authority to disclose the information held in that computer system (see Article 32 (a) and (b) of the Convention on Cybercrime). The Council of Europe is currently looking at whether Article 32 of the Convention on Cybercrime has been superseded and must be altered out of practical necessity.[435] But, for the time being, no other transborder access to computer data is permitted under international law. Article 39 of the same convention does not, however, preclude Member States from recognising each other broader powers in other conventions. It also states specifically that it has no effect on a party's other rights, restrictions, obligations or responsibilities (Article 39, §3). The parties to the convention explicitly adopted this 'saving clause' because they did not want to exclude broader options for transborder investigative work in the future or between

---

433 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ 2014 L 130/1.

434 H.W.K. KASPERSEN, 'Jurisdiction in the Cybercrime Convention' in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 20.

435 CYBERCRIME CONVENTION COMMITTEE (T-CY), 'Transborder access and jurisdiction: what are the options?', Report of the Transborder Group adopted by the T-CY on 6 December 2012, www.coe.int/TCY.

willing States.[436] Whatever the case, these other transborder network searches first require consensus between the States involved.[437]

Moreover, it is unclear if ISP's can serve as a 'lawful authority' within article 32 (b) Cybercrime Convention.[438] The CYBERCRIME CONVENTION COMMITTEE states: '*Service providers are unlikely to be able to consent validly and voluntarily to disclosure their users' data under Article 32. Normally, service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent. Of course, law enforcement agencies may be able to procure data transnationally by other methods, such as mutual legal assistance or procedures for emergency situations.*'[439]

This gives rise to the question if cooperation orders from a law enforcement authority to a service provider based in a foreign country might also be a non-physical, transborder exercise of authority. The Cyber Crime Convention seems to imply that this is the case. However, according to the Belgian Court of Cassation and the Belgian law of 25 December 2016, if the ISP is virtually present on Belgian territory[440], this is not an extraterritorial exercise of jurisdiction.[441] They choose to ignore the criticism that although Belgium might have jurisdiction to prescribe and adjudicate in the case of virtual presence of Yahoo, it still lacks the jurisdiction to enforce. Whereas under international law Belgium might lawfully request Yahoo to cooperate, but it cannot secure payment of the criminal fine applicable under article 46bis Belgian Criminal Procedure Code, since under international law it is forbidden to exercise jurisdiction outside its own territory (see *supra* Lotus case).

---

436 Explanatory Report to the Cybercrime Convention, §293.

437 The EU has been discussing this matter and the Commission has announced that it will come with proposals in June 2017. (Council of the European Union, Council conclusions on improving criminal justice in cyberspace, 9 June 2016; Commission services, Cover note of 2 december 2016, 'Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace', no. 15072/16.)

438 A. M. Osula, 'Transborder access and territorial sovereignty', *Computer Law & Security Review* 2015, (719) 728.

439 CYBERCRIME CONVENTION COMMITTEE (T-CY*), T-CY Guidance Note # 3 Transborder access to data (Article 32)*, Adopted by the 12th Plenary of the T-CY (2-3 December 2014), www.coe.int/TCY , 7.

440 In the Belgian Yahoo! Case this was concluded from the use of the domain name 'wwww.yahoo.be, the use of the local language, showing publicity based on the location of the users of his services and his reachability in Belgium for these users by installing a complaint box and a FAQ desk. (Belgian Court of Cassation 1 December 2015, *Yahoo!*, P.13.2082N/1, www.juridat.be, §9.)

441 Belgian Court of Cassation 1 December 2015, Yahoo!, P.13.2082N/1, www.juridat.be, §9.

Apparently, the intention is to use this unilateral approach to push for a change in international law, preferably through multilateral legal instruments.

LOSS OF OBJECT-LOCATION. - C. CONINGS notes that one of the weak points of an object-orientated approach is that it is not always possible to locate the data. She states: '*It is difficult or impossible to pinpoint the precise location of data. Cloud computing is a major contributing factor to this. The 'cloud' consists of various servers connected to one another through the internet. Data stored in the cloud are continually moved for financial reasons and in order to render optimum use of the storage capacity. Therefore, locating data at a given moment appears to be practically impossible. Moreover, files in a cloud can be split up into small parts, which can be stored at different locations.*'[442] This is one of the reasons why she suggests to move to a subject-orientated approach when determining procedural competence in criminal law.[443] The loss of location is also marked as a problem in the *Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace.* This report points out that '*criminals have the access and ability to make use of sophisticated techniques that allow hiding the location of infrastructure for the storage or processing of electronic evidence.*'[444]

---

[442] C. CONINGS, 'Locating criminal investigative measures in a virtual environment', 2014; Discussion paper on tackling cybercrime, Informal Meeting of the Justice and Home Affairs Ministers, Amsterdam 25-26 January 2016, (43) 56. With reference to: J.J. SCHWERHA, Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from 'Cloud Computing Providers', Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2012/presentations, 9; B.J. KOOPS, R. LEENES, P. DE HERT, S. OLISLAEGERS, Misdaad en opsporing in de wolken, knelpunten en kansen van cloud computing voor de Nederlandse opsporing in WODC, Tilburg, Universiteit van Tilburg, 2012, 12; J. SPOENLE, Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?, Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf.

[443] The fact that Criminals can easily abuse this system by storing their data in countries that are known to be difficult in providing international cooperation or by storing illegal content on servers located in countries where such content is not prohibited is also one of the reasons to opt for a subject-orientated approach.

[444] Commission services, Cover note of 2 december 2016, 'Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace', no. 15072/16, 14.

4.2 Cross-border unilateral cooperation orders allowed?

COMPULSORY MEASURE? – A duty to cooperate arises only after an explicit request or order. It is a reactive form of cooperation (*cf. supra*). This investigative measure was introduced as an alternative to other, more intrusive measures, such as the search and seizure.[445] Now that much of the 'necessary information' for criminal investigations is no longer stored with the authorities themselves, obligations of this kind to disclose information to the authorities are quite common. They arise in various contexts. The measure is less intrusive than a search, for example, but it is still a form of coercion which does not derive directly from the law (active obligation) but from a judicial order (reactive obligation).[446] This will especially be the case when the refusal to cooperate is punishable with a criminal sanction. The threat of a penalty gives the request an undeniably compulsory character. In the various cases in which the ECtHR has had to test these duties to disclose information against the non-incrimination principle, it has stressed that measures of this type have a compulsory nature. For example, in the *Weh* case, the Court ruled that '*without a sufficiently concrete link with these criminal proceedings the use of compulsory powers (i.e.* the imposition of a fine*) to obtain information does not raise an issue with regard to the applicant's right to remain silent and the privilege against self-incrimination*'.[447] In *O'Halloran* and *Francis*, the Court reiterated: '*The Court accepts that the compulsion was of a direct nature, as was the compulsion in other cases in which fines were threatened or imposed for failure to provide information*.'[448]
The request for information is not, therefore, an informal request, but the competent authority does exercise coercive powers on the person addressed.

