KU Leuven
Faculty of Law and Criminology

SURVEILLANCE RISKS IN IOT APPLIED TO SMART CITIES

Isadora NERONI REZENDE

Dissertation presented within the framewoek of the LAST-JD-RioE MSCA ITN European Joint Doctorate n. 814177, in partial fulfillment of the requirements for the degrees of:

- Doctor of Laws (PhD) at KU Leuven,
- Doctor in Law, Science and Technology (PhD) at Alma Mater Studiorium Università di Bologna (UNIBO),
- Doctor in Law (PhD) at Universitat Autònoma de Barcelona (UAB)

Supervisor:
Prof. Dr. Carles Górriz López (UAB)
Co-supervisors:
Prof. Dr. Anton Vedder (KUL-CiTiP)
Prof. Dr. Michele Caianiello (UNIBO)

March 2023

Alma Mater Studiorum – Università di Bologna
in cotutela con Katholieke Hogeschool Limburg-Associatie KULeuven e
Universitat Autònoma de Barcelona

DOTTORATO DI RICERCA IN

LAW, SCIENCE AND TECHNOLOGY

Ciclo 35

Settore Concorsuale: 12/G2 - DIRITTO PROCESSUALE PENALE

Settore Scientifico Disciplinare: IUS/16 - DIRITTO PROCESSUALE PENALE

SURVEILLANCE RISKS IN IOT APPLIED TO SMART CITIES

Presentata da: Isadora Neroni Rezende

Coordinatore Dottorato

Monica Palmirani

Supervisore

Michele Caianiello

Supervisore

Carlos Górriz López

Co-supervisore

Anton Herman Vedder

Esame finale anno 2023

Abstract

Nowadays, cities deal with unprecedented pollution and overpopulation problems, and Internet of Things (IoT) technologies are supporting them in facing these issues and becoming increasingly smart. IoT sensors embedded in public infrastructure can provide granular data on the urban environment, and help public authorities to make their cities more sustainable and efficient. Nonetheless, this pervasive data collection also raises high surveillance risks, jeopardizing privacy and data protection rights.

Against this backdrop, this thesis addresses how IoT surveillance technologies can be implemented in a legally compliant and ethically acceptable fashion in smart cities. To investigate this question, an interdisciplinary approach is embraced, combining doctrinal legal research (on privacy, data protection, criminal procedure) with insights from philosophy, governance and urban studies.

The fundamental normative argument of this work is that surveillance constitutes a necessary feature of modern information societies. Nonetheless, as the complexity of surveillance phenomena increases, there emerges a need to develop more fine-attuned proportionality assessments to ensure a legitimate implementation of monitoring technologies.

This research tackles this gap from different perspectives, analyzing the EU data protection legislation, as well as the United States and European case law on privacy expectations and surveillance. Specifically, a coherent multi-factor test assessing privacy expectations in public IoT environments and a surveillance taxonomy are proposed to inform proportionality assessments of surveillance initiatives in smart cities. These insights are also applied to four uses cases: facial recognition technologies, drones, environmental policing, smart nudging. Lastly, the investigation examines competing data governance models in the digital domain and the smart city, reviewing the EU upcoming data governance framework. It is argued that, despite the stated policy goals, the balance of interests may often favor corporate strategies in data sharing, to the detriment of common good uses of data in the urban context.

Table of Contents

Introductory Chapter

1. Background

Smartfying cities. As for anything else these days, being "smart" seems to be the latest trend for cities worldwide. Amidst smart fridges, toothbrushes and other beauty gadgets, smart cities are one of the most prominent instances of how the Internet of Things (IoT) is developing and will further change our daily lives. More than ever before, cities are dealing with ever-growing pollution and overpopulation issues, exacerbated by intensifying urbanisation processes. Under the promise of greater interconnectedness of urban services and infrastructure, smart technologies are supporting local authorities in making their cities more efficient and sustainable. Achieving efficient energy use, lower pollution rates and higher public safety are only some of the challenges that are being addressed by digital solutions worldwide.

Technology applications in smart cities are indeed varied. Distributed sensors interacting with centralised control systems are providing real time data on urban environments and offer actionable insights for optimising resources. In New York, sensors and cameras have been installed at more than 10,000 road intersections, providing vital information for the improvement of safety and traffic congestion[1]. At the same time, Sidewalk Lab's platform Replica draws on private data sources (e.g., GPS data, de-identified mobile location and credit transaction data, and real estate transaction data) and public data to recreate travel behaviour patterns and suggest alternative transit options[2]. In Barcelona, IoT sensors monitor rain and humidity levels to control park irrigation and water levels in public fountains[3]. Rio de Janeiro hosts the *Centro de Operações da Prefeitura do Rio*, the world's largest control room system which displays over 560 cameras and integrates data for more than 20 city agencies, improving emergency response times by 30%[4]. In Copenhagen, the non-profit *Miljøpunkt Amager* works closely with Google AirView, traffic and community-collected data to assess air pollution impacts and citizens' action in defined areas[5].

From canonical smart cities to retrofitted ones. The scale of smart city projects can also differ greatly across the globe. On the one hand, canonical examples of smart city development include entire urban centres built from scratch, with pervasive and seamless technology applications. Songdo, in South Korea, is an often-cited example. Here, sensors have been installed in streets and buildings to help public authorities monitor environmental and traffic flow conditions in the city. In the United Arab Emirates, Masdar City realises the utopia of the "zero-carbon city", designed to rely exclusively on solar energy and other renewable energy sources.

On the other hand, especially in Western countries, smart city initiatives are gradually integrated in the infrastructure of existing cities. This approach is evident in the European Commission's definition of the smart city, by which "a smart city is a place where *traditional* networks and services are made more efficient with the use of digital and telecommunication technologies for the benefit of its inhabitants and business"[6].

[1] Briodagh (2019).
[2] Wray (2021).
[3] Adler (2016).
[4] Soffel (2013).
[5] Castro P (2021).
[6] European Commission (2018a). [emphasis added]

In some cases, technology deployments are upgraded to neighbourhood level, creating smart districts within existing cities. These are comprehensive projects offering a vision for future technology-equipped, dynamic and carbon neutral cities. Notable examples in this regard are the 22@Barcelona and the recently failed Quayside project in Toronto.

Smart technologies can also be tested at the micro-infrastructure level (e.g., a street, a square), as the notorious Stratumseind project in Eindhoven shows. Notably, this initiative includes a predictive policing system for the early detection of deviant behaviour and situations prone to escalations, leveraging on AI-equipped video cameras (with face blurring and suspicious walking tracking capabilities) and sound sensors, as well as tweet sentiment analysis to look for anomalous data patterns. In addition, an adaptive lighting system smooths and manages "escalated" moods and environments through adaptive lighting scenarios.

Smart cities and the pandemic. In the wake of the Covid-19 pandemic, digital technologies and data assets have played a major role in the fight against the spread of the virus and the enforcement of social distancing measures[7]. Various examples can testify to this. In New York and Washington DC, public authorities relied on Unqork, a no-code software platform, to automate the delivery of food and medicines to vulnerable households and individuals[8]. In Spain, the bottom-up initiative Frena la Curva gathered more than 9000 public services freely available to citizens[9] on a no-code platform. In Florence, a traffic sensor network composed of video-cameras and Bluetooth devices provided daily traffic flow data during the lockdown, allowing public authorities to monitor citizens' compliance with mobility restrictions[10]. In Hong Kong, robots were deployed to disinfect subway trains and stations of the Mass Transit Railway system, which transports millions of passengers per day[11]. As vaccine campaigns advance worldwide, digital technologies are still regarded as key in supporting cities in these challenging times. Different converging factors suggest an exponential growth of smart-city investments in the near future, which are estimated to reach $203 billion globally by 2024[12]. Here, digital transformation appears to be fostered not only by current social distancing measures, but also by the heavy budgetary cuts suffered by municipal authorities, which are increasingly pushed to deliver more with fewer resources. In this regard, among the most popular initiatives to be undertaken by the tech industry, we find the widespread electrification of infrastructure, 5G, digital twins, but also the improvement of citizens' participation and equity.

The value of data in smart cities. If it was not clear before, after the pandemic the value of data in city governance is now uncontested. As long as data about cities has been collected, they have historically been leveraged as evidence bases to define urban policies and monitor their effectiveness. With the digital revolution, and the deployment of "data-hungry" technologies like artificial intelligence (AI), data now powers a great deal of innovation processes and its role in urban development is even more central[13]. Data is now a by-product of a number of daily activities, and its volume is only destined to increase (the quantity of data produced is estimated to grow from 33 zettabytes in 2018 to 175 zettabytes in 2025).

[7] Goldsmith (2021).
[8] Melendez (2020).
[9] Las Naves (2020).
[10] Sharing Cities (2020).
[11] Hui (2020).
[12] Combs (2020).
[13] On artificial intelligence in smart city development, see Pellegrin et al (2021).

Citizens in urban centres are being pushed to volunteer their data or may not even have a choice to opt-out of processing activities in public spaces. Ostensibly, cities are being transformed into machines for intensive data collection, as part of a trend – pushed at the highest political levels – that constantly seeks new ways to exploit data in more intelligent ways[14]. Data is arguably deemed to have the potential to bring huge benefits to society, from improved efficiency in mobility services to greater energy waste reduction.

In this backdrop, the European Union (EU) is also working to build new governance structures to manage quality data pools and maximise their reuse. Specifically, in the *European Strategy for Data*, the Commission has clearly stated that "data generated by the public sector as well as the value created should be available for the *common good* by ensuring, including through preferential access, that these data are used by researchers, other public institutions, SMEs or start-ups"[15]. Among the first data-related initiatives in this sense, the proposal of the Data Governance Act (DGA) and Data Act (DA) foresee the creation of "European data spaces" covering key areas for smart city development, such as energy, mobility and public administration.

Smart surveillance. The strong emphasis on data and technologies in the city does not come, however, without concerns. Privacy and data protection issues are often raised in the smart city discussion[16]. Indeed, cities are literally transformed into machines for intensive data collection where multifold surveillance activities can proliferate. CCTV cameras are probably the most obvious manifestation of urban monitoring activities, which get increasingly invasive with the use of (emotion) facial recognition software. More unobtrusive forms of surveillance can nonetheless be implemented through sensors seamlessly embedded in the urban infrastructure. Smart bins, lampposts or billboards can easily conceal sensors capturing MAC addresses or Wi-fi metering boxes recording mobile phones with an activated Wi-fi functionality in the vicinity. RFID-equipped travel cards offer granular insights into citizens' mobility patterns. Automated number plate recognition (ANPR) technologies detect vehicle locations and may be used for law enforcement purposes.

Overall, the increasing interconnectedness of these technology applications – whose data streams are often integrated in one single platform –considerably amplifies the chilling effects of surveillance in smart cities. Privacy in the public realm is significantly reduced as the scope of surveillance activities expands from enclosed contexts of disadvantage (e.g., prisons, warehouses, shelters) to everyday activities in urban open spaces.

Especially in public spaces, the spread and intensification of surveillance technologies has been comforted by the Western idea that people should not enjoy privacy outside their private dwellings. Despite this normative assumption, still persisting in privacy discourses, in the past people have counted on a certain level of *obscurity* in the public arena. In large urban centres, people could go easily unnoticed as they performed their mundane or most private activities –purchasing coffee in a bar, picking groceries at the market or holding hands with their partner in the park. People were visible, but not necessarily exposed. "Seen by hundreds, noticed by none", as Helen Nissenbaum put it. "Or, if we are noticed, it is by disparate observers, each taking in only discrete bits of information. As such, the information would be sparse and disjointed, limited by the capacities of the single human brain"[17].

---

[14] Christofi (2021), p. 67.

[15] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions. A European Strategy for data, COM (2020) 66, p. 8.

[16] Braun et al (2018); Hiller, Blanke (2017); Woo (2017); van Zoonen (2016); Finch et al (2017); Privacy International (2017); Picon A (2019).

[17] Nissenbaum (2009), p. 117.

With IoT and AI's computational capabilities, this paradigm is now rapidly shifting. Non-threatening data points from dispersed databases are now combined and processed by artificial agents looking for insightful patterns. Our digital trails can be used to granularly reconstruct our mobility patterns and commercial transactions. Even more worryingly, emotion prediction technologies can now expose our innermost feelings only because we dare to venture into the public space.

Framing surveillance normatively. Surveillance is not a new phenomenon, nor inherently problematic; on the contrary, it is naturally embedded in several social activities, and it is pivotal for the functioning of complex societies. As highlighted in sociological and philosophical literature, surveillance can be deployed at the same time for both caring and controlling purposes[18]. Significantly, Michel Foucault observed that the "art of government" required the sovereign to set up a form of "economy" – that is, a way of surveilling and controlling individuals – in the same way the head of a family does with his household and goods[19]. In digitally complex societies, ways of handling individuals and goods are increasingly dependent on data, which is becoming a key asset for any successful governance effort. Data about places, people and social activities are leveraged to get real-time insights into the dynamics, and to steer urban life and achieve a more sustainable management of common resources. Soft biometric technologies also help public authorities and commercial actors to make their services more responsive to citizens' needs, by capturing their emotional reactions in different situations.

Regardless of its benevolent or malicious purposes, surveillance is not neutral either, meaning that its social acceptability highly depends on its contextual implementation. The strong traction for the reuse of data collected in smart cities should therefore be questioned from both the ethical and legal perspective.

Digital technologies are bringing radical changes in the way societal processes are organised. The number of subjects that have access to data both within and without the city has grown exponentially. The objectives of the actors that have access to the data may vary considerably. Crucially, this does not only happen for interplays between the public and private sector, but also for transfers within the public administration itself.

It is evident that all these elements could directly impact on data processing, for instance by creating strong tensions to the principle of purpose limitation, one of the fundamental tenets of EU data protection law. In such a context, grasping the elusive goals and effects of multi-faceted surveillance phenomena becomes increasingly difficult. These dynamics are further exacerbated by the advent of the IoT paradigm – now evolved into the Internet of Everything (IoE)[20] – whereby points for data collection and channels for subsequent processing tend to be ubiquitous.

Against this background, the fundamental principles underlying privacy and data protection are going through a strong crisis. Smart cities are only one example of how current laws are being challenged in this respect. However, understanding how to achieve less impactful surveillance practices in urban contexts may play a significant role in legitimising data uses that can actually be beneficial for city governance.

2. Research questions, objectives and sources

Main research question. In light of the above-mentioned considerations, emerges a need to explore the normative implications of surveillance technologies in the urban space, especially those empowered by

[18] Galič (2019), p. 17.
[19] Foucault (1991), p. 92.
[20] Cisco (2013).