LOCATION OF COERCION. – The next question to be answered is where the coercive power is exercised. Does the public prosecutor for example in the *Yahoo* case exercised this compulsory power *in Belgium* or *abroad*? In directing his order to the American company based in the US, was the prosecutor actually conducting an investigative act on American

---

445 See Explanatory Report to the Cybercrime Convention, §170.

446 This also comes up in §11 of the Explanatory Report to the Convention on Cybercrime: '(…) iv. the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. (…) requiring service providers to comply with special obligations (…)'.

447 ECHR, 8 April 2004, *Weh/Austria*, consideration 56.

448 ECHR, 29 June 2007, *O'Halloran and Francis/United Kingdom*, consideration 57.

territory? The prosecutor did not believe so. He argued that the American company simply needs to fulfil the Belgian legal duty to cooperate *in Belgium*. He considers the duty cooperate as an active obligation, deriving directly from the law. Once a company falls within the territorial and personal operating sphere of the omission punishable under Article 46*bis* Belgian CPC, it is required to bring the information to Belgium when so requested by the prosecutor. The law, in other words, orders the company to bring the data to Belgium.[449] This view was confirmed by the Belgian Court of Cassation and the Belgian Legislator.[450]

In our opinion, the latter could indeed be correct, *provided that* the Belgian prosecutor's request had indeed 'activated' a duty to cooperate on the part of Yahoo. But the Belgian judges have put the cart (punishment for non-cooperative behaviour) before the horse (a duty to cooperate that is binding on the person in question). Substantive criminal law jurisdiction, i.e. the international law that allows Belgian judicial authorities to claim jurisdiction over behaviour that goes beyond their borders, does not entail full criminal procedure jurisdiction, without any complications. The Belgian omission offence requires a prior, compulsory obligation to 'bring' the information, i.e. an order to activate the obligation. We are of the opinion that a Belgian prosecutor can only obtain this coercion of a *US subject present in the US* with the cooperation or permission of the American government (jurisdiction to enforce).

If the identification information resides with a service provider based *abroad*, the law enforcement authority must, in our view, abide by international law. The competent authority could, of course, send a request, regardless of where the service provider is located. This location does, however, determine the way in which the prosecutor can *enforce* cooperation. The law enforcement authority has no procedural criminal jurisdiction over this foreign company and so cannot issue a direct order or, in this case, enforce the denial of cooperation.

The argument of an '*obligation to bring information to the forum*' does apply, as we see it, when a Belgian service provider administers the data *remotely*, with a third party or abroad, for example. In the latter case, in our opinion, that service provider could not argue

---

449 Corr. Dendermonde 2 maart 2009, *T.Strafr.* 2009, afl. 2, 117-120.

450 Court of Cassation of Belgium 1 December 2015, P.13.2082.N., *Yahoo! Inc.,* www.juridat.be; Article 5 Wet van 25 December 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *B.S.* 17 January 2017.

on the basis of legal assistance that these data are not accessible through it because they are located abroad. Therefore, the location of the data is not decisive under the duty of cooperation. We are of the opinion that this follows from Article 18 of the Cybercrime Convention, which concerns existing ('historical') data in the possession and under the control of the service provider. [451]

As similar enforcement problem arose in the French Yahoo! Case (for the facts of the case, see *supra* III.3.3.4). Yahoo! successfully sought a declaration in the US that the orders made in France were not enforceable under US law.[452] If Yahoo! is only virtual present in a country, and thus does not have any assets in that country, cross-territorial enforcement without the cooperation of the state of incorporation is rendered impossible. Even if a State is allowed to take decisions with a possible extraterritorial effect such as prosecute offences committed in another State, it generally lacks the jurisdiction to enforce it on the territory of the other State.[453]

The view that there is no exercise of extraterritorial jurisdiction when a cooperation order is made to a company that is virtual or physically present on the requesting state's territory, regardless of where the data are stored is not generally accepted as follows from the *Microsoft* case.

MICROSOFT CASE. - In the Microsoft case the traditional view that the search takes place where the data are stored was confirmed by the United States Court of Appeals for the Second Circuit. Microsoft, a company incorporated in the US, refused the US Department of Justice access to a customer's e-mails relevant to a drug trafficking investigation, stored on a Microsoft server in Ireland. Microsoft refused to do so because it would be '*an unlawful*

---

451 See the Explanatory Report to the Cybercrime Convention, §173. Some see this as a breach of the sovereignty of the State in which the data are stored, as is demonstrated by the US case Microsoft v. Ireland. See CYBERCRIME CONVENTION COMMITTEE (T-CY), 'Transborder access and jurisdiction: what are the options?', Report of the Transborder Group adopted by the T-CY on 6 December 2012, 10, www.coe.int/TCY.

452 United States District Court, N.D. California, San Jose Division, *Yahoo! Inc. v. La Ligue contre le racism et l'antisemitsme*, 169 F. Supp. 2d at 1194; D. IRELAND-PIPERA, 'The Future Extraterritorial Criminal Jurisdiction: Does the Long Arm of the Law Undermine the Rule of Law?' *Melb. J. Int'l L.* 2012, (122) 136.

453 A. OSULA, 'Transborder access and territorial sovereignty', *Computer Law & Security Review* 2015, (719) 723.

extraterritorial application of the Stored Communications Act (SCA)[454] *and would work an unlawful intrusion on the privacy of Microsoft's Customer*'.[455] The government on the other hand was of the opinion that there was no extraterritorial enforcement of jurisdiction, as long as the requested data were subject to the recipient's custody or control.[456] The question is where the relevant state action takes place when the government compels the production of e-mails from an Internet Service Provider: at the place where data is accessed or the place where it is stored?[457] The District Court ruled that the proposed execution of the warrant was not extraterritorial because '*a SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. [I]t places obligations only on the service provider to act within the United States*.'[458] However, the United States Court of Appeals, Second Circuit reversed this decision and agreed with Microsoft. It ruled that the enforcement of the warrant was an extraterritorial enforcement of jurisdiction since the data were stored outside the U.S. and therefore the conduct that falls within the focus of the SCA would occur outside the US, regardless of the customer's location and regardless of the Microsoft's home in the US.[459] To get access to emails stored outside its borders, the U.S. government must turn to a mutual legal assistance treaty and make a request to the foreign government that happens to have jurisdiction turn it over.[460]

---

454 The SCA permits the government to require ISPs to produce the contents of certain priority stored communications only pursuant to a warrant issued by a court of competent jurisdiction.

455 United States Court of Appeals, Second Circuit, IN RE: a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation Microsoft Corporation, Appellant, v. United States of America, Appellee, No. 14-2985, 14 July 2016.

456 United States Court of Appeals, Second Circuit, IN RE: a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation Microsoft Corporation, Appellant, v. United States of America, Appellee, No. 14-2985, 14 July 2016.