IoT's far-reaching capabilities. The aim is first to unpack the privacy and data protection issues stemming from these systems, combining theoretical and doctrinal research with the analysis of pragmatic instances of technology implementation. From the legal standpoint, the objective is to propose solutions which are coherent with privacy and data protection overarching principles. From an interdisciplinary perspective instead, this research work could be of interest for those engaging in sociological and ethical scholarly disciplines (e.g., surveillance studies, digital ethics) which stand at the intersection with the law.

Against this backdrop, the main research question of this dissertation is: ***How can IoT surveillance technologies be implemented in an ethically acceptable and legally compliant fashion in the context of public places in smart cities?***

The overall research question is *normative*. Legal scholarship is naturally interested in addressing questions of how certain phenomena should be regulated in society. Nonetheless, legal analyses are not always bolstered by a clear understanding of the phenomena subject to regulation. A theoretical understanding of what is to be governed is often lacking[21]. Therefore, to address the main research question properly, descriptive and explanatory sub-questions will also be tackled, in order to outline the phenomena analysed (see the Methodology section for more remarks in this regard).

This dissertation is structured in two main parts. From the very beginning, a contextual approach will be adopted, addressing proposed sub-questions by looking specifically at smart cities. General legal concepts and principles will be explained as they come into play in the analysis (e.g., meaning of the rights to privacy and data protection, purpose limitation principle). In doing this, a conceptual analysis of these legal concepts will be conducted, breaking down their meaning and content into different sub-components.

Nonetheless, the first and the second part will be explored at two distinct levels of abstraction. The first part will take a broader or more theoretical perspective on legal, societal and ethical problems arising in the smart city context. It will include: (1) examining general privacy and data protection issues in smart cities; (2) defining individuals' reasonable expectation of privacy in IoT environments like public spaces in smart cities; (3) scrutinising different theoretical frameworks to analyse surveillance schemes and the proportionality assessments they require in smart cities. The second part will build on general findings of the first part to investigate questions that are more focused in scope. In particular, (4) the use of specific IoT surveillance technologies will be assessed against the delineated normative frameworks; (5) data governance frameworks will be outlined to best exploit the value of data in smart cities, while also mitigating the effects of reckless surveillance.

Legal framework. From a legal perspective, the relevant questions will be addressed by narrowing down the scope of the research to the European sources on the rights to privacy and data protection. Having in mind the funders of this project, it makes sense to take into consideration the sources pertaining specifically to the European human rights framework, comprising relevant provisions of both the European Convention of Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (CFREU). Related case law of the two European courts – the European Court of Human Rights (ECtHR) and the European Court of Justice (CJEU) – will also be analysed to better understand the nature, contents and rationale of the two examined rights. At the level of secondary law, two central data protection instruments will be primarily taken into consideration: The General Data

[21] Pałka (2017), p. 18.

Protection Regulation (GDPR)[22] and the Directive 2016/800/EU (Law Enforcement Directive, LED)[23]. These instruments will be reviewed to the extent to which they could already provide for solutions to privacy and data protection conundrums in smart cities. At the same time, a critical standpoint on this legislation will potentially highlight potential gaps in the existing protection, so as so to identify possible ways forward on the basis of underlying principles.

It is important to point out that a previous doctoral work dealing with the topic of surveillance in smart cities explicitly excluded data protection analysis from its purview[24]. Differently, the data protection perspective will be highlighted here, in order to account also for non-consensual data processing practices in smart cities. In addition, from a privacy standpoint, the issue of "reasonable expectations" will be at the centre of the investigation.

While this work does not fully commit to a comparative approach, case law stemming from the United States' jurisdictions will tangentially be taken as a benchmark, specifically when it comes to decisions pertaining to Fourth Amendment rights. In the North American constitutional framework, this fundamental provision is underlined by significant privacy considerations, which justifies its relevance for the purposes of this dissertation. The importance of taking into account this case law also emerges from a methodological perspective, as will be explained in a dedicated section.

Ethical analysis. Ethical principles such as security or privacy will be taken as relevant normative benchmarks for the analysis of surveillance practices in smart cities. Exploring data governance issues will also require going beyond the strict purview of the legal analysis to embrace broader ethical considerations over the use of digital data. With regard to the smart city, specifically, communitarian outlooks and Lefebvre's idea of the Right to the city will be leveraged to outline alternative (data) governance models for smart cities.

3. Methodology

A conventional approach in legal research is taken, thereby relying mainly on desk-research. However, some methodological caveats should be outlined. The interdisciplinary nature of the topic will be presented, requiring the integration of different backgrounds and reasoning methods. To this end, there is a need to define some ambiguous key terms in the research and provide some working definitions. This will help restricting the scope of the investigation as well.

3.1. Interdisciplinarity

An inherently interdisciplinary research. Starting from the very title of this dissertation, it is noticeable that the term "smart city" can have different meanings according to the angle and academic discipline that comes into play[25]. For instance, Rob Kitchin poignantly represents the (lack of) dialogue between two streams of literature revolving around smart cities, one focusing on the technical representation of the city itself and another purporting sociological critique of the smart city paradigm[26]. Surveillance and

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
[23] 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 penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.
[24] Galič (2019).
[25] Research on smart cities is generally regarded as an interdisciplinary. See Bibri (2018), pp. 40-42.
[26] Kitchin et al (2019a), pp. 3-4.

privacy issues have also been studied from manifold scholarly perspectives, transgressing the boundaries of traditional academic disciplines. The inherently interdisciplinary character of the topic under investigation entails a similar approach being undertaken in this dissertation. Importantly, an interdisciplinary approach differs from merely multidisciplinary ones because it takes insights from diverse disciplines and applies them with synthesis and coherence.

Disciplines taken into consideration. Given the multiplicity and diversity of technology-related issues in smart cities, the scope of this dissertation should be restricted. First and foremost, legal doctrinal approach will be taken, performing an analysis of current positive law, reconstructed through a combination of primary sources (e.g., legislation and court cases) and scholarship work (e.g., journal articles and handbooks)[27].

In this regard, it should be considered that recent developments in law have brought new questions about the true meaning of legal doctrinal scholarship. According to some authors, legal doctrinal scholarship is increasingly "contaminated" by broader approaches to law in general, which makes us distinguish proper doctrinal work that primarily concentrates on the current state of play in positive law, and other legal disciplines. The latter are mainly represented by "*law and*" disciplines, whose broad spectrum is only partially oriented towards the law. Among these, we find "law and economics", "law and technology", "socio-legal studies", "legal philosophy".

In the domain of "law and technology" studies, for instance, Pałka maintains that "the object of inquiry has switched from the law to socio-technological phenomena seen from the perspective of the law"[28]. This way of looking at the legal implications of technology-related phenomena seems to best fit the objectives and topics of this dissertation. Specifically, Pałka formulates a step-by-step methodology: (1) description of facts; (2) conceptualisation of facts from a certain perspective (explanation); (3) evaluation of explained facts, according to a selected normative theory; (4) in the case of a negative assessment, surveying and postulating the desired goals; (5) surveying and postulating the means of achieving these goals[29].

In this dissertation, each of the proposed sub-research questions will firstly be addressed with a factual description of relevant smart city initiatives and an explanation of the related privacy, data protection, surveillance or governance practices. In light of the chosen normative framework (see below), these practices will be evaluated. Where gaps are identified, legal and ethical solutions will be proposed.

Normative framework. Importantly, adopting a legal doctrinal approach entails making the underlying normative framework explicit. In doing so, the position that tends to implicitly conflate normative frameworks with the relevant legal system should be rejected. This approach, however, bears the risk of looking at the law indiscriminately, whereas existing provisions also need to be assessed against additional normative benchmarks. In this regard, it is indeed useful to distinguish between "internal" and "external" normative standards. The former refers to those standards that *are part* of the law – including broader principles that stem from an overall consideration of the legal system – while the latter are to be identified with the theories that provide for such standards. Here, moral and political philosophy might come into play. Privacy as a value and a fundamental right has traditionally been studied in both philosophical and sociological research. Conceptual insights derived from political and moral philosophy, as well as philosophy of information, can broaden the understanding of these rights,

[27] Taekema (2018), p. 1.
[28] Pałka (2017), p. 24
[29] Pałka (2017), p. 118.

and assist in assessing current policy choices of implementation. Both continental and analytical philosophical traditions will thus be integrated as relevant.

Underlying reasoning techniques. In legal scholarship – as well as in other inherently normative disciplines like philosophy – descriptive and explanatory questions are tackled with *interpretative* methods, rather than empirical ones[30]. This means that descriptive and explanatory efforts in legal analysis mainly revolve around reconstructing a coherent picture of the current *status quo* of the law with regard to specific questions.

Such attention to normative sources may however result in a lack of theoretical understanding of the practical phenomena regulated by the law. To avoid this risk, descriptive and explanatory questions will be dealt with not only through strict legal analysis, but also by broadening the horizon to other social science disciplines. Specifically, sources stemming from the domains of surveillance and urban studies will be integrated. These fields will provide for both theoretical insights and a practical and contextual understanding of surveillance phenomena in smart cities. In fact, the contribution of these two streams of scholarship seems promising in this work. On the one hand, surveillance studies is in itself an interdiscipline, which highly reinforces its suitability to being included in the scope of this study[31]. Because of their critical theoretical approach and tendency for "totalising dystopian narratives"[32], surveillance studies have actually had a complicated relationship with the law, which instead bears liberal roots and is more oriented toward achieving pragmatic results.

Nonetheless, legal scholarship has always thrived on interdisciplinary inspection, and surveillance studies can bring interesting insights to the table. For instance, research in surveillance studies is mainly ethnographic, meaning that it acknowledges social processes as being culturally embedded[33]. This specific angle connects surveillance studies to another fundamental discipline in this research. Urban studies and its sub-disciplines (in particular critical urban theory[34]) is indeed one of the bodies of literature where the most extensive analyses on smart cities have been made.

Overall, diverse reasoning techniques will be adopted in this dissertation: (i) descriptive and (ii) explanatory, on the one hand; (iii) evaluative and (iv) normative, on the other. With respect to questions that require normative and evaluative reasoning, a few caveats are necessary. It is well known by now that the law has long struggled to keep up with the challenges raised by digital technologies. The law naturally aims to regulate and downsize the uncertainties of the future, but the world is decreasingly stable in its dynamics. Globalisation and digitisation processes bring different legal systems closer together, and the instances of interaction between these are relentlessly growing, especially in the framework of integration projects like the EU. Hence, interpreters are now dealing with: (i) new issues, (ii) old issues with magnified technological outreach and (iii) foreign – but sometimes similar – legal systems.

Against this backdrop, legal questions require answers that are not inscribed plainly in the law or may not be retrieved by means of a strict method of literal interpretation. New solutions are often built upon more creative heuristic methods, e.g., teleological, analogical or evolutionary, which often aim to extend the means and objectives of existing provisions to previously unregulated – and unforeseen – situations.

---

30 Taekema (2018), p. 2.
31 Cohen (2015a), p. 99.
32 Id.
33 Cohen (2015a), p. 97.
34 For a definition of critical urban theory, see Marcuse (2009), p. 186.

The Translation Problem. This more flexible way of interpreting and applying the law has often thrived in common law systems, which feature non-formalistic cultural stances, particularly prone to axiological reasoning[35]. Indeed, Lawrence Lessing has rightly explained that the digital revolution poses challenges of *translation* for constitutional rights[36]. Touching upon issues of interpretation and legitimacy, the "translation problem" fundamentally forces us to give renewed meaning and application to provisions written in general terms, which could follow the changes in society. This is particularly relevant for data protection and privacy law, which is often blamed for its "lack of clarity and vagueness of the statutory concepts and the open-ended terminology, especially in key terms and definitions"[37]. That is why the law is slowly undergoing a subtle metamorphosis while facing the ever-changing issues posed by digital technologies. It is ever more distant from its previous image of purity and abstractness that prevailed in civil law systems; its application is instead increasingly fact- and context- dependent[38]. This is reflected, for instance, in the rising importance of jurisprudence as a source of law in European civil law countries, which must also interact with supranational frameworks – namely the EU and the ECHR – where the interpretation of provisions by the respective competent Courts has a pivotal role hierarchy of legal sources[39]. This more central role of the judges crucially affects the principle of legality as traditionally conceived in Europe: reasoning *through principles* – rather than strict provisional rules – gains the upper hand and enhances creative opportunities for the interpreter who is often called upon to resolve new legal issues[40].

The Principle of Proportionality. In this background, one principle among others best expresses this material – rather than abstract – legal rationality and will extensively be employed throughout this dissertation: the principle of proportionality[41]. As the European Data Protection Supervisor (EDPS) underlined, the necessity and proportionality principles in data protection law are to be understood as fact-based rather than abstract legal concepts, requiring a contextualised assessment integrating the specific circumstances of a case (or of a specific technology implementation)[42]. This dissertation will fully embrace this reasoning approach, especially in light of the above-mentioned assumption about the need to contextually assess surveillance applications. To this end, practical knowledge of particular smart city programs and initiatives will be fundamental in the analysis.

Potential weaknesses and dangers of an interdisciplinary approach. While an interdisciplinary approach may potentially bring innovative findings and personal enrichment for the researcher, it also brings considerable uncertainties into the work. As a researcher with a primary legal background, I am venturing into new fields of knowledge that feature their own methodology, terminology and assumptions. Dialogue between different disciplines is being increasingly advocated for in academia, but dealing with unfamiliar disciplines makes compromises inevitable and may lead to failures in knowledge and methodological accuracy. It is acknowledged that such an approach may not be fruitful in the short term, being potentially subject to criticism from diverse angles. In the field of legal scholarship, these efforts may be regarded with scepticism – considering that some steps in the work may not be essentially *legal*. The same kind of criticism may come from the experts in the areas that are simply being "visited", where this investigation could be perceived as one by an outsider who lacks

[35] Washington et al (2019).
[36] Id., p. 1.
[37] Koops BJ (2014a), p. 254.
[38] Kostoris (2018), p. 57.
[39] Id., p. 58.
[40] Id., pp. 58-59.
[41] See Chapter IV, §3.1.
[42] EDPS (2017a), p. 8.

proper background knowledge. Exploring other areas of research may also derail this thesis from its original legal vocation. Therefore, constant efforts will be made to keep my investigation legal in its core, leveraging other disciplines only as a means to improve the accuracy and factual orientation of the analysis.

3.2. Working concepts

Defining the key terms of the research. When investigating surveillance technologies, different kinds of social ordering instruments will be explored, from the more tangible (e.g., hard law) to the more subtle ones (e.g., soft law, ethical principles). As outlined above, globalised and digitally informed societies now feature highly distributed networks of actors mutually involved in their respective capacities. Complex communities are run thanks to the cooperation of diverse stakeholders, who not only bring specific expertise and perspectives on the table, but also leverage different instruments in their efforts to shape and steer innovation processes.

Generally, these endeavours may go under the name of *governance*. Governance has been at the centre of intense debates from the 1990s, especially in the wake of the World Wide Web development . The term has also spurred much confusion regarding its exact meaning, sometimes being perceived as a buzzword.

From a legal perspective, its relationship with other patterns of rule, such as (legal) regulation, has often been questioned. In line with the interdisciplinary vocation of this dissertation, however, all kinds of regulatory instruments and efforts will be considered in order to go beyond the strict domain of the law and cross over to the wider domain of governance. This is also coherent with the specificity of the smart city as an arena populated by diverse private and public actors.

Nonetheless, many key terms in the research are not unambiguously understood in literature. Diverging interpretations may be rooted in different scholarly backgrounds and terminological choices. To avoid misinterpretations, the understanding of the relevant concepts (and their relationship with one another) will be clarified below.

3.2.1. Governance

Definition. Governance has been broadly defined by Borrás and Edler as the "ability of a society to develop and implement collective choices"[43]. With the increasing complexity of pluralistic information societies, the term became a popular catchphrase around the mid-1990s[44] and its boundaries have been loosely defined ever since[45]. Nonetheless, three distinctive features seem to emerge in scholarly literature, which often defines governance as being (i) collective, (ii) distributed, and (iii) reflexive.

Collective, Distributed, Reflexive. Governance is collective because it goes beyond regulatory actions of the government and other institutions of the State, engaging a heterogeneous web of societal and economic stakeholders in social ordering processes[46]. Private-sector entities, NGOs and other non-state actors thus cooperate alongside public institutions to address manifold issues in the public realm. As larger networks of stakeholders are involved in decision-making processes, modes of governance have also become more distributed. Its tools have become more diversified. Indeed, governance is not only focused on the hard rules of the State, "but develops also from (social) interactions, cooperation and negotiations between stakeholders at the horizontal level"[47]. Means of rulemaking are no longer

[43] Borrás et al (2020), p. 2.
[44] Marsden (2008), p. 116.
[45] Hofmann et al (2017), p. 1411.
[46] Id., pp. 1409-1410; Madison (2020), p. 33; Bennett et al (2020), p. 448; Micheli et al (2020), p. 2; Pagallo et al (2019), p. 2.
[47] Micheli (2020), p. 2.

centralised in state-based legislation, but are the result of decentralised inputs, comprising non-binding norms (e.g., standards, soft-law instruments)[48]. More pluralistic patterns of rule eventually lead to a procedural shift in regulatory mechanisms[49]. Governance is a process by which diverse actors can interact reflexively to steer and control societal transformations[50]. According to Hofmann, understanding governance as "reflexive coordination" means to capture the way in which stakeholders debate and negotiate shared principles, normative principles, expectations and assumptions underlying their regulatory efforts[51].

3.2.2. Regulation

Definition. As a concept, regulation is stricter in scope with respect to governance, being traditionally identified with State-centric, command-and-control legal regulation. Indeed, hard law is only one of the tools by which society can govern public issues[52]. Although regulation has often been equated with governance[53], we consider here that one key component of regulation is the involvement of public institutions in the ordering process[54].

Self-regulation. This conceptualisation allows us to exclude from its scope those governing actions that take place within market regulatory systems. For instance, this is the case of corporate governance, or standards and practices developed across the industry, when these are agnostically viewed by the law[55]. Counterintuitively, these instances of self-regulation may not be labelled as regulation after all[56]. Indeed, according to Marsden, self-regulation consists of "self-regulatory arrangements whose modus operandi consist of non-binding norms of action, process, and behaviour, for whom sanctions of the formal regulatory type play no part"[57].

Co-regulation. By contrast, once there is a formal institutional involvement, a case of co-regulation is at stake. Indeed, co-regulation refers to numerous regimes where there is a complex interaction of general legislation and a self-regulatory entity[58]. Self-regulatory efforts of the private sector are framed within legislative and governmental regulation, which provides for their legitimacy. Co-regulation is thus a concrete output of governance where the law meets further regulatory systems of the market and society. Of course, the interactions between these regulatory forces may occur with higher or lower intensity. Institutional intervention may be only indirect, like when the State only imposes sanctions for failures to adopt standards or codes of practice (i.e., enforced self-regulation)[59]. The legislator may also set out a framework of general principles to be technically implemented by private sector actors, which are best positioned to give practical application to these norms. This is the case of principle-based regulation, of which the GDPR is one prominent example[60].

---

[48] Id.; Marsden (2008), p. 116.
[49] Bevir (2010), p. 1; Bevir (2009), p. 3; Trubek et al (2007), p. 549; Zachariadis (2019), p. 107.
[50] Borrás et al (2020), p. 2; Hofmann (2017), pp. 1412 ff.
[51] Hofmann (2017), p. 1414.
[52] Pagallo et al (2019), p. 3. On the distinction between legal regulation and legislation, see Kosti et al (2019).
[53] This is the position of Julia Black, as referenced in Hofmann (2017), p. 1411; Finck (2019), p. 145.
[54] Australian Government (2014), p. 3.
[55] Marsden (2011), p. 28.
[56] Bennett et al (2020), p. 454.
[57] Marsden (2008), p. 118.
[58] Marsden (2011), p. 1; Pagallo (2019), p. 2; Australian Government (2014), p. 28 (referring also to "quasi-regulation").
[59] Terminological choices may vary. See, e.g., Black (2012), p. 1045 (referring to "meta-regulation").
[60] Bennett et al (2020), p. 453.

3.2.3. Smart cities

The Lack of a Common Definition. If there is one consensus in the multidisciplinary literature on smart cities, it is that one universally agreed and solid definition of the "smart city" does not exist[61]. The term is cited everywhere and often labelled as fuzzy and evasive. Experts, scholars and policy makers with different backgrounds compete to provide their own interpretation, often complicating the challenge of unambiguously determining the meaning of the expression. While some have given up on this quest by simply providing a set of parameters to measure out cities' smartness[62], others have engaged on theoretical discussions on this seemingly empty notion, sometimes reaching converging findings.

Historical Perspective on the Smart City. To overcome this uncertainty, an effort of synthesis will be made with the aim of proposing a composite working concept of the smart city within this dissertation. Before that, a brief historical reconstruction of the smart city paradigm will be nonetheless provided, highlighting the meanings and goals behind the notion of "smart" and how they have evolved over time. The present digression will serve as background and provide justification for the building blocks of the chosen smart city definition.

From the historic perspective, Vanolo argues that the adjective "smart" merges a two-fold perspective on urban planning. On the one hand, the smart component stands for the exploitation of information and communication technologies (ICTs) in the daily administration of the city[63]. Historically, digital technologies were first used to manage urban services and infrastructures in the 1950s, concurrently with the shift from electromagnetic to computational systems[64]. Cybernetic thinking in the 1960s further spurred on this process, promoting a picture of the city as "system of systems" that could be computationally managed[65]. Gradually, the idea of the "intelligent city" concurred to legitimising the extensive use of technologies in the design and management of urban space.

On the other hand, the "smart" label has also been used to express environmental concerns, coupled with urban growth and development goals. From this perspective, Vanolo retraces the origins of the smart city concept in the Smart Growth movement developed within the framework of New Urbanism, originated in the United Stated in the 1980s. New Urbanism sought indeed to improve urban planning by embracing a communitarian approach and circumscribing urban sprawl (and the environmental impact of cities)[66].

These two approaches to urban development were timely integrated into corporate strategies starting from the end of the 1990s. Large multinational companies increasingly relied on narratives advertising the use of digital technologies in urban infrastructure and services. Cisco, one of the major players in the circulation of the smart city discourse, tried to sponsor a private-public partnership (PPP) in Milan back in the late 1990s[67].

Unsurprisingly, this technocratic, corporate "quest" for the urban environment was quickly spotted by scholars of critical urban studies, as highlighted in Hollands' influential critique of the smart city label[68]. It is interesting to note how environmental and communitarian concerns, which had originally animated the smart city discourse, were increasingly absorbed by a more technocratic, entrepreneurial

---

61 Hollands (2008); Albino et al (2015); Cocchia (2014), pp. 14, 17.

62 Researchers indicate that smart cities can be identified simply by referring to six key features: smart economy, smart mobility, smart environment, smart people, smart living, smart governance. See Giffinger et al (2007), pp. 11-12.

63 Vanolo (2014), p. 888; Vanolo (2016), p. 27.

64 Kitchin R (2017a), p. 19; Kitchin et al (2019b), p. 2.

65 Kitchin (2017a), pp. 19-20; Finger (2017), p. 6.

66 Vanolo (2014), p. 887.

67 Id.

68 Hollands (2008), p. 308; Purcell M (2002).

drive in urban planning. The semantic flexibility of the word "smart" clearly played a role in this process. Morozov and Bria underscore the "elusive" nature of the term, which is often used by corporations as innovation-friendly synonym for "flexible", "wise", "self-adjusting", "intelligent", "autonomous", "resourceful", "lean", and even "ecologically friendly"[69]. This semantic ambiguity was indeed seized by corporations that indiscriminately depicted smart technologies as a means to achieve urban resilience and sustainability. Indeed, while the term "smart city" itself was first coined in 1994, it was finally popularised in corporate literature by IBM in 2008[70]. On the other hand, in the same period, the "smart" label was increasingly integrated into the narratives of supranational institutions, which began to stress the importance of initiatives aimed at fostering the sustainability of cities[71].

In this way, the smart city became mainly an economic project for companies in search of new markets, especially in the wake of the global financial crash of the 2010s[72]. Austerity was indeed one factor that pushed city administrations to outsource smart technologies that could help to make the most of recently cut budgets and increase competitiveness[73].

In this context, cities became growingly dependent on competitive funding from supra-national bodies in order to acquire technologies and implement services[74]. The EU also played a major role in the dissemination of a neoliberal model of urban growth through funding allocation mechanisms. In particular, Kitchin and Cardullo explored how the European Innovation Partnership for Smart Cities and Communities (EIP-SCC) promotes neoliberal practices through their Marketplace platform, where city officials and different stakeholders can meet and cooperate to develop smart city projects. According to the authors, the Marketplace seeks to boost entrepreneurial urbanism and technological solutionism by scaling up urban solutions that have proved to be successful across the consortium[75]. However, this replication process takes place without any consideration for the peculiarities of specific urban environments, nor the actual needs of citizens, who are often seen as mere consumers or recipients of smart city initiatives[76].

Recurrent Elements in Conceptualising Smart Cities. It is clear that the debate revolving around the smart city idea has spurred on different constitutive elements of this concept, involving both descriptive and normative dimensions. Considerations of a purely descriptive nature, pointing out the delineative features of a (quasi-)smart city, have gone along with the discussion on how a true smart city *should* be.

At the bottom line, the core idea behind smart cities is the integration of ICT components in the city infrastructure – whether existing or built from scratch – to achieve greater efficiency and sustainability in urban resource management, as well as better quality of life for citizens[77]. This process of digitisation of urban environments was accompanied by a change in the governance setting, which has increasingly foreseen the intervention of private sector parties, primary depositaries of the technical expertise required for smart technology implementations[78]. Indeed, it is no surprise that a research report

[69] Morozov et al (2018), pp. 2-4; Cocchia (2014), p. 14; Thorne et al (2014), p. 91.
[70] Cocchia (2014), pp. 26-28.
[71] Id., pp. 14, 29.
[72] See also Kitchin et al (2019b), p. 2.
[73] Cardullo et al (2019b), p. 816.
[74] Id.; Morozov (2018), pp. 9-10.
[75] Cardullo et al (2019b), p. 815; Vanolo (2014), pp. 888-889.
[76] Id.
[77] This can be traced back to the first understanding by IBM of the smart city concept, which implied "the use of information and communication technologies to sense, analye and integrate the key information of core systems in running cities". See Harrison et al (2010); Woo (2017), p. 955; Mohanty et al (2016), p. 60; Kummitha et al (2017), pp. 43, 45; Cocchia (2014), pp. 32-33, 35.
[78] See Kummitha (2017), p. 46.

requested by the European Parliament mentions PPPs as a highly important success component of smart city projects[79]. While the involvement of private companies – often through different PPP configurations – is an important and often present element in smart city development, it is not a necessary one. Some cities indeed, with Barcelona as leading example, have recently been trying to downsize the involvement of private parties in technology-oriented initiatives, as a way to regain their "digital sovereignty"[80].

When the discussion moves onto the normative level, debates have mainly counterposed corporate, technocratic visions of the smart city and more communitarian and citizen-centric views, often coming from the field of critical urban studies[81]. From the outset, it should be noted that normative ideals have always had a bearing on the smart city concept. At first, in the 1990s this label was leveraged to refer to the more *human* and *political* aspects of urban life, highlighting the objectives of sustainability and quality of life for city dwellers. On the contrary, the more dated concept of "digital city" had a more neutral connotation, simply focusing on the integration of ICTs in the urban infrastructure[82]. When the smart city brand was finally popularised in the late 2000s, it was meant for a broader scope, incorporating the "hard" components of a digital city with more social and environment-oriented purposes of a smart city.

Despite this evolution, two polarised strands in approaching the smart city concept still exist today. Popular in the engineering and corporate domains, technocratic – or restrictive – approaches to smart cities heavily focus on the role of ICTs alone in making the urban space a more sustainable, thriving and accessible place for citizens[83]. The proponents of such perspective place significant emphasis on technical solutions, which are regarded as neutral, politically benign and often implemented with top-down approaches. The city is mainly seen only through the lens of systems theory, and thus conceptualised as an entirely knowable, rational and manageable machine[84]. Privatisation and corporatisation of the urban sphere are an inevitable by-product of this approach. Indeed, the task of practically implementing technical solutions is frequently outsourced to the private sector, and more specifically to a limited number of multinationals leaders on the market (e.g., IBM, Cisco)[85].

Starting from Holland's seminal work, critical perspectives on the technocratic conception of the smart city have denounced the growing privatisation of the urban space connected to the implementation of ICT projects[86]. Smart cities are uncovered to be primarily a business model, rather than a means to pursue broader societal goals like social justice, inclusion and sustainable development[87]. In these communitarian and citizen-centric perspectives, proponents of the technocratic approach are heavily criticised for different reasons. Firstly, they seem to forget the role of human agency, political, social and cultural variables affecting the implementation of technological artefacts[88]. Also, they seem to develop no critical reflection on the wider societal effects of smart technologies (e.g., fairness, democracy, surveillance, citizenship, human rights), and on how these reproduce certain models of political economy[89]. To counter the downsizing or these top-down approaches, bottom-up models of governance are proposed, where citizens and disadvantaged communities can actually be

79 European Parliament's Committee on Industry, Research and Energy (2014), p. 10.
80 See Chapter VI, §3.2.1.
81 See Kummitha (2017), pp. 46-47. See Chapter VI, §3.
82 Cocchia (2014), p. 33.
83 Kummitha (2017), pp. 45-46.
84 Id. On the impact of system theory on the conceptualisation of the city, see Merricks White (2019), pp. 35-36.
85 Sadowski et al (2019); Taylor et al (2017b).
86 Kummitha (2017), p. 48; Hollands (2008).
87 Kummitha (2017), p. 48.
88 See De Waal (2017).
89 Kitchin et al (2019a), pp. 3-5.

empowered by the introduction of smart technologies, improving participation, inclusivity and creativity[90].