457 J. DASKAL, 'The UN-Territoriality of Data', Yale L.J. 2015, (326) 326.

458 United States District Court for the Southern District of New York, re Warrant, 15 F. Supp. 3d at 475–76.

459 United States Court of Appeals, Second Circuit, IN RE: a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation Microsoft Corporation, Appellant, v. United States of America, Appellee, No. 14-2985, 14 July 2016. The 2nd Circuit disagree with the magistrate judge that all of the relevant conduct occurred in the United States. See In re Warrant, 15 F. Supp. 3d at 475–76.

460 J. DASKAL, 'Congress Needs to Fix Our Outdated Email Privacy Law', *Slate* 26 January 2017, http://www.slate.com/articles/technology/future_tense/2017/01/the_confusing_court_case_over_microsoft_data_on_servers_in_ireland.html.

However, this ruling is very controversially, and the case can still be appealed to and ultimately reversed by the Supreme Court.[461] Furthermore, the presumption against extraterritoriality could easily be rebutted by congress, if it were to introduce an explicit clause in the law.

OTHER RELATED ISSUES. – The procedural rules of the game do not suddenly change because a failure to fulfil the duty to cooperate is punishable with a fine, on the basis of broad rules of substantive jurisdiction (as is the case under Belgian law).[462] That would circumvent the rules of international legal assistance. Obtaining this foreign evidence [463] is still a matter of international cooperation.[464]

When assessing these jurisdictional issues, we must also bear in mind that if a State allows its own people to conduct far-reaching, transborder, unilateral investigative work, then it must also, in view of the reciprocity principle, allow other States to do the same. While we might be able to live with this from our EU partners, it would be more difficult to accept that Chinese investigators were able to search the servers of EU companies with a territorial link to China, or that a EU service provider would be forced to disclose its information to the American government without the EU Member State being able to exercise any form of control. The company also risks getting into trouble due to non-fulfilment of the European data protection laws.[465]

---

461 *Ibid.*

462 See also C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 23: 'Likewise, a State cannot resort to legal implementation measures such as penalties, fines, seizures, investigations, or demands for information to give extraterritorial effect to its rules.'

463 'Foreign' because it is held by a legal subject based abroad, not 'foreign' because the data are abroad.

464 See, among others, G. HOSEIN, 'International co-operation as a promise and a threat' in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 29 et seq.

465 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31 (see also Regulation No 2016/679 of the European Parliament and 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 95/46EC (General Data Protection Regulation), OJ 2016 L 119, 1.); Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L 350, 60 (See also Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

DISTRUST US DATA PROTECTION. - The distrust with regard to the data protection in the US was shown in the *Schrems* case[466] of the CJEU. The Data Protection Directive provides that the transfer of personal data to a third country may, in principle, take place only if that third country ensures an adequate level of protection of the data (article 25).[467] The European Commission therefore had taken a decision[468] that recognized the adequate level of protection for the transfer of data from the EU to the US if organisations declared its will to obey the data protection principles as envisaged under the Safe Harbour Agreement. Nonetheless, in the *Schrems* case[469] the CJEU declared this decision of the Commission invalid because it failed to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of articles 7, 8 and 47 of the EU Charter.[470] The Court held that the system of self-certification of a company could only constitute a reliable measure of adequacy if US Companies violating the Safe Harbour principles were identified and punished. There was no such mechanism put in place. Moreover, the rules could be overridden by national security requirements set out in US law, state interference was not limited to what is strictly necessary and US authorities were allowed to store all personal data on a general basis.[471] Furthermore there was no possibility for an individual to pursue

---

penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119, 89.)

466 Judgement of 6 October 2016, *Schrems,* C-362/14, EU:C:2015:650.

467 See also article 45 GDPR.

468 European Commission, Commission decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 520, 7.

469 Following facts underlied the case: Mr. Schrems an Austrian facebook subscriber challenged Facebook's transfer of his personal data to the US under the Safe Harbour Agreement. Facebook subscribers residing in the EU sign a contract with Facebook Ireland, a subsidiary of the parent company Facebook Inc. established in the US. Mr schrems made a complaint to the Irish Data Protection Commissioner. He contended in his complaint that the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. Mr Schrems referred in this regard to the revelations made by Edward Snowden concerning the activities of the United States intelligence services, in particular those of the National Security Agency ('the NSA'). (*Schrems,* §28)

470 Judgement of 6 October 2016, *Schrems,* C-362/14, EU:C:2015:650, §86-90.

471 M. S. VIDOVIC, 'Schrems v Data Protection Commissioner(Case C-362/14): empowering national data protection authorities', *Croatian Y.B. Eur. L. & Pol'y* 2015,(259) 267-268.

legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data.[472]

From the invalidity it follows that national supervisory authorities can examine the claim of a person in the EU concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to the US. If they are of the opinion that, pursuant to the Data Protection Directive, a company in the US does not provide an adequate level of protection, the transfer of the data to that company can be suspended. Consequently, US companies were no longer allowed to transfer private data from the EU to the US solely on the basis that they are members of the Safe Harbour Scheme. The judgement had an impact on the cross-border economy between the US and the EU. It was very unclear if and under which conditions companies were allowed under EU law to transfer data to the US. Moreover the impact of the judgement on other transfer tools for personal data was put into question as well, especially in relation to cross-border transfers of personal data to the US. For example the Police Directive,[473] containing harmonised rules for law enforcement cooperation, also made the transfer of data to third states conditional to an adequate level of protection. Therefore a new framework for the transfer of personal data between the U.S. and the EU became a priority. On the 12th of July 2016 the Commission launched the EU-U.S. Privacy Shield.[474] In its press release[475] the Commission stated that: '*This new framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers*'. It also added that the new arrangement lives up to the requirements of the European Court of Justice in the *Schrems* case. Unless the Court of Justice would come to the conclusion that this new arrangement also violates fundamental rights, companies can safely transfer personal data to the States again. This new framework prevents that companies in case of a request for personal data by US authorities should either violate the EU data protection

---

472 Judgement of 6 October 2016, *Schrems,* C-362/14, EU:C:2015:650, §95.

473 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L 350, 60

474 EUROPEAN COMMISSION, Commission implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

475 EUROPEAN COMMISSION, Press release, 'European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows', Brussels 12 July 2016,

rules or otherwise risk penalties in the US for not complying with the request.[476] However, there are already two cases pending before the CJEU asking to annul the EU-U.S. Privacy Shield on the basis of articles 7 and 8 of the EU Charter.[477]

SUBPOENAS AND INDIRECT EXERCISE OF JURISDICTION. - This problem of issuing direct orders to foreign legal subjects actually dates from before the internet era. The practice is reminiscent of the American 'discovery orders'.[478] They obliged US citizens, who fall within US jurisdiction, usually under the threat of a penalty (subpoena), to bring documents from abroad to the US.[479] The US sees this as an *indirect* territorial exercise of its jurisdiction because it does not itself conduct investigations in the foreign territory. Because the documents are brought to the US, the 'discovery' is made on American territory. Therefore it shifts the border when it orders discoveries on foreign territory. However, the practice runs into systematic resistance from other States, particularly in Europe. Europe views the execution of this type of unilateral request without the permission of the other State as an intervention in the territorial sovereignty of that State. A typical example is the controversy surrounding the 'Belgian' corporation SWIFT, which was intended to give the American authorities access to financial data.[480]

Therefore, America may not object too strongly to these direct orders. A recent Council of Europe report shows that the same US Government uses such a practice in relation to cloud service providers falling under their jurisdiction. This is the case when the company or one of its subsidiaries is based in the US, but also when a company '*conducts continuous and*

---

476 M. S. VIDOVIC, 'Schrems v Data Protection Commissioner(Case C-362/14): empowering national data protection authorities', *Croatian Y.B. Eur. L. & Pol'y* 2015,(259) 273.