Working concept of the Smart City. In light of the above, two descriptive elements, and a normative one, are identified in the notion of "smart city". For the purposes of this dissertation, the term is defined as follows:

> *A Smart city is a city where ICT solutions are leveraged to increase (i) the sustainability and efficiency of public services, (ii) the economic attractiveness of the city, and (iii) the overall quality of life of citizens. These solutions are often implemented thanks to multi-stakeholder cooperation, namely through public-private partnerships. Fairness, democracy, citizenship, social justice and human rights should be core values of the Smart City and should oversee the implementation of ICT solutions.*

This definition is still too general in relation to the scope of the present research. Indeed, it covers both *conventional* smart cities (e.g., smart cities built from scratch) and *retrofitted* smart cities (e.g., existing cities that are made smart through the progressive integration of technologies in the infrastructure). Since this study mainly chooses a European perspective, retrofitted smart cities seem to be the most pertinent reference setting for the investigation. This does not mean that notes to practical initiatives and issues in conventional smart cities will be completely avoided. They will be introduced where relevant for the arguments. Nonetheless, whenever smart city scenarios will be referenced throughout the dissertation, the mind should go to retrofitted smart cities.

3.2.4. The Internet of things

Definition. The IoT can be defined as a "global, distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, with other machines and with computers"[91]. For the last decade, the IoT has been considered one of the key technologies for building successful smart cities[92].

IoT architecture, model and layers. The IoT creates a seamless network fabric between "things" that is technically structured in three different levels and layers. According to Ning, the *architecture* and the *model* of the IoT should be distinguished: if the former describes the IoT from a network topology perspective, the latter outlines how the structure works from a functional point of view[93]. In IoT architectures, three different *levels* can be identified: (a) the basic connectivity level, establishing physical and logical connectivity between systems; (b) the network interoperability level, allowing communication between the connected systems; (c) the syntactic interoperability level, enabling the understanding of the data structure in all messages exchanged across the interconnected systems[94]. Differently, in a functional perspective, the IoT can be articulated in three different *layers*. In this sense, Ning proposed a three-layered model, comprising a sensor-actuator layer, a network layer and an application layer[95]. A more recent framework devised by Rayes and Salam conversely foresees four different layers:

---

[90] Id., p. 5.
[91] Davis (2015), p. 1; see also Pagallo et al (2017), pp. 59-78.
[92] On the importance of the IoT for smart cities, see Commission Staff Working Document (2016), pp. 34-35; OECD (2016), pp. 15-17.
[93] Ning (2011), p. 11.
[94] See Pagallo (2017), p. 64.
[95] Id., p. 65. Cf. Atlam et al (2020), p. 128.

1. IoT *Device Level* includes all IoT sensors and actuators (i.e., the Things in IoT) […].
2. IoT *Network Level* includes all IoT network components including IoT gateways, routers, switches, etc. […].
3. IoT *Application Services Platform Level* includes the key management software functions to enable the overall management of IoT devices and network. It also includes main functions connecting the device and network levels with the application layer […].
4. IoT *Application Level* includes all applications operating in the IoT network […][96].

A Functional Understanding of the IoT Paradigm. This dissertation will contemplate a *functional* understanding of the technology, setting aside the technical knowledge of the IoT. This should best grasp its features and the challenges it brings about from the legal perspective. In this sense, IoT applications comprise: (1) sensing hardware able to capture data from the outside world in real time[97]; (2) network capabilities enabling the flow of data gathered from different sensors; (3) software applications able to make sense of the data, also to produce predictive assessments (e.g., through profiling and big data techniques). According to this "reductionist" approach, Chapter 5 will analyse the legal implications of implementing different surveillance technologies building on the IoT.

4. Structure

Overall structure. The aim of this preliminary chapter has been to acquaint the reader with the main concepts and objectives of the research. Having set the stage for the analysis, the proposed main research question will be unpacked in six different sub-questions. Each sub-question will be addressed in a dedicate chapter of this dissertation. Each chapter will take a specific perspective on the topic and will comprise both the description and analysis of the state-of-the-art, as well as propositive contents and arguments. The logic underlining the chosen order reflects the need to first unravel foundational concepts of the research (Chapters I-IV), upon which more targeted analysis will be built (Chapters V-VI).

Chapter I. This is the first of two chapters revolving around data protection issues in smart cities. The addressed sub-question is the following: *Which legal grounds legitimise data collection in smart cities and what balancing exercises do they entail?* At the outset, the right to data protection represents one of the main normative benchmarks for the legal analysis in this dissertation. The analysis will thus start from the rationale, content and essence of the right to data protection – as enshrined in the CFREU and ECHR – which will serve as a background for the investigation. Because of their close interconnectedness, the right to privacy will also be taken into account, even though the study will mainly revolve around the foundational texts of the EU data protection framework (the GDPR and the LED). Therefore, the very applicability of the EU data protection legislation will be first scrutinised by making examples of different technology applications. Subsequently, relevant legal bases for data collection in public spaces will be identified, focusing on grounds that can justify urban surveillance activities. Specifically, the analysis will try to uncover the nature of the necessity and proportionality assessments that these legal bases entail.

Chapter II. This chapter will continue to investigate the data protection issues, tackling the following sub-question: *What are the issues that rise from personal data flows in smart cities and how should they be addressed?* Chapter II will take a more dynamic perspective in studying data flows within the city. Therefore, the

[96] Rayes et al (2019), p. 8.
[97] For an overview of different sensors, see Petersen (2012), pp. 157-165.

legal issues examinedare the purpose limitation principle, data controllership PPPs and participatory data protection impact assessments (DPIAs) in smart city projects. These research focuses have been selected based on the particularities of the smart city environment, as a governance setting populated by a diversity of actors handling city data (commercial players, public authorities and law enforcement agencies). The seamlessness of data flows among numerous actors raises tensions with the purpose limitation principle, a crucial tenet of EU data protection law. This strain appears to be magnified in the context of institutionalised PPPs, where intensive information sharing acquires stable features. In both cases, careful balancing between private and public interests is required. Through participatory DPIAs, these exercises could be opened up to the public at large, thus ensuring greater legitimacy of large scale smart city projects. All these aspects will be addressed in the analysis, comprising both an interpretation of relevant provisions and their potential translation in smart city scenarios.

Chapter III. Chapter III will mainly take a privacy perspective. The sub-question addressed in this chapter is: *Which reasonable expectations of privacy can individuals have in complex IoT environments such as public places in smart cities?* Again, the analysis will start with the reconstruction of the theoretical rationale behind the acknowledgement of the right to privacy. Specific attention will be drawn to the topic of privacy in public spaces, which is at the core of this research. Afterwards, attention will be drawn to ECtHR case law on the matter. Comparisons will be made with the case law of US jurisdictions (the United States Supreme Court, USSC, especially), which make use of the "reasonable expectation of privacy" standard to assess Fourth Amendment violations. Arguments embedded in the European and American case law will be critically examined to see whether and how these can apply to the smart city context. A multi-factor assessment to determine the existence and serious of privacy interferences in public IoT environments will be proposed.

Chapter IV. The findings of the first chapters will lay down the basis for a broader theoretical and legal discussion on surveillance in Chapter III. This analysis will focus on three perspectives: philosophical, sociological and legal. The sub-question addressed in this chapter is: *Which theoretical frameworks can best conceptualise surveillance schemes in smart cities and which proportionality assessments do they require?* The analysis will reflect the interdisciplinary nature of the field of surveillance studies. An overview of the philosophical theories on surveillance will be provided, in their chronological order of development. The focus will then shift to sociological perspectives on surveillance. The aptness of these theories to describe surveillance dynamics in smart cities will be scrutinised. The analysis will conclude with the extensive investigation of the latest (mass) surveillance case law of the CJEU and the ECtHR. The latest decisions will be studied through the lens of the proportionality requirement, whose implementation is increasingly problematic in preventive policing activities, as well as beyond the security domain. The arguments of the two Courts will also be evaluated within their possible translation in smart city environments.

Chapter V. In the second part, the focus will first shift to the analysis of specific surveillance technologies implemented in smart cities worldwide. Therefore, the sub-question addressed in this chapter is: *Which IoT surveillance technologies in smart cities can affect individuals' rights to privacy and data protection and how can these be proportionally implemented?* Some of the most relevant surveillance technologies deployed in urban environments will be chiefly discussed from a theoretical-legal perspective. Research focuses will revolve around the following technologies: facial recognition and biometric classification systems; sensor-based predictive policing (environmental policing); drones; smart nudging. As for the methodology, proportionality assessments will be consistently leveraged to evaluate the compliance of these instruments with the European human rights framework. The assessments will not target

concrete marketed technologies but will draw inputs from practical instances of implementation to provide the proposed arguments with a factual evidence basis.

Chapter VI. The last chapter closes the dissertation and integrates the findings from a broader ethical and governance perspective. The sub-question addressed in this chapter is: *Which data governance frameworks can most mitigate the impacts of surveillance in smart cities, ensuring a fair balancing of public and private interests in the urban sphere?* The analysis will take the privacy, data protection and surveillance issues that have been dealt with in the previous chapters (specifically chapters I-IV) as its background. Such hurdles highlight the power asymmetries that underlie the relationships between data subjects (citizens) and controllers (public authorities and data economy players) in the smart city. Where such gaps are magnified by the pervasiveness and opacity of the processing, bespoke solutions should be devised to limit the damages stemming from urban data flows. If previous chapters have provided answers from a legal regulatory standpoint, this last work will take a broader perspective by focusing on data *governance* frameworks. Community-based models will be outlined as alternatives to the data economy. Specifically, legislative Acts and proposals ensuing the *European Strategy for data* will be scrutinised to understand if and how smart cities could actually influence data and technologies for the common good of the city.

Conclusions. Some conclusive remarks will be introduced, summarising the major results of the research, which will be organised in a coherent fashion. To answer the chief research question, normative solutions about how to conceive privacy and data protection, and how to implement them in smart cities, will be proposed. These proposals will focus on the balancing exercises that ethical and legal implementations of surveillance technologies require in the urban sphere. From a data governance perspective, fine-attuned co-governance mechanisms will be identified to ensure a fair balancing of private and public interests in smart cities, also in light of the upcoming EU governance framework.

I. Data Protection Issues in Smart Cities:
Rationale and Grounds for Collection

1. Introduction and overview

Anonymity and Opacity in Datafied Cities. Digital data is one of the backbones of the smart city. It provides for insights and useful knowledge to better run services and boost citizens' quality of life. By connecting numerous objects over the Internet, the IoT serves smart cities' "data-hungry agenda". Traffic, people's gatherings, air pollution and humidity rates are all subject to an intense process of datafication[98], thus being translated into data and used for predictive judgements.

This invaluable intelligence on the city, its places and dynamics does not come, however, without a cost. For people living in these intensively "datafied" environments, privacy is in fact very much at risk. If once people could walk around the city streets going unnoticed, today sensors installed in bins and lampposts can track our movements meticulously[99]. A senior officer of the Dutch Data Protection Authority (DPA) expressed her concern on the matter: "You expect a certain degree of anonymity when you walk down the street, but in reality there are more and more cameras and sensors belonging to municipalities and companies that register or follow you, sometimes without you even realising it"[100]. On the roads, vehicles are traced with ANPR cameras[101]. CCTVs are now integrated into centralised systems, being checked in real time by dedicated police officers in control rooms[102]. Public transportation systems can be accessed with RFID cards or credit cards passed through tolls, tracking all passengers' tap-ins and tap-outs. In a not-so-distant future, data collection may directly bypass the boundaries of private homes, with devices allowing government authorities to zoom in on apartments to analyse energy consumption and detect possible gas leaks[103].

When is data personal in smart cities? It is not to be taken for granted that all data processed by smart city sensors can be qualified as "personal" under EU data protection law. For instance, many urban sensors only gather data on the environment (i.e., "environmental data"), like data about the weather, sound, crowding levels. These may not, at least at a first glance, be considered personal in the sense that their content relate to specific individuals. In addition, even when collected data concerns individuals directly, these are often subject to anonymisation techniques, which should in principle exclude applicability of data protection law.

Nonetheless, research in the field has shown that the scope of EU data protection law can be much more extensive than it first appears. Art. 4(1) of the GDPR defines personal data as any data that relates to someone who is identified or identifiable on the basis of that data. According to the broad interpretation of this provision given by Article 29 Working Group, data may relate to individuals not only in "content", but also in "purpose" or "result"[104]. In smart cities, this implies that almost *any* data

[98] As reported by Van Dijk, datafication "is the transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis". Van Dijk (2014), p. 198 (citing Mayer-Schoenberger et al (2013)).
[99] Vincent (2014); Yang (2019).
[100] Autoriteit Persoongegevens (2020).
[101] On ANPR see, e.g., Jansen (2018), pp. 5-6; Milaj et al (2020).
[102] In Rio the Janeiro, IBM worked to realise the largest urban control room, the *Centro de Operações da Prefeitura do Rio.* In New York, Microsoft partnered with the New York Police Department to set up the "Domain Awareness System", as reported by Ferguson (2017), p. 182; Froomkin (2015), p. 1721 ff.
[103] Privacy International (2017) (reporting of one project in Singapore).
[104] For an explanation on these requirements, see §2.4.

collected may in some way be qualified as personal, considering that the ultimate goal of all processing operations is to change the environment and positively affect the individuals living in it[105].

Furthermore, the advancements in big data analytics combined with the plurality of data sources in smart environments poses high risks of re-identification for individuals, even when their personal data have been anonymised or pseudonymised[106]. For instance, citizens can also be singled out in a group through unique combinations of non-unique identifiers. Notably, anonymised data about the use of taxis released by the New York Taxi and Limousine Commission was used to show where visitors to a local strip bar live[107]. In these circumstances, the applicability of EU data protection law may sometimes be extended also to supposedly non-personal data.

Lack of transparency in data collection, impossibility for consent. A fundamental attribute of the "smart" experience is its seamlessness. In the IoT paradigm, data collection is designed to be unobtrusive, and so are data flows. This also applies to smart cities, but with extended challenges[108]. Since sensing devices mostly go unnoticed when "hidden" in public spaces, data subjects are unaware of whether and how they are monitored. This prevents citizens from giving free consent for such data collection activities and makes urban surveillance dangerously subtle.

Unsurprisingly, the lack of meaningful opportunities for data subjects to express prior consent has been described as one of the biggest challenges for smart cities, especially in public spaces[109]. Stakeholders on the ground are already dealing with such issues. In a roundtable discussion on data protection issues in smart cities, one participant referred to consent-based data processing in smart cities as "a nice idea but unworkable", giving people a "false sense of power"[110]. In such a context, increased transparency obligations may not be the most pertinent solution. Citizens may be made aware of sensors' locations through public registries, but this cannot be equated to freely given consent to data collection[111]. The same goes for opting-out options: users can be enabled to switch off their smartphone's Wi-Fi tracking when in public, but opting-out is not the same as consent[112].

Power imbalances between public authorities and private companies, and respective positions towards data processing. As explained, one of the fundamental features of the smart city paradigm is the multiplicity of actors participating in the urban agenda. The involvement of the private sector in city management is certainly part of a broader shift in governance trends, which has only increased with digitalisation processes. Local governments do not normally dispose of the expertise and knowledge to equip their city with digital technology, and often turn to the private sector for that purpose. Big tech corporations involved in the smart city market have profited from the increased demand for software and devices. Because of the existing power imbalances, however, commercial giants have often unilaterally imposed their terms and conditions on municipalities, possibly to the detriment of citizens' interests and public good of the city[113].

---

105 Galič et al (2021), p. 7.
106 Woo (2017), pp. 960-961.
107 Bass et al (2018), p. 11.
108 Consent (or notice and choice) has been defined as one of the major challenges for the IoT in the consumer domain. Resource-constrained devices often lack large screens (or do not have one at all), thus making the display of privacy policies and other notices extremely difficult. See Peppet (2014), pp. 139 ff.
109 Edwards (2016), pp. 28-29; Kitchin (2016b), pp. 37-38; Finch et al (2017), p. 133.
110 Van Zeeland et al (2019), p. 10.
111 Id.
112 Id.
113 Taylor (2019), p. 5. (referring to Google's traffic management software Flow).

Furthermore, public and private actors may not hold the same position and attitudes towards privacy and data protection standards. Scholars have reported that there are already gaps in how the public and private sector comply with the relevant legislation[114]. On the one hand, commercial companies mainly rely on cost/benefit analysis, providing for enough privacy to keep their consumer basis loyal to the brand. On the other, public authorities running essential services may have higher ambitions in terms of what constitutes adequate privacy and personal data protection, with them also being more likely to be held responsible by the public in case of data protection breaches occurring in the context of outsourced activities[115].

Data re-use and sharing with third parties. Another way in which commercial actors are exploiting their commercial power over public authorities is claiming a right to data reuse[116]. Indeed, one of the biggest concerns around big data technologies is the constant push towards data repurposing[117] (a phenomenon also known as "function creep" or "data creep"[118]). This tendency, supported by important political actors, seems at odds with the principle of purpose limitation, as enshrined in EU data protection. If the value of big data lies in detecting unknown correlations, predetermining the means of the processing may not necessarily help in making the most of data[119]. In the smart city, this trend towards data reuse presents further challenges because of the diverse nature of public and private players that participate in processing. Many scholars and practitioners have claimed that data initially collected for public purposes should not in principle be transferred to private actors pursuing their own commercial gain[120]. Nonetheless, public-private partnership models often need mutual data transfers to function, thus favouring data repurposing by the involved entities.

Lack of control and ownership. With this plurality of actors involved, concerns over data ownership are also raised in smart city initiatives[121]. As stated by one data protection expert participating in a workshop about smart cities, "[t]he complexity of a project is related to data governance. Figuring out the ownership of data can take a long time"[122]. Indeed, since digital data is now commonly regarded as a financial asset, private companies have a prominent interest in gaining control(lership) over these priceless resources. Especially when it comes to complex processing operations, the possibility that data subjects exercise effective control over their own personal data is only an illusion [123]. And yet, the GDPR still aims at providing individuals with a sense of greater control over their personal data by strengthening information and consent requirements.

Data security issues. Lastly, smart cities also face important security and safety challenges. If the IoT makes urban infrastructure increasingly interconnected, it also extends attack surfaces available to hackers and other ill-intentioned agents, exposing citizens to potential consequences for their personal safety[124]. With data security being a fundamental element to the right to data protection, public authorities and private actors need to cooperate to achieve the highest standards of protection for collected data, despite economic and expertise challenges.

---

114 Braun et al (2018), p. 500. Cf. Ranchordás et al (2020), p. 14.
115 Id.; Finch et al (2017), p. 132.
116 Van Zeeland et al (2019), p. 8.
117 Edwards (2016), p. 45; Wisman (2013).
118 On function creep, see Koops (2021).
119 Moerel et al (2016), p. 7.
120 Van Zeeland et al (2019), p. 10; Vandercruysse et al (2019), p. 558.
121 Van Zeeland et al (2019), p. 10; Vandercruysse et al (2019), pp. 7 ff.
122 Vandercruysse et al. (2019), p. 7.
123 Moerel et al (2016), p. 9.
124 Kitchin et al (2019c); Dodge et al (2019), pp. 205-216. For examples, see also Douglas (2018); Teale (2020).

Outline. Against this backdrop, this first chapter will provide a first overview of data protection issues in smart cities. The sub-research question addressed here is: *Which legal grounds legitimise data collection in smart cities and what balancing exercises do they entail?* The applicability of EU data protection legislation will be assessed as preliminary question. Then, grounds for data collection in smart cities will be examined, outlining viable options for lawful smart city processing. The main objective in this review is discerning the balancing exercises that these legal basis entail with more granularity. On the contrary, the issues stemming from the circulation of personal data within the city will be examined in a separate chapter.

2. On the applicability of the data protection legislation

Should we distinguish data protection from privacy? It is clear that many of the above-mentioned situations pose both "privacy and data protection risks" in smart cities. It may have already resonated with the reader that these rights are often mentioned in a single breath[125], as one inseparable binomial. But to be truthful, is there a difference between privacy and data protection? Does keeping them separate allow us to better understand the issues of urban digitisation?

Before delving into specific smart cities issues, these questions will be addressed by providing a brief historical and theoretical account of the emergence of the right to data protection in Europe. Despite their overlapping scope, privacy and data protection are often coupled as a matter of undue simplification[126]. On a closer look, however, data protection appears to be underlined by a very specific rationale that deserves to be highlighted in the study at hand. Therefore, in the following sections will explain what data protection is and why it should (often) be kept separate from privacy, and will demonstrate why this distinction is relevant in smart cities. Lastly, the applicability of EU data protection legislation will be scrutinised in concrete smart city scenarios.

2.1. Historical account of the emergence of the right to data protection in Europe

First steps for the right to data protection. Like Eve was born from Adam's rib, so data protection appears to have surfaced as a precipitate of the right to privacy. As computers became increasingly widespread, the first pieces of legislation that started to regulate (automated) data processing practices in the 1970s were adopted mainly to protect what we would call privacy[127]. Among these, the *Hessische Datenschutz* (1973), which first introduced the expression "data protection", deserves special recognition, as does the Swedish *Datalag* (1973) and the French law on "computers and freedoms" (*informatique et libertés*). Other European States took a different approach, by providing the right to the protection of personal data with an early constitutional protection (e.g., Portugal in 1976, Spain and Austria in 1978).

At the international level, by the end of the 1970s different organisations had begun to work on how to regulate the processing of personal information. Most notably, two international instruments were adopted: in 1980, through the influence of the United States, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (the OECD Guidelines)[128]; in 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (the Convention 108)[129]. At this conjuncture, a (misunderstood) equivalence between the rights to data protection and

[125] See Raab (2020), pp. 7, 11; Pagallo et al (2017), pp. 59- 62 ff. Amnesty International (2017).
[126] González Fuster (2014), p. 255
[127] This conception still persists in some EU Member States (e.g., Belgium, Luxemburg, Ireland), see González Fuster (2014), p. 183.
[128] OECD (1980).
[129] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

privacy was first established[130]. Indeed, different legal instruments began to refer to the same matter as privacy or data protection laws interchangeably. On the one hand, Convention 108 referred for the first time to national data protection legislation adopted so far as "privacy" laws. On the other, under US influence, the OECD Guidelines also labelled these national norms as "privacy" laws. As a result, a vision that saw privacy and data protection as inevitably interconnected (if not synonymous) was legitimised.

The emergence of data protection legislation in the EU: The Data protection Directive. At this point, the EU as such had not yet laid down any bespoke legislation for data protection, although processing operations in Europe were covered either by sporadic national acts, or Convention 108 and the OECD guidelines. Convention 108, however, had a huge impact on the soon-to-be EU data protection legislation. In fact, this laid down the fundamental principles of European data protection, which were later crystallised in EU secondary law (namely Directive 95/46/EC[131] and Directive 2002/58/EC[132]). Directive 95/46/EC (the Data Protection Directive, DPD) became the main European Community instrument for the protection of personal data. Specifically, the Directive described one of its main objectives not as the protection of personal *data*, but as the protection of fundamental rights and freedoms of natural *persons* with regard to the processing of personal data[133]. At the same time, the DPD aimed to avoid restrictions to the free flow of personal data between Member States[134]. The DPD went beyond the scope of Convention 108, which only applied to *automated* data processing[135]. However, it excluded the protection of legal persons, activities falling outside the ambit of European Community law (i.e., public security, defence, national security), State activities in the domain of criminal law (which were later covered by Framework Decision 2008/977/JHA[136]), and those falling within the so-called "household exception". Content-wise, the DPD listed the principles relating to data quality (Art. 6), lawfulness (Art. 7), confidentiality and security, and laid down a special regime for the processing of special categories of personal data (Art. 8), as well as data protection rights (Section IV).

An important step in the shaping of the right to data protection: Informationelle Selbsbestimmung. Constitutional recognition of the right to data protection did not only occur by means of legislative action. The landmark judgment *Volkszählungsurteil*[137] by the German Constitutional Court (*Bundesverfassungsgericht*) played a crucial role in how the right to data protection is often conceived to this day. In 1983 indeed, the *Bundesverfassungsgericht* acknowledged the existence of a right to informational self-determination (*Recht auf informationelle Selbstbestimmung*), attributing to individuals the prerogative to decide which data about them are processed. The Court considered this right as a specific aspect of individuals' self-determination and free development of personality (Art. 2(1) of the German Constitution), that is their capacity of deciding autonomously and making free decisions, in their individual life and in society[138].

---

130 González Fuster (2014), pp. 254-255.
131 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, Official Journal L 281 (Data Protection Directive, DRD).
132 Directive 2002/58/EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector.
133 Art. 1(1) DRD.
134 Art. 1(2) DRD.
135 González Fuster (2014), p. 136.
136 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 L 350, 30.12.2008, p. 60–71.
137 *Urteil des BVerfG* v. 15.12.1983 zum VZG 83 (1 BVerfGE 65); *Mikrozensus-Urteil*, 16.07.1969 (1 BVerfGE 27, Rn. 20). For a detailed analysis, see Rouvroy et al (2009), pp. 45-76.
138 González Fuster (2014), p. 177.

Importantly, the Court emphasised the non-absolute nature of the right: individuals do not possess an unfettered mastery of their data; limitations are foreseeable, but only if they are provided by law and justified in light of general interests[139]. Admittedly, the approach of the German Constitutional Court had already played a role in the DPD's architecture, which comprised various provisions aiming at giving the individual comprehensive control over their personal data (e.g., rights of information, access, erasure).

The making of the Charter. As seen, the emergence of the right to data protection in Europe followed an inconsistent and fragmented pace. While in some countries a specific right to data protection was constitutionally introduced (e.g., Germany, Finland, Spain), in others, including France, a separate and autonomous right has not been explicitly established to this day[140]. Thus, in the absence of a common constitutional tradition among EU Member States, the adoption of Article 8 CFREU as a bespoke provision for data protection (independent of privacy) was crucial in affirming the self-standing value of data protection in the EU[141].

The CFREU is the outcome of a long journey aimed at strengthening EU's commitment to safeguarding fundamental rights. During the preparatory work[142], attempts to integrate the notion of informational self-determination were made[143]. However, this conceptualisation was rejected as the main underlying principle to the right to data protection in the EU and was thus subsequently excluded from the drafting of Article 8 CFREU[144]. Its definitive version appeared in 2000 and reads as follows:

> "1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority".

It should be noted that the CFREU constitutes an *uniquum* among supranational human rights instruments for the presence of two separate provisions dedicated to the right to the respect of private life (Art. 7), and the right to the protection of personal data (Art. 8)[145]. The choice was certainly innovative with respect to the ECHR. It also marked a distinction with Convention 108 and Directive 95/46/EC, which featured a vision of data protection as a prerogative merely serving other rights and freedoms (e.g., privacy, freedom of speech, principle of non-discrimination). However, the co-presence of Arts. 7 and 8 CRFEU has actually been seen as a compromise between the different constitutional views on privacy and data protection existing at the time[146]. If Art. 8 aimed at establishing a "new" fundamental right, the impact of such change was somehow curbed by the coexistence with Art. 7, thus reinforcing an image of data protection as purely instrumental to privacy[147]. Indeed, this ambiguity has

---

139 Id.
140 Id., p. 184.
141 however, that Rouvroy and Poullet point out that the recognition of the right to data protection as a separate right in the Charter may lead to the erroneous understanding that data protection is an "intrinsic" or "final" value, thus shadowing the rather *instrumental* or *intermediate* function that the right at stake bears in relation to other basic rights. See Rouvroy et al (2009), p. 50.
142 As reconstructed by González Fuster (2014), pp. 186 ff.
143 The German Professor and former member of the *Bundesverfassungsgericht*, Roman Herzog, proposed to employ the literal wording used by the German Constitutional Court to describe the right to self-determination. Marsch (2020), pp. 33-52, 43.
144 Kranenborg (2014), pp. 223–266, 229.
145 Id., p. 228.
146 González Fuster (2014), p. 199.
147 Id., p. 200; Lock (2019), p. 2123.

raised many questions on where the dividing line between the two rights should be drawn, and the CJEU has not shed light on the matter either, often referring to these rights jointly[148].

Data protection after Lisbon: the enactment of the GDPR. In 2016, a data protection reform package repealed the DPD with the enactment of the GDPR, which today constitutes the general instrument regulating personal data processing in the EU. Its provisions predominantly apply to the area of the former EU First Pillar, while processing in the law enforcement domain (i.e., former Third Pillar) is regulated by the Law Enforcement Directive (LED)[149].

The GDPR aims to enable the free movement of personal data, while also ensuring the right to data protection (Art. 1). Certainly, the adoption of Art. 16 TFUE enabled the EU legislator to take more incisive harmonisation initiatives in the data protection field. The choice of a Regulation, specifically, reflects the more advanced harmonisation level achieved through the DPD in First Pillar matters, while the former Third Pillar was subject to scattered regulations and specifically to a Framework Decision[150]. That is arguably why, in this latter field, the EU legislator opted for a less "penetrating" instrument like a Directive.