477 Action brought on 16 September 2016, *Digital Rights Ireland v. Commision,* Case T-670/16; Action brought on 25 October 2016, *La Quadrature du Net and Others v commission*, Case T-738/16.

478 See more on this in C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 79-83.

479 See, for example, *United States/Bank of Nova Scotia*, discussed by G. HOSEIN, 'International co-operation as a promise and a threat' in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 37 and C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 82.

480 Which eventually led to the agreement of 28 June 2010 between the European Union and the United States of America concerning the processing and disclosure of data in relation to the financial messages from the European Union to the United States as part of the terrorist finance tracking programme (TFTP agreement), *Official Journal of the European Union - Legislation* 195, 27 July 2010.

systematic business in the United States'.[481] Because the US uses the practice itself, it might have no objection to unilateral orders against US private companies coming from the EU. Then again, the practice does not tally with the traditional uncooperative European attitude to American orders for information. If Europe were to change track, it would be forced, in view of the reciprocity principle, to stop being uncooperative with these unilateral American orders, and this is something that the Americans would only applaud.[482] RYNGAERT rightly concludes: '*Europeans may indeed reason that arguments of reciprocity counsel against unilateral assertions of jurisdiction in the field of the law of evidence. Although such assertions may confer short-term litigation benefits, such benefits may be outweighed by the burdens of future unilateral assertions of jurisdiction of other States*.'[483]

We should not lose sight of the fact that investigators might also run the risks of being prosecuted in other countries. Unilateral, transborder tapping orders and network searches could be described in other States as unlawful eavesdropping and hacking.[484] As KASPERSEN rightly notes: '*Under public international law, there is no rule that law enforcement officers of one State can lawfully execute their duties as imposed by national law, nor can they invoke legal competences or coercive measures in that State as provided by their national law*.'[485]

---

481 CYBERCRIME CONVENTION COMMITTEE (T-CY), 'Transborder access and jurisdiction: what are the options?', Report of the Transborder Group adopted by the T-CY on 6 December 2012, 48, www.coe.int/TCY.

482 However, in the light of the *Microsoft* case this can be questioned. Although the government argued that '*similar to a subpoena, an SCA warrant requires the recipient to deliver records, physical objects, and other materials to the government no matter where those documents are located, so long as they are subject to the recipient's custody or control*', the Second Circuit decided that Congress intended the SCA warrant procedure to function like a traditional subpoena and that Microsoft could not be obliged to transfer data that were stored outside the territory of the US. (United States Court of Appeals, Second Circuit, IN RE: a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation Microsoft Corporation, Appellant, v. United States of America, Appellee, No. 14-2985, 14 July 2016.)

483 CYBERCRIME CONVENTION COMMITTEE (T-CY), 'Transborder access and jurisdiction: what are the options?', Report of the Transborder Group adopted by the T-CY on 6 December 2012, 83, www.coe.int/TCY.

484 See, for example, the American *Gorshkov and Ivanov* case in which FBI agents lured two Russian suspects to the US. The FBI gained access via the internet to Russian servers using the passwords they had obtained from the Russian suspects. Russia then accused the FBI agents of hacking. See, among others, N. SEITZ, 'Transborder Search: A New Perspective in Law Enforcement?', *International Journal of Communications Law & Policy* 2004, issue 9, 1-18.

485 H.W.K. KASPERSEN, 'Jurisdiction in the Cybercrime Convention' in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 19. See also P.L. BELLIA, 'Chasing Bits across Borders', *The University of Chicago Legal Forum* 2001, 35-101.

CONCLUSION. - When a law enforcement authority directly orders legal subject based abroad, for instance by threatening with fines for non-fulfilment of a *unilateral* request for foreign evidence, it is exercising its power across its borders. In other words, this is a unilateral request with an extraterritorial effect. It cannot be claimed that this is a purely territorial and domestic affair simply because the law enforcement authority has not physically left his own territory. Such order is a coercive measure and comes down to an extraterritorial exercise of enforcement jurisdiction. Without permission from the foreign government, an action of this kind is, in our opinion, contrary to international law. Multilateral treaties facilitating access to data without the burdensome MLAT-procedures should be a priority for policy makers. The European Council and Commission seem to acknowledge that.[486]

486 Council of the European Union, Council conclusions on improving criminal justice in cyberspace, 9 June 2016; Commission services, Cover note of 2 december 2016, 'Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace', no. 15072/16.

5 The road ahead

5.1 Need for international cooperation

CRIMINAL PROCEDURAL MEASURES. – Based on the case law of the ECtHR, legislators have a positive duty *actively* to provide for an *effective* response to the risks to secure identity.[487] Such an effective and comprehensive response implies:

- Reporting mechanisms to victims in order to tackle the underreporting of the offence;[488]
- Ensuring the identification of perpetrators by implementing an IT infrastructure designed to protect all fundamental human rights and freedoms at stake, for example keeping logs and transaction records and constructing reliable identification and authentication while at the same time securing the storage of these logs and personal data, controlling the access to it and executing effective audits.
- Block access to compromising illegal content in order to avoid further damage while at the same time ensuring the respect of the other fundamental rights at stake;

INTERNATIONAL COOPERATION '2.0'. – All these principles are only effective to the extent they can be enforced. In an international context, individual Member States cannot act on the basis of unilateral measures. Efficient solutions must of necessity be international in scope.[489] An effective enforcement of ISP cooperation requires an effective, flexible system of international cooperation.

In a digitised society, evidence need not necessarily be on one territory, but it can be on foreign servers or held by foreign third parties. International law however draws the line between the different sovereign legal orders and, when compared with the extraterritoriality of substantive criminal law, it seems very strict in procedural criminal law matters. This gap is normally bridged by international legal assistance.[490] The path of

---

487 ECtHR 2 December 2008, no. 2872/02, *K.U. v. Finland*; T. PÖYSTI,'Judgement in the case of K.U. v. Finland', *Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 45.

488 See Diagram 'personal data breach notification duties' in annex.

489 T. PÖYSTI,'Judgement in the case of K.U. v. Finland', *Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 43.

490 P.L. BELLIA, 'Chasing Bits across Borders', *The University of Chicago Legal Forum* 2001, 44.

legal assistance however is too cumbersome and slow. A study of the practice reveals that the American authorities have often returned requests for legal assistance in the identification of users of electronic communication services without processing them.[491] Although the US is conventionally obliged to assist states like Belgium[492], this traditional legal assistance contains no mechanism by which to penalise the US or force it to act if assistance is not forthcoming or is too late. It is just not worth the effort for the average criminal case. Diplomatic pressure is the only possible solution, but we fear that the individual EU Member State will not really have much impact on the American authorities at that point.

It goes without saying then that increasing internationalisation and digitisation will increase pressure for flexible and efficient international cooperation.[493] For the time being, compromises are being sought, such as the aforementioned Article 20 of the EU Convention on mutual legal assistance in criminal matters and Article 32 of the Convention on Cybercrime.[494] These two articles make legal assistance slightly more flexible, but they constitute an insufficient attempt to render the cooperation practical and efficient. For example, we see that Article 32 of the Convention on Cybercrime is much stricter on transborder network searches than its counterpart provision, in relation to the transborder tap, in the EU's Convention on mutual legal assistance. This is because the EU States tend to go for intra-EU transborder cooperation.

But even the provision of Article 20 of the EU Convention applies only when there is no need for active cooperation from foreign intermediaries. This shows that the Parties to the Convention considered it a step too far to allow States unilaterally to coerce foreign IT-intermediaries to cooperate, which Belgium undeniably tried to do in the *Yahoo* case.

---

491 Unless it involves terrorism, international drug or arms trading, or there is a proven American interest in the request (e.g. linked to a current American case file or concerning an American citizen).

492 See also G. HOSEIN, 'International co-operation as a promise and a threat' in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 34-35.

493 See also M.A. SUSSMAN, 'The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium', *Duke Journal of Comparative & International Law* 1999, issue 9, 468 et seq.

494 H.W.K. KASPERSEN, 'Jurisdiction in the Cybercrime Convention' in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 20.

Other compromises in the Convention on Cybercrime are, for the time being, the expedited preservation measure (Article 29), the expedited disclosure measure (Article 30) and the setup of permanent points of contact (Article 35). These measures should relieve the problems relating to the speed and transience of electronic communication to a certain extent and prevent States from acting on their own initiative. On the basis of Article 29, a State can request that another State impose an expedited preservation of stored computer data. The requesting State must then, subsequently, send a legal assistance request in order to obtain these data.[495] There is one important exception to this. Article 30 stipulates that if, when implementing a request made under Article 29, the requested State discovers that a service provider in another State was involved in transmission of the electronic communication, the requested State must provide the requesting State with the necessary 'traffic data' as soon as possible[496] so that this service provider and the path through which communication was transmitted can be identified.[497] The combination of these two articles therefore appears to solve (at least on a theoretical level) the prosecutor's problem in the Yahoo case and enables, more generally, a faster acquisition of the data held by service providers based abroad. The procedure sounds great in theory, but in practice appears to run into the same problems experienced with traditional mutual legal assistance. Implementation of the measure may yet be too slow to allow the capturing of the needed data[498], and the willingness of some States to cooperate with requests of this type is often limited.

---

495 Explanatory Report to the Cybercrime Convention, §283 and 284: '*At the same time, a requested party is permitted to use other procedures for ensuring the rapid preservation of data, including the expedited issuance and execution of a production order or search warrant for the data. The key requirement is to have an extremely rapid process in place to prevent the data from being irretrievably lost. (…) Finally the requesting Party must undertake to subsequently submit a request for mutual assistance so that it may obtain the production of the data*.'

496 Article 1, (d) of the Cybercrime Convention states that this includes data relating to the origin of the communication (IP addresses, numbers, etc.). See Explanatory Report to the Cybercrime Convention, §30.

497 See Explanatory Report to the Cybercrime Convention, §290: '*In doing so, the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself.*' For example, if the data lead back to the requesting State itself, it can obtain the necessary information through internal measures. If they lead back to a third State, the requesting State can again make an expedited preservation or expedited disclosure request, this time to the third State.

498 H.W.K. KASPERSEN, 'Cybercrime and Internet jurisdiction (Draft discussion paper prepared in the framework of the Project on Cybercrime of the Council of Europe)', 28, www.coe.int/cybercrime.

It is to be hoped that Article 35 will satisfy the high expectations of those who look for better cooperation. This article stipulates that States establish a point of contact that is to be continually available and guarantees immediate assistance, among other things for the location of suspects.[499] The setup of a 24/7 network of this type is, in our opinion, one of the most important achievements of the Convention on Cybercrime.

THE 'POWER OF DISPOSAL'. – As we have said, the Council of Europe is currently considering amendments to Article 32 of the Convention on Cybercrime. The report by the Cybercrime Convention Committee gives several interesting suggestions to 'update' transborder access to data.[500] Of the policy options under consideration, we think that the suggestion to replace the location of the data as a condition for procedural criminal jurisdiction with '*the power of disposal'* is a deserving one. It binds the data to the person or people who have the right to access and 'administer' them (edit, delete, deny others the right of access and use, etc.). For these data to fall under the jurisdiction of the investigating State, this 'administrator' would have to physically be in the territory of the investigating State or be a national subject.[501]

This new criterion offers prospects for transborder network searches and production orders issued to national based service providers who choose to store their data abroad but not for coercive orders issued to foreign based service providers who nonetheless provides services on other states' territories. When the latter is the case, it is still not the place where the data are stored that should be relevant, but the place where the person charged with the duty to cooperate (the 'administrator') is located.

SUBJECT-ORIENTATED APPROACH.**[502]** - C. CONINGS suggests that '*the habitual residence of the subject regarding his virtual past'* should become the main criteria for localizing

---

499 States can themselves choose who to appoint. For Belgium, it is the Federal Computer Crime Unit (FCCU). See Explanatory Report to the Cybercrime Convention, §298.

500 The scope of the present contribution does not allow us to go into this in any more detail. See the report of the CYBERCRIME CONVENTION COMMITTEE (T-CY), 'Transborder access and jurisdiction: what are the options?', Report of the Transborder Group adopted by the T-CY on 6 December 2012, www.coe.int/TCY.

501 J. SPOENLE, 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?', Discussion Paper of 31 August 2010, www.coe.int/cybercrime.