Without going into the details of the differences between the GDPR and the DPD[151], a first striking novelty brought by the Regulation is the addition of transparency and accountability as key principles of processing (Art. 5 GDPR); modifications were also introduced with regard to purpose limitation[152]. Also, the overall strategy underlying the Regulation is both preventative and adaptive: controllers are tasked with anticipating the risks associated with processing (e.g., through instruments such as DPIAs), and modulating the provided safeguards according to the assessed risk level (i.e., risk-based approach)[153].

Trying to overcome the lack of effectiveness of the safeguards provided in the DPD, the GDPR mandated private and public organisations processing sensitive or personal data on a large scale to appoint a Data Protection Officer (DPO). And most importantly, it significantly increased the level of imposable penalties, which under the DPD had a very low deterring effect on big companies[154].

2.2. Data protection: More than privacy and informational self-determination

Overlapping but different scope for privacy and data protection. It is a common understanding in literature that the protection of personal data has its roots in the right to privacy. Privacy per se is often described as having a wider scope than data protection. Not only it concerns the protection of personal information, but also involves the inviolability of the home, human body, private communications, or mind[155]. Data protection legislation thus appears to relate to a *specific* aspect of privacy, the protection of personal

148 Kranenborg (2014), p. 230; Lock (2019), p. 2116. In case law, see CJEU, *Volker und Markus Schecke GbR) and Hartmut Eifert v Land Hessen*, judgment of 9 November 2010, C-92/09 and C-93/09 §52. However, the EU jurisprudence does not always couple the two rights. In *Bavarian Lager*, the Court of First Instance of the CJEU stated that "[not] all personal data necessarily fall within the concept of 'private life'. A fortiori, not all personal data are by their nature capable of undermining the private life of the person concerned". See CJEU, *Bavarian Lager*, judgment of 8 November 2007, Case T-194/04, §§118-119. This approach was also confirmed by the CJEU in *Client Earth*, in which the Court stated that "the concepts of "personal data"… and of "data relating to private life" are not to be confused". See CJEU, *Client Earth,* judgment of 16 July 2015, Case C-615/13, §32. This inconsistency is criticised by Linskey (2014), p. 574.

149 Kosta (2022) provides an analysis of this choice. The draft LED was firstly analysed by de Hert et al (2012).

150 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 L 350, 30.12.2008, p. 60–7. Analysed by De Hert et al (2009c).

151 An overview can be found in De Hert et al (2013) and Hoofnagle et al (2019).

152 De Hert et al (2013), p. 134. For an analysis, see also Chapter II, §2.

153 See Chapter II, §4 for a specific analysis of these requirements.

154 Hoofnagle et al (2019), pp. 67-68.

155 Tzanou (2017), p. 23. Linskey (2015), pp. 11 ff.

data. At the same time, data protection covers processing activities that do not properly fall within the purview of privacy (e.g., data that is not necessarily "private" or "intimate", like the name). Therefore, privacy and data protection do overlap significantly, although not completely.

Weaknesses of the informational self-determination approach. A conceptual overlap between privacy and data protection is also found in the concept of informational self-determination[156]. If privacy is conceptualised as *control* over how and when one's information is communicated to the outside world[157], data protection is the *tool* allowing individuals to exercise control over their own personal data[158]. At the same time, however, considering informational self-determination as equivalent to the protection of personal data conveys a faulty representation of how data protection is actually conceived in the European framework[159].

Various reasons support this argument. First of all, from an historical perspective, privacy and informational self-determination have not always been the primary rationales leading to the emergence of data protection legislations in Europe[160]. In some Member States (e.g., Germany or Sweden), the right to the protection of personal data mostly ensured transparency in relationships between citizens and public administrations that are increasingly relying on computer databases or was conceived as an instrument to uphold other fundamental rights[161].

In the ensuing EU legislation, data protection was not initially inspired by fundamental rights concerns, but it was mainly seen as a crucial ingredient for the strengthening of the EU internal market[162]. Unsurprisingly, the DPD was adopted based on the former Art. 101a of the EC Treaty, which established EU competence in this matter. The Commission indeed believed that ensuring an equivalent level of protection of fundamental rights in all Member States would foster mutual trust in the performance of cross-border commercial transactions[163].

The multifaceted rationale of data protection was also reflected in the drafting of the Charter, which rejected a formulation including an explicit mention to informational self-determination. This distinctly emerges in the fact that consent does not represent the only basis for personal data processing in the EU[164]. In fields like the public sector, informational self-determination cannot function as a viable tool to regulate the relationships between data controllers and data subjects[165]. Data processing in this domain rarely relies on consent and rather uses grounds such as "public interest" or "legal obligations". Data protection rights are enforced, but to a minimum standard: citizens can request that their data is kept up-to-date or erased under certain circumstances, but they cannot decide whether their data should be processed at all or for which purposes. In the private sector, the German Constitutional Court slightly deviated from the original contents of the right to informational self-determination. Acknowledging the weaknesses of the right at issue in an increasingly "non-linear" data processing

156 Kranenborg (2014), p. 228; Rouvroy et al (2009), p. 68; Rodotà (2009), pp. 77-82.
157 As Helen Nissenbaum puts it, in theoretical scholarship on privacy two main approaches can be discerned: some characterise privacy as a form of restraint on access on information; others as a form of control over information. See Nissenbaum (2009), pp. 69 ff.
158 Cfr. Rouvrouy, Poullet (2009), p. 70; Tzanou (2017), p. 23.
159 Rouvrouy, Poullet (2009), p. 51 (also mentioning that the right to self-determination is often misunderstood); Marsch (2020), p. 43; von Grafenstein (2020), pp. 515 ff.
160 Christofi et al (2019), p. 32.
161 González Fuster (2014), pp. 56 ff.
162 Tzanou (2017), p. 16.
163 González Fuster (2014), p. 125.
164 Kranenborg (2014), p. 228; Koops (2014a), pp. 252-253. Instead, consent is increasingly seen as a problematic legal basis for processing in online contexts, especially in light of the IoT and AI.
165 Koops (2014a), p. 253.

world, it clarified that individuals may retain a right to disclosure of the data concerning them, but not always a right to decide how their data will be subsequently used by private companies[166].

Two different rationales. The efforts to distinguish privacy from data protection have also been centred on the *structure* of the rationale underpinning these rights. In the opinion of various scholars, privacy is underpinned by a negative (or prohibitive) rationale, while data protection is instead underpinned by a dynamic (or permissive) one[167]. In other words, the right to privacy functions as a prohibition rule, aiming to avoid undue interferences from the outside. Data protection, instead, starts from the assumption that personal data *can* be processed, although under certain conditions. Gutwirth and de Hert provide the most powerful reconstruction in this sense[168]. On the one hand, they contend that privacy mainly serves as a "tool of opacity", setting the normative limits to power; on the other, data protection is described as a "tool of transparency", regulating and channelling necessary, reasonable and legitimate power of public authorities to process personal data[169].

Prohibitive rationale. Embracing a permissive or prohibitive rationale has a very direct bearing on the meaning of data protection as enshrined in the Charter. Generally, those that value self-determination and control over one's information as the core of data protection privilege the idea of a prohibitive rationale to the right at stake[170]. This approach is based on a literal interpretation of Art. 8(1) CFREU, which reads: "[e]veryone has the right to the protection of personal data concerning him or her". Such wording has been viewed as essentially prohibiting *any* data processing operation. On the contrary, the six data protection principles recalled in paragraphs (2) and (3) identify conditions in which the processing would then become permissible[171]. While this reconstruction is not unanimously upheld in literature, it received an important endorsement by the CJEU. In *Digital Rights* the Court found that any measure providing for the processing of personal data "constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter"[172], thus automatically triggering the application of Art. 52(1) CFREU.

Permissive rationale. Differently, the permissive perspective underscores the idea of the enabling rationale of data protection. The underlying idea is not control, but *fairness*, as data protection is devoted to providing safeguards to the processing, rather than prohibiting it[173]. This claim could also be anchored to literal wording of Art. 8 CFREU, which does not enshrine the concept of self-determination[174]. The proponents of this theory also see Art. 8 as unitary provision determining the contents of the right to data protection. This is important because it provides a different definition of how an interference to the right at stake is established. In this case, indeed, not all data processing activities encroach upon the right to data protection, but only those that specifically violate one of the

166 Von Grafenstein (2020), p. 515.
167 See Rodotà (2009), pp. 79-80; Marsch (2020), p. 44. *Contra* see Christofi et al (2019), pp. 55 ff.
168 De Hert et al (2006). Cf. Hildebrandt, Koops (2010), p. 448.
169 This approach is certainly one of the most comprehensive elaborated so far, but its contradictions have been highlighted among scholars. Tzanou for instance argues that while this theory is aimed at showing the autonomous value of data protection, it ends up defining it always in relation to privacy. Indeed, Gutwirth and de Hert hold that if data protection identifies which are the acceptable forms of exercising power, the question of whether power can be exercised at all should still be determined according to privacy standards. See Tzanou (2017), p. 33.
170 Cfr. Christofi et al (2019), pp. 55 ff.
171 Id.; Tzanou (2017), p. 40.
172 CJEU, *Digital Rights Ireland Ltd v Minister for Communications Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* judgement of 8 April 2014, Joined Cases C-293/12 and C-594/12, §36; see also CJEU, *Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union,* Opinion of 26 July 2017, §126.
173 Christofi et al (2019), p. 54. On fairness in data protection law, see Clifford et al (2018).
174 Id.

six principles enshrined in paragraphs (2) and (3)[175]. Overall, under the positive or permissive theory, data subjects do not have a claim to forbid any processing of their personal data, but certainly have a right to have their data processed fairly.

2.3. Why should we distinguish privacy from data protection in smart cities

Enabling rationale of data protection and innovation. As seen above, cities find their way to smartness mainly thanks to digital technologies. Thus, innovation represents a core objective in smart city agendas worldwide. Against this backdrop, choosing a negative or prohibitive rationale for data protection would not certainly favour a fruitful development of digital technologies in this and other domains[176]. Quite the opposite, seeing smart city issues through the lens of permissive interpretation of data protection enables the interpreter to highlight the positive connotations behind data collection practices. These may not only be associated with invasions of citizens' private spheres, but also with the pursuit of goals of general interest, such as the improvement of quality of life or the protection of the environment. Admittedly, privacy and data protection matters may often conflate, especially when privacy interferences stem from the use of smart technologies. Nonetheless, giving data protection an *enabling* rationale may help us to avoid an overly restrictive or conservative view on some the legal issues at stake.

The role of fairness. From a human rights perspective, a positive construction of data protection appears to be more interesting for the centrality of fairness. As an overarching principle of EU data protection law, fairness receives explicit recognition in several provisions of the GDPR[177]. This principle entails that data subjects should not be submitted to unjustified adverse consequences as a result of processing. More broadly, however, fairness also evokes the idea of balancing between competing interests: those of the controller or the company, or those of the data subject. Through the lens of the law, real world situations and relationships often entail a clash between a plurality of norms and principles. Decision makers (e.g., judges, data controllers) may be then called on to weigh up opposing interests, all considered socially protected, and to settle the conflict in a reasonable and equilibrated manner[178]. Data-driven activities make no exception in this regard. Legitimising data processing normally requires justifications and concrete balancing exercises[179]. Given the importance of data in smart cities, this perspective seems the most adequate to deal with competing interests arising in these politically, socially and culturally complex settings. The concept of fairness in data protection is also pivotal for its *procedural* nature. Indeed, it has been argued that in a world of pervasive large-scale processing, major challenges for the law concern "access to justice and procedural fairness"[180].

Data protection and the "publicness" of smart city processing. A permissive conceptualisation of data protection also seems to better match the specificities of the urban context. An approach to data protection that mainly revolves around the idea of control and informational self-determination may indeed disregard the role that "*publicness"* occupies in urban life (e.g., with regard to the spaces of data collection, and grounds for processing).

Firstly, consent-based processing in public spaces is extremely problematic (if not impossible) in smart cities[181], which makes any attempt to attribute sufficient control over their own personal

[175] Id.; Tzanou (2017), p. 40.
[176] Cf. Marsch (2020); cf. van der Sloot B et al (2021b), p. 304.
[177] Arts. 5(1)(a), 13, 14 GDPR.
[178] Durante (2013), p. 440.
[179] Clifford et al (2018), pp. 140 ff.
[180] van der Sloot B et al (2021b), pp. 304-305.
[181] Indeed, non-consual legal bases for processing are currently in smart cities, see §§3.2. and 3.3.

information to citizens rather utopian[182]. In some cases, instead, consent is not a viable legal basis *at all*. Emblematically, this is the case of (smart) CCTV cameras used in law enforcement contexts. Under the LED, consent cannot legitimise data processing: only the prevention, investigation, detection or prosecution of criminal offences, as well as the protection of public safety can serve this function[183]. Given the importance of safety objectives in smart cities[184], therefore, consent- or control-oriented views of data protection may not be the right conceptual tool to look at data processing in these settings.

Secondly, life in smart cities is often hectic and marked by a fast pace[185], and citizens cannot reasonably be expected to spend too much intellectual effort in deciding whether to allow data collection, and for which purposes, or whether to opt for different paths or services. In other words, smart citizens are too often placed in situations where convenience is easily prioritised over personal data control.

Thirdly, applying consent and traditional data protection rights appears problematic in the public sector domain, which plays a pivotal role in the smart city[186]. Governmental authorities are obliged to respect data protection rights, but limited only to basic standards of fair processing (e.g., keeping data accurate and up to date). Data subjects are not provided with any form of control over if and how the data are processed, and for which purposes. Put simply, there is no informational self-determination in the public sector[187].

Data protection and private/public space. Data protection can help to better grasp the changes brought about by the IoT also due to the lack of a strong conceptual dichotomy between public and private space[188]. It is well known that privacy theories have consistently leveraged the traditional gulf between private and public spheres[189]. While these conceptual categories are not totally absent in data protection legislation[190], they do not usually refer to the nature of the place where the processing originated[191]. In this perspective, data protection appears to provide interesting tools to deal with IoT technology, which is blurring the boundaries between public and private spaces[192] more than ever.

Conclusion: Different but overlapping scopes. In these sections, various arguments have been put forward to highlight the difference between privacy and data protection. These differences gain special relevance in smart cities, which explains why a bespoke analysis of these rights should be made in separate chapters. This *per se* does not mean that privacy and data protection are radically different in all their aspects. Especially when digital technologies are involved, the protection of privacy often goes through the protection of our personal data, which explains why privacy and data protection have overlapping scopes and go hand in hand in several scholarly analysis. While acknowledging this conceptual proximity, however, it may be useful to keep them separated in the legal analysis. For instance, as it will be shown in the next chapter, privacy appears more apt to look at matters that bear a

[182] In relation to online contexts, see Koops (2014a), p. 251.
[183] Art. 1(1) LED.
[184] Marat et al (2021), p. 248; Wiig (2019), pp. 49-58.
[185] See Kitchin (2017a); Edwards (2016), p. 54.
[186] Koops (2014a), p. 253.
[187] Id.
[188] Edwards (2016), p. 40.
[189] Galič (2019), pp. 17-18; Nissembaum (2004); Koops (2014b).
[190] See Art. 23 GDPR or the so-called 'household exception'.
[191] Edwards (2016).
[192] See Koops (2014b).

strong *spatial* dimension, and it also covers aspects that cannot necessarily be captured through the lens of data protection.