502 This part is entirely based on the findings of C. CONINGS in her PhD 'A coherent criminal procedure regime for search in the physical and digital world'. (C. CONINGS, *Een coherent regime voor strafrechtelijke zoekingen in de fysieke en digitale wereld,* onuitg. Doctoraatsthesis Rechten KU Leuven, 2016, 554-581; The part of the PhD on territorial search competences was also published in C C. CONINGS, *Locating criminal investigative measures in a virtual environment. Where do searches*

investigation measures and, hence, indicating which state has jurisdiction. She justifies her choice by stating that*: 'Focusing on habitual residence ensures that the most important competencies of control of both the virtual and the physical life are vested in one and the same state. Individuals can no longer escape from the local legal system by storing data abroad, whilst enjoying full access and use of that data'*. Furthermore she adds: '*The autonomous investigative competence relates to the investigated subject's legal virtual environment. Making this competence dependent on the will of the state of storage or the service provider's state should, in our opinion, be excluded. As is the case with investigations in real time, the focus should be on the subject. Moreover, in a subject-oriented approach, legal subjects are given the protection they expect. Regardless of where the data are to be found, the human rights of a person are protected on the basis of the law of the country where he has habitual residence and, in general, where he habitually consults his data. In this way, every virtual action falls within the scope of a coherent and, for the person concerned, familiar system of protection of privacy and other human rights. This also ensures that there is legal certainty*.'[503] In addition to this, CONINGS is of the opinion that territorial competence should also be attributed to the state where the service provider is located[504] and to the

take place in cyberspace. B-CCENTRE Legal Research Report 2015, 43-72 and in B. J. KOOPS, C. CONINGS and F. VERBRUGGEN, *Zoeken in computers naar Nederlands en Belgisch recht,* Oisterwijk, Wolf Legal Publisher, 2016, 136-187.)

503 C. CONINGS, *Locating criminal investigative measures in a virtual environment. Where do searches take place in cyberspace*. B-CCENTRE Legal Research Report 2015, 62. However, she notes that: ' *illegal access (e.g. hacking) cannot extend the territorial competence of the respective state due to the fact that this causes illegal entrance in another person's virtual environment. An authority which wants to access this must do so by means of international cooperation with the authority having the sovereign competence over the hacked system.'* (*Ibid,* 65).

504 CONINGS is of the opinion that denying the service provider's state the competence to autonomously investigate the data linked to that service could infringe its sovereignty. *'If the data sought are accessible to the service provider and are linked to its service, which is consulted by the subject, the service provider's state displays a well-founded link with the data sought and its claim to sovereignty cannot merely be brushed aside.*'. However, the server state only has competence if: '*service was consulted by the investigated subject and that the sought data are related to the subject's use of the service*.' If this is the case the legal subject could expect that his data can be investigated under the service provider's state's law. (*Ibid,* 63.)

state where the subject his data are stored but only if the data subject stored his data himself in the foreign territory.[505, 506]

Although there have been a few Court decisions (see *supra*) about the obligations of service providers, enforceability remains a challenge unless the service provider is established in the relevant country.[507]

Unfortunately, the T-CY report pays little attention to the problems posed by *Yahoo*-like cases (transborder request or ISP cooperation as an alternative of transborder access). It merely states that when data are in the hands of a service provider in a foreign country, the investigating authorities must generally take the path of legal assistance. However, they will experience technical and legal difficulties in this regard. Some States do allow service providers to respond directly to requests from foreign law enforcement authorities. Under some circumstances, information might be voluntarily exchanged.[508]
The time has come to find an international generally agreed solution to this problem. Just as the US first negotiated an agreement with Belgium and then with the EU over more rapid American access to financial data of the type held by companies like SWIFT in its fight against terrorism, it would seem recommendable that the US oblige its internet companies to comply directly with requests for user information coming from judicial authorities from EU-states or the EU as such. The EU could set a first example of such direct ISP cooperation. It would be desirable, of course, to have a standardised electronic communication system for this, which could guarantee speed, authenticity and confidentiality. In more sensitive cases, such as when the request could endanger relevant interests (e.g. medical confidentiality, professional secrecy, business confidentiality or

---

505 If the service provider (e.g. Google) has control over which country has competence over the legal subordinate's data by storing them in a place that is financially more viable, it becomes difficult to the subject to know which state has competence over his data and legal certainty in a virtual environment is therefore eroded. (*Ibid,* 63-64).

506 For an extensive justification of these choices see C. CONINGS, *Locating criminal investigative measures in a virtual environment. Where do searches take place in cyberspace*. B-CCENTRE Legal Research Report 2015, 43-72.

507 Commission services, Cover note of 2 december 2016, 'Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace', no. 15072/16, 12-13.

508 CYBERCRIME CONVENTION COMMITTEE (T-CY), 'Transborder access and jurisdiction: what are the options?', Report of the Transborder Group adopted by the T-CY on 6 December 2012, 31 and 44, www.coe.int/TCY.

other national interests), the Member State could then intervene. With the right guarantees, it might be possible, for example, to oblige service providers to respond to requests to disclose identification data to foreign law enforcement authorities, provided that the requested data has substantial links with the territory of the investigating State, such as the suspect or victim is a national subject of that State.[509] In those cases, the data are identification information relating to electronic communications. Those communications were generated for the most part in the investigating State, and use was made of internet access and/or service providers based in that State. The role of the foreign service provider was merely secondary, the communication had its centre of gravity in the investigating State.

5.2 Semi-private take down procedures

SOURCE OF INSPIRATION. - Since the CJEU ruled in G*oogle Spain* that there is a right to be forgotten, we could say that there is *a fortiori* a right to rectify when false information concerning one's identity circulates on the internet.**510**

This is also in line with the positive obligations of states under article 8 ECHR. Because ID fraud takes place in an online context without territorial borders, international cooperation is very much needed if we want to offer victims an efficient redress. In the context of child sexual abuse online, INHOPE an international association of hotlines was set up to take down images of child abuse more efficiently. Another project worth assessing is the European Internet Referral Unit (EU IRU) launched by Europol to take terrorist propaganda offline. Both projects could be a source of inspiration when looking for remedies to take offline a compromised ID.

---

509 We refer in this matter to the current doctoral dissertation by LEWIS CHEZAN BANDE at KU Leuven entitled 'Cross-Border Access to Computer Data by Foreign Law Enforcement and the Position of Private Actors: Reducing the Role of Requested-State Authorities in International Cooperation against Cybercrime?'.

510 This right can also be derived from the Data Protection Directive and the GDPR that state that the data controller has the task of ensuring that personal data are processed 'fairly and lawfully' , that they are 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes' , that they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/ or further processed', that they are 'accurate and, where necessary, kept up to date', and finally, that they are 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed'. (see *Supra* III.3.3.2)

INHOPE. – The International Association of Internet Hotlines (INHOPE) brings together 51 hotlines in 45 countries[511] and offers the public a way of anonymously reporting Internet material including child sexual abuse material they suspect to be illegal.[512] The project is co-funded by the European Union.[513]

HOW DOES IT WORK?[514] – Civilians can make a complaint of internet material of sexual child abuse to a reporting portal of one of the hotlines. A highly trained analyst will manually assess the report. If the analyst qualifies the received content under the national law as an image of sexual abuse, he or she will trace and determine the geographical location of the server on which the content is hosted at the time of assessment. If the content is hosted in the country where the complaint is made, the hotline will contact the police as well as the host provider in question to ensure a quick removal of the url. The specific method of cooperation with the police, the judiciary and the ISP's is different in every country. When the content is being hosted in an INHOPE country a report will be send to the INHOPE reporting system which then forwards the report to the relevant INHOPE hotline. An analyst of this hotline will reassess the report and if found illegal under its national law the analyst will start the Notice and Takedown procedure in consultation with the police and the judicial authorities.[515] Most of the time URLs of sexual abuse are then removed from the internet within 72 hours.[516]

A similar structure could be set up to report ID fraud online and to take down false information concerning one's identity circulating on the internet. Moreover it would also bypass the problem of territoriality since under the INHOPE system it are always the hotlines in the country of the ISP that hosts the illegal content, that start the notice and take

---

511 A list of the participating countries and hotlines is published at the INHOPE website (www.inhope.org)

512 www.inhope.org

513 https://ec.europa.eu/justice/grants/results/daphne-toolkit/en/content/child-pornography-internet-cooperation-between-hotlines-inhope-forum

514 Internet Watch Foundation, How we assess and remove content, https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content ; Child Focus, Hoe werkt het concreet in het buitenland?, http://childfocus.be/nl/seksuele-uitbuiting/kinderpornografie/burgerlijk-meldpunt/hoe-werkt-het-concreet-in-het-buitenland.

515 The cooperation with law enforcement is necessary to secure the possibility of an criminal investigation and in this regard to protect evidence.

516 When the content is not hosted in an INHOPE country, hotlines can report it to the national police who then can forward it to INTERPOL, who then can pass it on to the hosting country's police.

down procedure. ISPs therefore do not receive direct legal orders from foreign authorities which might conflict with their obligations under national law.

The EKSISTENZ project's technology could also help hotlines with their assessment. If the victim himself makes a complain, it could easily use the EKSISTENZ-tool to prove its identity.

EU IRU. – On 1 July 2015 Europol launched the European Union Internet Referral Unit (EU IRU) to combat terrorist propaganda and related violent extremist activities on the internet. The unit is aimed at reducing the level and impact of terrorist and violent extremist propaganda on the internet.[517] One of the core tasks of the EU IRU is flagging terrorist and violent extremist content online and cooperating with online service providers with the aim of removing this content.[518] Furthermore, EU IRU supports Member States with operational and strategic analysis.[519] The EU IRU works closely with relevant social media and other private companies and national expert contact points (due to be established in all Member States).

A referral activity (meaning the reporting of terrorist and extremist online content to the concerned online service provider) does not constitute an enforceable act. The decision to remove the referred terrorist and extremist online content is left to the concerned service provider under their own responsibility and accountability (in reference to their Terms and Conditions). Nevertheless, in 91.4% of the EU IRU referrals, the material has been swiftly removed.[520] Referrals to the online platforms are made both following requests received from Member States and as a result of Open Source Scanning by the EU IRU team.[521]

---

[517] EUROPOL, 'Europol's Internet Referral Unit to combat terrorist and violent extremist propaganda', *Press Release* 1 July 2015, https://www.europol.europa.eu/newsroom/news/europol%E2%80%99s-internet-referral-unit-tocombat-terrorist-and-violent-extremist-propaganda

[518] EUROPOL, 'EU Internet Referral Unit Year One Report Highlights', 22 July 2016, https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights, 4.

[519] EUROPOL, 'Europol's Internet Referral Unit to combat terrorist and violent extremist propaganda', *Press Release* 1 July 2015, https://www.europol.europa.eu/newsroom/news/europol%E2%80%99s-internet-referral-unit-tocombat-terrorist-and-violent-extremist-propaganda

[520] For the first working year of EU IRU.

[521] EUROPOL, 'EU Internet Referral Unit Year One Report Highlights', 22 July 2016, https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights, 4.

Following the Year One Report a 24/7 referral service an real time access to referral information for Member States' investigators will be set up by July 2017. Furthermore it states that: '*the development of a strong referral capability, which will be informed by tactics derived from operational analysis and outreach to the private sector, will bridge the gap between prevention and attribution'.*

CONCLUSION. – Both the INHOPE project as the EU IRU can be seen as examples of successful cooperation with the private sector. This type of cooperation on a voluntary basis seems to be very effective to take down online content. Both projects work with experts in the field when assessing possible illegal content. For example the EU IRU comprises of a team of experts with multiple and diverse knowledge and skills, ranging from experts in religiously inspired terrorism, translators, ICT developers and law enforcement experts in counter terrorism.[522] This is important, the more expertise these central bodies have the more credibility they have towards the private sector.

Setting up a similar cooperation network when dealing with ID theft seems the way to go. It should be seen as a first step to take compromised personal data offline. Only when ISPs refuse to voluntarily take down referred information, coercion mechanisms should come into play.

---

522 EUROPOL, 'EU Internet Referral Unit Year One Report Highlights', 22 July 2016, https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights, 4.

Conclusion

A key goal of the EKSISTENZ-project is *to prevent* identity theft, but it has to be assumed that absolute watertight prevention will never be possible. Criminal law only plays a role in the aftermath, as the legal basis for authorities to start criminal investigations. It acknowledges the suffering of the primary victims and gives them a stepping stone in the legal process of recovery of their compromised identity.

Under the case law of the ECtHR, member state lawmakers have a positive duty to actively provide for an *effective* response to the risks to secure identity.[523] Such an effective and comprehensive response requires notification, identification and blocking mechanisms. All of these measures face particular stumbling blocks. They all require cooperation of service providers: voluntarily if possible, compulsory if necessary.

With regard to notification duties, under EU law a patchwork of notification duties currently exists, all different in scope. This creates legal uncertainty for service providers as to when, to whom and what they should notify. Furthermore, notification duties entail operational costs and possible reputational damage for service providers. In practice, compliance with notification duties seems very low. From May 2018 onwards, a notification duty for '*all data controllers',* will apply under the GDPR. This duty is backed up with high administrative fines to ensure compliance. These measures can only be applauded. The sooner data breaches are notified, the sooner they can be remedied. In this way ID fraud can be redressed swiftly in order to limit or even avoid harm to a victim's identity.

As for identification duties, article 18 Cybercrime Convention obliges the Member States to adopt legislative and other measures to order a service provider to submit subscriber information, including the subscriber's identity. This obligation is in line with the case law of the ECtHR. In *K.U. v Finland*[524] the Court stated that States should implement a legal procedure where a judicial authority may order, under certain conditions, the release of

---

[523] ECtHR 14 February 2012, nr. 7094/06, *Romet/The Netherlands*; ECtHR 2 December 2008, no. 2872/02, *K.U. v. Finland;* T. PÖYSTI,'Judgement in the case of K.U. v. Finland*', Digital Evidence and Electronic Signature Law Review* 2009, Vol. 6, 45.