2.4. Multi-layered identifiability in smart environments

Outline. Some further preliminary considerations need to be devoted to the purview of EU data protection legislation, especially in smart environments. Traditionally, the applicability of data protection is triggered by the notion of "personal data". The following sections will unpack this concept and examine its potential meaning and shortcomings in smart urban environments.

2.4.1. The concept of personal data in the GDPR

Overview. The Regulation has not deviated from the original notion of personal data enshrined in the Data Protection Directive. Indeed, under Art. 4(1) of the GDPR:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

This definition also comprises pseudonymous data, which are data that cannot be attributed to a specific individual without specific additional information (Art. 4(5) GDPR). On the contrary, anonymous data cannot be related to any identified or identifiable person, and are excluded from the scope of data protection law (Recital 26 GDPR).

Art. 4(1) GDPR is also complemented by Recital 26, which provides a dynamic and contextual notion of personal data, i.e., the *reasonable likelihood* test of identification of the data subject. To see whether a natural person is identifiable, controllers should consider all the means that are likely to be used in light of the costs, the amount of time required for identification, and the technology available at the time of the processing given the technology developments.

Based on this test, the same datasets may not be personally identifiable at the beginning of processing, but may become so as circumstances change, and vice-versa[193]. In fact, different studies have shown how big data applications are able to re-identify individuals in seemingly anonymised datasets by combining disparate data sources[194].

Furthermore, another element adds further blurriness to the boundaries of the concept of personal data: the "relate to" criterion. How data should relate to individuals to be considered personal is not explained by the GDPR nor was it by the Directive. As a result, this expression has been subject to different interpretations by the Article 29 Working Party and the CJEU.

Against this confusing background, the approach of the Article 29 Working Party will be leveraged to explain the concept of personal data[195]. Although non-binding, the Working Party's Opinion has been regarded as highly authoritative and influential in literature[196]. According to the Working Party, the enshrined notion of personal data can be unpacked in four different building-blocks: (i) any information; (ii) relating to; (iii) an identified or identifiable; (iv) natural person (which will not be examined here).

---

[193] Purtova (2018a), p. 47.
[194] Id., pp. 47-48.
[195] Article 29 WP (2007), p. 6.
[196] Purtova (2018a), p. 43.

(i) Any information. The concept of information is not defined at the legislative level, although the Working Party and the CJEU interpret it broadly[197]. The concept covers all statements about a person, whether objective or subjective (e.g., opinions and assessments), true or false, private or sensitive[198]. Also the format in which information is presented bears no relevance (e.g., alphabetical, numerical, graphical, photographical or acoustic, on paper etc.)[199].

Experts have also remarked on the broad nature of the "any information" criterion[200]. Some even argue that to be considered information, data does not need to be *meaningful* to those who use it. For instance, Hildebrandt explains that, for both organisms and artificial intelligence machines, information does not "necessarily imply the attribution of meaning, as may be the case of humans"[201]. Consequently, the concept of personal data could be significantly stretched in smart environments, where artificial machines now manage information as much as humans do, if not more.

(ii) Relating to. The Working Party has explained that data may "relate to" a specified individual in *content*, *purpose*, *result*[202]. Most intuitively, data concerns an individual when it is *about* that individual (e.g., one's medical records, image recorded by a camera). In some situations, data may directly concern objects and not individuals[203]. Electronic devices may convey information about specific individuals because of their physical or geographical proximity[204].

Also, data relates to an individual when it is used *with the purpose* to assess him or her, treat him or her in a certain way or affect his or her status or behaviour[205]. The Working Party specifies that this purpose-based relationship can be established not only when data has already been used, but also when it will be likely used with the aim of having an impact on specified individuals.

Over time, the CJEU gave contrasting interpretations of this criterion. In *YS and others,* the Court excluded that the legal recommendations contained in the minutes of an immigration interview could qualify as personal data[206]. The legal analysis of the applicants' situation could not possibly be considered personal data, as it was "not in itself liable to be the subject of a check of its accuracy by that applicant and a rectification"[207]. Later in 2017, however, the Court revised its approach in *Nowak*, which had several similarities with *YS and others.* The preliminary ruling question essentially focused on whether the exam script containing candidate's answers and the relative examiner's comments might constitute personal data. Following the Opinion of AG Kokott[208], the Court considered that the comments evaluating the exam performance related indirectly to the candidate and thus were subject to data protection law. In its reasoning, the Court also reproduced almost *verbatim* the position of the

197 Id ; CJEU, *Criminal proceedings against Bodil Lindqvist*, judgement of 6 November 2003, Case C-101/01, §88; CJEU, *Peter Nowak v Data Protection Commissioner*, judgment of 20 December 2017, Case C-434/16, §34.
198 Id; CJEU, *Nowak*, §34.
199 Id., p. 7.
200 Purtova (2018a), p. 50. It is widely acknowledged that information is a rather fuzzy concept with different meanings, which can vary across time and disciplines. In the legal field, a frequently adopted definition is the General Definition of Information (GDI): information is data + meaning. Data here is understood as a description of anything that can be recorded, analysed of reorganised; data becomes information when we (humans) make sense of it.
201 Hildebrandt (2010), p. 10; Purtova (2018a), p. 53.
202 Article 29 WP (2007), pp. 9-10.
203 Id., p. 9.
204 Id., pp. 9-10. The Working Party brings the example of the value of a house. While data protection law would not usually apply to this kind of data showing only the level of real estate prices in a certain district, under certain circumstances these could actually be considered as personal data, e.g., if the value of a house is used to determine taxes obligations of a citizen. The same can be argued for RFID tags.
205 Id., p 10.
206 Cf. Opinion of Advocate General Sharpston in C-141/12 and C- 372/12 *YS and others*, §§50-56.
207 Id., §45.
208 Opinion of Advocate General Kokott in C-434/16 *Nowak*, §61.

Working Party, declaring that data may be linked to a particular person "by reason of its *content, purpose or effect*"[209].

Lastly, data relates to an individual by result when its use is likely to have an impact on a person's rights and interests, considering all the contextual factors of the case at stake[210]. The Working Party specifies that it is not necessary for the potential result to have a major impact on the data subject; it suffices that he or she may be treated differently because of the processing of his or her personal data[211].

(iii) An identified/identifiable (natural person). The Working Party explains that one person is identified when it can (or could) be "singled out" or "distinguished" from other people within a group[212]. Identification can be direct or indirect. On the one hand, direct identification can be achieved with the most common identifier, a person's name[213]. On the other, indirect identification is made possible by "unique combinations" of seemingly innocuous identifiers (e.g., gender, address) and other pieces of information, which allow one individual to be singled out.

Identifiability should be established according to the "reasonable likelihood" test in Recital 26 GDPR. The Working Party indicated that the means "reasonably likely to be used" should not be understood in relation to the subjective, factual capabilities of the controller[214]. It should not be measured in light of the specific technologies available *in concreto* to the controller (e.g., a company or a municipality), but considering the tools that could be reasonably used by any other entity. Nonetheless, a pure hypothetical possibility is not enough for data protection law to apply. The reasonable likelihood standard should indeed be assessed in light of specific factors identified by the Working Party:

- the cost of identification;
- the intended explicit or implied purpose of processing;
- the advantage expected by the controller in case of identification;
- the interests at stake for individuals;
- the risk of organisational dysfunctions and technical failures, data breaches included;
- the state-of-the-art technology at the time of processing, including possible technological developments in the future, within the processing cycle;
- measures to prevent data identification should be taken into consideration to understand whether personal data is processed at all, rather than to comply with data security obligations under the Regulation[215].

The CJEU addressed the issue of identifiability in *Breyer*[216], where it endorsed an objective interpretation of this criterion. The legal question at the centre of the case was if dynamic IP addresses could be considered personal data. In a previous case, the CJEU had found *static* IP addresses to be personal data, as they allow Internet service providers to precisely identify users[217]. *Dynamic* addresses, however, are different: they change each time there is a new Internet connection and do not allow controllers to directly establish links between a given computer and an Internet connection. This means

209 Id., §35 [emphasis added].
210 Article 29 WP (2007), p. 11.
211 Id.
212 Id., p. 12.
213 Id., p. 13.
214 Recital 26 GDPR (emphasis added).
215 Article 29 WP (2007), pp. 15-17.
216 CJEU, *Patrick Breyer v Bundesrepublik Deutschland,* judgement of 19 October 2016, Case C-582/14.
217 CJEU, *Scarlet Extended*, judgment of 24 November 2011, Case C-70/10, §51.

that controllers cannot identify individuals without the support of additional information. Against this background, the Court considered that it is not necessary that (1) data should allow for *direct* identification of an individual to be considered personal; (2) all the data needed for identification are in the hands of one controller (objective approach to identifiability)[218].

Furthermore, the Court established an additional criterion: the legality of identification. It stated that identification by combining dynamic IP address with additional data held by Internet service providers could be reasonable if not "*prohibited by law* or practically impossible" due to "a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant"[219]. Following this analysis, the Court found dynamic IP addresses in *Breyer* to be personal data under EU law.

Considering all the elements at play in the qualification of personal data, the following sections will explore when EU data protection applies to smart cities. In such environments, pervasive data collection and the capabilities of big data technologies significantly increase the chances of (re-) identification of individuals, despite the anonymisation measures. The wide notion of personal data and the objective interpretation of identifiability only reinforce this expanding trend of EU data protection law.

2.4.2. *Identifiability* in smart cities

Changing environments with the IoT: Ambient intelligence. Originally, data protection case law and scholarship focused on traditional large database processing, which did not pose great problems in terms of identifiability. The first challenges in this sense emerged only in online contexts, with the proliferation of big data processing. Nowadays, conversely, the IoT and the proliferation of smart environments have arisen additional problems. This novel paradigm, built on the idea of ubiquitous computing, has taken the name of "ambient intelligence", and is endorsed by the European Commission as a "vision of our technological future"[220]. In these settings, the distinction between what is online and what is offline is increasingly blurring[221]. The environment itself can infer people's needs and preferences based on behavioural and biometric profiling. Interconnected data collection points are infused in our homes, offices, cities, and allow the online and offline worlds to communicate. These adaptive environments learn about when and how we get up, go to work, spend time with our special ones, and adjust their features and services to our desires in a loop. In other words, they are our seamless "digital butlers"[222].

Issues of ambient intelligence in smart cities. To date, the smart city represents one the most ambitious versions of ambient intelligence. Public lighting switching on automatically for passers-by, traffic lights accommodating road flows, or noise levels alerting about potentially escalating situations exemplify how the urban environment can mould itself to better serve its inhabitants. Data is the primary basis to support decision-making, rationalise resources and develop urban planning[223]. Therefore, smart environments heavily rely on profiling techniques on a large scale, e.g., to detect movement patterns within the city[224]. Invisible sensors in urban infrastructure interact with people's IoT devices (e.g., smartphones), potentially registering all kinds of data emitted towards public networks (i.e., passive

[218] CJEU, *Breyer*, §§40-43.
[219] Id., §46 (emphasis added).
[220] See Hildebrandt, Koops (2010); Hildebrandt (2008), p. 430; De Hert et al (2009b).
[221] Floridi (2015), p. 5.
[222] Hildebrandt, Koops (2010), p. 431.
[223] On the notion of big data, see Barocas et al (2013), p. 46.
[224] Hildebrandt, Koops (2010), p. 431.

tracking or fingerprinting). As it previously happened in the online context[225], the industry working in the sector often claims that the data being processed is not personal[226]. Nonetheless, businesses may work with a very restricted notion of identifiability. Of course, public sensors may not record our names as they detect our smartphones within their range – but that does not mean that we cannot be singled out in a crowd and targeted, even by malicious actors. Besides, even the processing of seemingly non-personal data may, in progressively more scenarios, have some sort of impact on groups or non-specifically identified persons.

Granularity of IoT data makes anonymisation more difficult. Identifiability in smart environments is also significantly impacted by the technical features of the IoT. Indeed, IoT data are particularly difficult to anonymise because of its granularity, as underlined by the Working Party[227]. Research has shown that robust anonymisation of sensor data is extremely difficult to achieve, or, at least, that re-identification is far easier than one could imagine[228]. Against this backdrop, scholars point out that preserving the anonymity of these datasets is extremely hard [229]. In smart cities specifically, recent research highlights that big mobile data is particularly prone to "de-anonymisation" in urban planning[230]. As a matter of fact, technologies seem to be available on the market precisely to single out individuals' moving patterns within cities[231].

The law of everything? In light of this, what amounts to identifiability can be highly debatable in smart environments[232]. The notion of personal data, for its fuzziness and flexibility, does not always lead to black or white solutions when it comes to assessing the applicability of EU data protection law. The advent of the IoT, with its blurring effect on the online and offline spheres, put an additional strain on the concept of personal data and on the scope of data protection legislation.

For instance, drawing a clear-cut line between personal and non-personal data is not easy, especially when it comes to environmental sensors. Smart environments are designed to adapt to the needs of the people living in them. In this sense, all data processing operations in such contexts relate to individuals in some way. In literature, this argument has been made with regard to the Stratumseind project[233]. Specifically, it has been asserted that weather data in this context, although not *about* people, may be leveraged to assess and influence (deviant) behaviour of persons walking down the streets[234].

Concretely, people may be considered to be less likely to engage in (micro)criminal activities (e.g., drug dealing, rioting) in specific weather conditions. Identification of suspicious individuals certainly does not come from weather information alone, but from its combination with Wi-Fi tracking, sound and video recording[235]. Nonetheless, it could be argued that, in this project, weather data would always relate to people at least in *impact*[236]. Although not *about* people, these data can indeed be used to make decisions *impacting* on them. The personal nature of weather data may be thus argued, although applying all traditional data protection rights in this case may not be straightforward.

---

225 Leenes (2007), p. 137.
226 Cf. Galič et al (2021), p. 4.
227 Article 29 WP (2014a), p. 8.
228 Peppet (2014), p. 130; Hardesty (2013).
229 Id.
230 Lin et al (2021), p. 78.
231 Id, pp. 78, 83.
232 Leenes (2007), p. 138; van der Sloot et al (2021a), p. 310.
233 See Purtova (2018a), pp. 57 ff.
234 Id, p. 57.
235 Id.
236 Id.