[524] ECtHR 2 December 2008, no. 2872/02, *K.U. v. Finland.*

information required to identify an internet user, provided that there are reasonable grounds to believe that he or she has committed a criminal offence. In *I v Finland*, the ECtHR decided that the respect for private life under article 8 ECHR, holds a positive obligation for the state to provide for effective information security measures to exclude the possibility of unauthorised access to data.[525] One might argue that this also demands technical measures which provide for the reliable identification and authentication of users of electronic communication services. Here the Project's technology might provide a handy tool in the fight against ID Fraud and other misuse of personal data. However, the need for identification is hindered and in some cases even made impossible by the CJEU's principled case law on data retention based on article 7 and 8 of the EU Charter. [526] One can only hope that the CJEU will come up with a more nuanced position in the near future.

Due to concerns of private censorship and the importance of freedom of speech, the blocking of information by service providers is perhaps the most controversial measure. First and foremost it should be stressed that in the EU, a general monitoring obligation cannot be imposed on ISPs. However, the neutrality of service providers ends as soon as they actually take note of illegal activities committed with use of their services, for instance through notification by a user, a victim or a law enforcement agency. To continue to benefit from the exemption of liability, the internet host provider has to act expeditiously to remove the information concerned or to disable access to it.[527] Moreover, under the Data Protection Directive and the GDPR, data subjects can in certain circumstances request the *rectification, erasure or blocking* of data. This is certainly the case when false information concerning the victim's identity circulates on the internet.

However, some important questions remain. For example how can the ISP be sure that the individual that notifies ID fraud does not act in bad faith and/ or that the notified content is indeed compromised? One of the possibilities would be to create a hotline where complaints of ID-fraud can be made, together with specialized identification centers. This identification center can then assess (in cooperation with law enforcement and the authorities best placed to verify identities and identification instruments) the complaint

---

[525] ECtHR 17 July 2008, no. 20511/03, *I. v. Finland*, paragraph 37.

[526] Judgement of 21 december 2016, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Joined Cases C-203/15 and C-698/15, EU:C:2016:970.

[527] Article, 14 (1) b and recital (46) e-Commerce Directive.

and confirm the authentic ID of the complainant. Again the EKSISTENZ-project tools can prove to be of great value for such assessment centres, since identification through the tools may offer additional safeguards to establish the victim's true identity. If ID fraud is established, the assessment center can send a notice and a take-down request to the service provider. Similar semi-private take down procedures are already set up to take down online child abuse and terrorist propaganda.

All these duties for internet service providers are only effective to the extent they can be enforced. In an international context, individual Member States cannot act on the basis of unilateral measures. An effective enforcement of ISP cooperation requires an effective, flexible system of international cooperation. Both the Council of Europe and the European Union are currently looking for possibilities to 'update' transborder access to data.[528] In the current object-orientated approach, the place where the data are stored determines the procedural competence in criminal law. We suggest to move to a subject-orientated approach. '*The habitual residence of the subject regarding his virtual past*' should become the main criteria for localizing investigation measures and, hence, indicating which state has jurisdiction.[529] Territorial competence should in addition be attributed to the state where the service provider is located and to the state where the subject's data are stored respectively, but only if the data subject itself knowingly decided to store the data on the foreign territory. These new criteria would enhance legal certainty by giving the data subject the protection it can expect. Moreover, criminals could no longer abuse the existing system by storing their data in countries that are known to be difficult in providing international cooperation or by storing illegal content on servers located in countries where such content is not prohibited. Last but not least, international cooperation can be hindered by European Data Protection law. Under the Data Protection Directive as well as under the GDPR personal data can only be transferred from the EU to a third country if an adequate level of protection is ensured by that country.

---

528 CYBERCRIME CONVENTION COMMITTEE (T-CY), 'Transborder access and jurisdiction: what are the options?', Report of the Transborder Group adopted by the T-CY on 6 December 2012, www.coe.int/TCY; Council of the European Union, Council conclusions on improving criminal justice in cyberspace, 9 June 2016; Commission services, Cover note of 2 december 2016, 'Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace', no. 15072/16.

529 C. CONINGS, *Locating criminal investigative measures in a virtual environment. Where do searches take place in cyberspace*. B-CCENTRE Legal Research Report 2015, 43-72.

In the borderless internet environment, criminals can easily escape responsibility or remain out of the reach of law enforcement by operating from countries with less or no regulation. A criminal offence has limited deterrent effect if there is no means to bring the perpetrator to justice. Not so much harmonisation of identity fraud criminalisation, but joint efforts at international and supranational level to implement and enforce specific procedural measures are the key to successfully tackling identity fraud and identity theft.

Annex

Personal data breach notification duties					
	e-Privacy Directive (2002/58) + Regulation 611/2013	**Framework Directive (2002/21)**	**eIDAS Regulation (910/2014)**	**e-Commerce Directive (2000/31)**	**GDPR (2016/679)**
Scope	Provider of publicly available electronic communications services	Undertakings providing public communications networks or publicly available electronic communications services	Trust service providers	Information society services providers	Data controllers
Notification to Supervisory authority/ DPA[530]	Article 4 (3): All personal data breaches ➔ 24 hours after the detection of the personal data breach, where feasible (Article 2 Regulation)	Article 13a (3): "A breach of security or loss of integrity that has had a *significant impact* on the operation of networks or services."	Article 19 (2): "(…) any breach of security or loss of integrity that has a *significant impact* on the trust service provided or on the personal data maintained therein." ➔ Without undue delay but in any event within 24 hours after having become aware of it	Article 15: "Member States may establish obligations for information technology, widely recognised and used by industry, to society service providers promptly to inform the competent obtain data on the use of the information; and public authorities of alleged illegal activities undertaken or information provided by recipients of their service …"	Article 33: Personal data breach is likely to result in *a risk to the rights and freedoms of natural persons.* ➔ Within 72 hours (if not accompanied by reasons for the delay)

530 Data Protection Authority

	e-Privacy Directive (2002/58) + Regulation 611/2013	**Framework Directive (2002/21)**	**eIDAS Regulation (910/2014)**	**e-Commerce Directive (2000/31)**	**GDPR (2016/679)**
Notification to data subject	Article 4(3): "When the personal data breach is likely to *adversely affect* the personal data or privacy of a subscriber or individual, …" ➔ Without undue delay		Article 19(2): "Where the breach of security or loss of integrity is likely to *adversely affect* a natural or legal person to whom the trusted service has been provided, …" ➔ Without undue delay		Article 34: "When the personal data breach is likely to result in a *high risk to the rights and freedoms of natural persons*,…" ➔ Without undue delay
Notification to the public		Article 13a (3): "The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is *in the public interest.*"	Article 19 (2): "The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is *in the public interest*."		