Against this backdrop, the following subsections will firstly outline various ways to conceive identifiability in (semi)online contexts, which should be taken into account when determining if data protection applies in smart cities. Subsequently, such categories will be applied to specific instances of urban technologies, performing a case-by-case analysis. Lastly, potential solutions to achieve a reasoned application of data protection in smart environments will be sketched.

2.4.2.1. Beyond Look-up identifiability

Look-up identifiability (L-identifiability). One of the most influential and authoritative classifications of identifiability in data protection literature is provided by Leenes in 2007[237]. He distinguishes four kinds of identifiability which should trigger the application of EU data protection law. The most intuitive type is L-identifiability, which presupposes the existence of a register that links identifier and specific individuals[238]. This allows the individual's unique identity as a private citizen to be established[239]. Names, telephone numbers, ID numbers and IP addresses are all examples of L-identifiers[240]. From a privacy perspective, the particularity of L-identifiers is that they allow the individual to be targeted beyond the contexts where the identifier was originally used[241].

It is important to highlight that static and dynamic IP addresses both qualify as L-identifiers and constitute personal data. Therefore, data generated by IoT devices should be considered personal, unless appropriate anonymisation measures are taken. Before *Scarlet Extended* and *Breyer*, however, this conclusion was not straightforward, as data generated in the IoT domain can only be linked to machines and other non-human objects, and not directly to data subjects[242].

Recognition identifiability (R-identifiers) and Session identifiability (S-identifiers). R-identifiers allow individuals to be singled out without associating the identifier with a named individual[243]. They require the presence or an activity of the individual, whose identity is verified based on the presentation of an identifier, a token or a set of features (e.g., description of physical appearance). Such identification is legitimate and trustworthy only insofar as the recipient acknowledges the validity of the identifier[244].

S-identifiers are instead a subset of R-identifiers allowing web servers to track users during one *session* of interaction with their website. This might be the case of an e-commerce site that places a cookie on the user's machine in order to follow him or her throughout his or her shopping experience (e.g., right language, shopping cart)[245].

R-identifiers are very common on the internet. Cookies and identity credentials, are notorious examples. Compared to L-identifiers, however, they do not allow the person to be singled out outside the context in which they were issued. R-identifiers can be turned into L-identifiers only if centrally stored and linked with further personal data (as happens with biometric technologies)[246]. Potentially, this does not make R-identifiers any less privacy-invasive than L-identifiers. In big data environments, it does not necessarily matter whether the individual is identified, but rather if he or she is *reachable* by the technology, and thus subject to its predictive inferences[247].

---

237 Cf. Koops (2014a); Prins, Moerel (2016); Purtova (2018a); Earls Davis (2020).
238 Leenes (2007), p. 148.
239 Prins, Moerel (2016), p. 31.
240 Leenes (2007), p. 148.
241 Id., pp. 148, 154.
242 Cf. Urgessa (2017), pp. 524-525.
243 Leenes (2007), p. 149; Prins, Moerel (2016), p. 31.
244 Leenes (2007), p. 149.
245 Id., p. 152.
246 Id., p. 150.
247 Barocaset al (2013), p. 45.

Classification identifiability (C-identifiability). In this case, predefined group profiles or categories are set, and individuals are distributed into them, according to how they interact with specific websites. The purpose of this operation is not so much to obtain the civil identity of the individual, but rather to ascribe the individual to one of the predefined profiles. Therefore, like R-identifiers, C-ones do not need to be tied to the civil identity of the individual to fulfil their function[248]. Usually, R-identifiers are issued by the controller (e.g., the website owner) to monitor the behaviour of specific users and recognise it in the future[249]. In this sense, R-identifiability is used to build C-identifiers.

In literature, this process normally goes by the name of profiling. This term describes a partially automated process used to discover correlations in large datasets, with the aim of building classes of categories of characteristics that can be leveraged to generate profiles of individuals and groups, or whatever is of interest[250]. This allows to adopt specific decisions based on how the individual has been classified. Therefore, profiling qualifies as a form of surveillance, which monitors people's behaviour to tackle the uncertainties of the future.

Profiling and personal data. The question of whether profiling (always) amounts to processing personal data has sparked heated discussions among scholars for many years; and yet, this debate cannot be considered fully solved to this day[251]. On the one hand, some have excluded that profiling always involves the processing of personal data. This argument builds on the fact that profiling is a process articulated in a three-fold way: (1) collecting personal and/or non-personal data; (2) creating the profile; (3) applying the profile[252]. If no personal data is processed in the first step (e.g., in the case of behavioural biometric profiling), the whole process will escape the scope of data protection law[253].

On the contrary, in its Recommendation on profiling, the Council of Europe adopted an opposite approach, arguing that when the profile is applied to a specific individual, the latter always becomes identifiable[254]. Thus, the processing should be submitted to data protection law. This "anti-formalistic" approach seems to reflect the position of the Working Party, which focuses on the final *purpose* or *impact* of the processing on the data subject to determine the applicability of data protection law. For the purposes of this analysis, this second position may be more apt to *concretely* address the potential harm brought by surveillance technologies. Nonetheless, concrete evaluations on whether data protection can only be applied on a case-by-case basis, as will be shown next[255].

2.4.2.2. Identifiability in smart city applications

1) Sensor tracking. With the development of the IoT, more and more data will be broadcast to public networks, also "*by default*", that is unbeknownst to data subjects[256]. Data collected with machine identifiers (e.g., MAC and IP addresses) can be leveraged in "passive tracking" or device fingerprinting, thus allowing for more stable identification of the individual[257]. The potentialities of location tracking practices are even amplified by the possibility of combining different data sources (e.g., CCTV cameras

[248] Leenes (2007), p. 152; Prins, Moerel (2016), p. 31.
[249] Leenes (2007), p. 152.
[250] Bosco et al (2015), p. 4.
[251] Galič et al (2021), p. 10.
[252] Schreurs et al (2008).
[253] Id., p. 243.
[254] Committee of Ministers of the Council of Europe (2010), §§40, 50.
[255] See below some examples at §2.4.2.2.
[256] EDPS (2017b), p. 28.
[257] Id.

and internet logs)[258]. In smart cities, the most relied upon data source probably comes from smartphones. Sensors can be infused in the infrastructure and subtly collect phones' and other devices' MAC addresses. Citizens and tourists can be asked to log in and provide their credentials to public Wi-Fi networks. Subsequently, big data analysis of mobile datasets can easily reveal individuals' workplaces and residence locations, as well as a complete user profile (e.g., membership to poor or high-end communities, working hours, education levels, etc.).

Against this backdrop, the Working Party warned that the full development of IoT capabilities could curb the possibilities of maintaining users' anonymity[259]. Similar conclusions had been drawn previously on the use of RFID technology[260]. The Working Party noted that wearables kept close to data subjects could reveal a whole range of identifiers (e.g., MAC addresses) which could be used to track their location[261]. Taking this into consideration, it would be advisable to extend data protection safeguards to data generated by IoT devices in smart cities.

2) Biometric identification and classification systems. Diverse types of technologies fall under the umbrella of biometric classification and identification systems. The personal nature of the data processed by biometric identification systems is not under question. Specifically, biometric data follows the more protective regime laid down at Art. 9 GDPR and Art. 10 LED[262].

However, the case of biometric *classification* systems, which infer human-defined characteristics from one's biometric features, is different. AI tools trained to assess people's gender or age, as well as emotional states, fall within this category. Recently, *face detection* technologies have been one of the most discussed topics in data protection. These have often been integrated in smart billboards (or digital signages) to select targeted adverts to, and/or gather analytics of, passers-by based on their appearance, gestures or other behaviour (such as length of time spent looking at the billboard)[263].

Since these systems do not directly perform face identification analysis, but rely on face detection only, their developers often claim not to process personal data[264]. In literature too, opposing views have been upheld on the matter[265]. National data protection authorities have also adopted contrasting opinions. For example, the Italian[266] and Dutch[267] data protection authorities have taken positions in favour of applicability of the GDPR to smart billboards (although much discussion was devoted to how identifiability was established), while the Irish data protection authority has shown an opposite stance on the issue[268].

The main argument supporting the thesis of non-applicability of the GDPR is the "ephemeral" or "transient" nature of the data involved, that would not allow the individual to be re-identified in the future[269]. This view builds on a narrow notion of identifiability, which considers data protection to be applicable only where the unique civil identity of the individual can be established in the real world[270].

---

258 Id.
259 Article 29 WP (2014a), p. 8.
260 Article 29 WP (2005)
261 Article 29 WP (2014a), p. 8.
262 See Chapter V, §2.2.
263 See Yalcinkaya (2017).
264 See Quividi (https://quividi.com/%20privacy/) and Landsec (https://landsec.com/policies/privacy-policy/visitors); Earls Davis (2020), p. 366.
265 As reported in Earl Davis (2020).
266 Garante per la protezione dei dati personali (2017).
267 Autoriteit Persoongegevens (2019).
268 Data Guidance (2017) (original statement now deleted).
269 Earl Davis (2020), pp. 368, 371.
270 Id., pp. 372 ff.

Nonetheless, this approach is problematic under different profiles. Opinions and case law on the concept of personal data refers to a broad list of identifiers other than people's names, also covering online identifiers relating to the physical, physiological, genetic, mental, economic, cultural or social identity of a person. This approach has been implicitly integrated in Recital 26 GDPR, which again refers to "singling out" as a standard for identification. Secondly, no references seem to be found in the Regulation as for the *time* in which the individual should be targeted or identified for his or her data to be considered personal. Neither the Working Party seems to hint at such kind of parameter. And indeed, not all kinds of identifiability are designed to track the individual over time. In this regard, Leenes clarifies that only L- and especially R-identifiers embody a temporal dimension, as they recognise controllers to be individuals that return to their websites; on the contrary, S- and C-identifiers serve their goal in the session in which they are created[271].

Taking this into consideration, whether the smart billboard can actually uncover the civil identity of the pedestrian and target him or her in the future, does not seem to be relevant. Contrariwise, the key to establish identifiability is whether the passer-by has been impacted at all by the processing, even if this has lasted only a few (fractions of) seconds[272]. If a broad conception of the "relating to" criterion is adopted[273], smart billboards should process personal data relating to individuals at least in *purpose* or *effect*. For instance, if a passer-by is shown a high-end cosmetic advert just because she is targeted as a white-collar woman based on her gender, age group and appearance, the personal nature of the data processed by the machine should not be questioned. Our face and appearance, even if not connected to our names, can actually be useful to the biometric recognition software in order to serve people tailored advertising even in the lifespan of a few seconds spent before the smart billboard. It does not matter whether this assessment can be traced back to us in the future, as long as the controller has reached its nudging goal within that brief session.

3) Criminal surveillance. The processing of personal data in the Area of Freedom, Security and Justice is regulated by the LED, which adopts the same notion of personal data as the GDPR (Art. 3(1) LED). Therefore, the same concept of personal data applies in this context as well. Among the criteria to assess the personal nature of processed data listed by the Working Party, some acquire significant weight in this domain: the intended explicit or implied purpose of the processing; the advantages expected by the controller in case of identification; the interests at stake for individuals.

For their very nature, it is safe to argue that law enforcement activities tend towards the identification of individuals involved in illicit enterprises. In criminal investigations, identification is a logical pre-condition for prosecuting the offences. Lately, however, traditional investigatory measures are being coupled with strategies that do not directly rely on individuals' identification. Especially in the preventive sphere, local police departments use AI to achieve a more rational use of resources, rather than identifying potential suspects or dangerous people (e.g., crime mapping software). Certainly, this type of predictive policing may impact on the *communities* residing in the areas flagged by the software, but it cannot be said that they directly *impact* on individuals, nor it is their *purpose* to do so. Hence, the personal nature of the data processed by these algorithms is questionable[274], and at the same time highlights the shortcomings of an individual-based conception of data protection law.

---

271 Leenes (2007), p. 153.

272 Garante per la protezione dei dati personali (2017) (considering that the processing involves personal data regardless of the length of the processing).

273 See above §2.4.1.

274 *Contra* Linskey (2019), pp. 171 ff.

AI tools that do not directly target individuals also include video-cameras equipped with a face-blurring function. For instance, the *City-Pulse* project in Eindhoven involved the installation of cameras that do not record faces but can detect suspicious walking patterns (e.g., somebody walking up and down the street various times at a slow place) [275]. Such data is cross-referenced with different data sources (e.g., sound and weather sensors, sentiment analysis, etc.) to better anticipate and react to potentially escalating situations. If the system spots any anomalies in data patterns, an alert is sent to the regional police control room so that officers can decide whether additional patrolling is needed.

Do these face-blurred video streams process personal data? If faces are not immediately available for identification, the answer could be negative. Nonetheless, not all the doubts about the personal nature of the data processed can be dismissed. People could be re-identified if auxiliary information or means of processing were available. While the police in Stratumseind do not have access to high-dimensional datasets for easy re-identification, they certainly avail of other data sources that could do the job. Among these, Wi-Fi, Vodafone subscription data and social media feeds[276]. Not to mention the technical possibility of removing the blur from faces.

Most importantly, what plays a major role here is the underlying goal of law enforcement, which arguably needs identified subjects to fulfil its mission. In this perspective, it would not be unlikely for local police departments to decide to re-identify individuals in video-streams, if labelled as suspicious for their walking or caught on camera carrying out illicit activities (e.g., fights, aggressions, drug exchange). Arguably, this may suggest a positive answer as to whether face-blur video streams used by the police involves personal data processing.

4) Environmental data. Lastly, a great part of IoT data in smart cities stems from sensors measuring different environmental parameters (e.g., sound, lightning, temperature, pollution levels, wind speed, humidity, weather)[277]. Counterintuitively, the personal nature of the data collected by these sensors could be debated.

To suggest possible answers, a case-by-case analysis focusing on the *provenance* of the data and/or the *purpose* of the processing could be adopted. As far as the provenance of data is concerned, it should be considered whether smart city IoT data is collected by fixed or mobile sensors[278]. Indeed, while the former are installed in the urban infrastructure, the latter are embedded in the IoT devices of citizens participating in crowdsourcing initiatives[279]. If the data is not linked to any personal device or identifier, potentially revealing their owners' location, its personal nature could be excluded. That would be the case of data collected by environmental sensors embedded in the urban infrastructure. On the contrary, if environmental data is tied to any identifier (e.g., MAC or IP address of a personal IoT device), its personal nature could be presumed if they have not been properly anonymised. Indeed, this data could show the environmental conditions in which the owner of the device lives, possibly revealing her health or economic conditions.

Different and rather new are the instances where environmental data is integrated in security-related activities. For example, certain weather conditions or lighting levels are increasingly infused in predictive analyses on how criminal activities are likely to occur in certain areas or timeframes. Sometimes, environmental data on sound pollution levels is also collected and stored with the specific

[275] Cf. Galič et al (2021), p. 5.
[276] Id., p. 9.
[277] See Poon (2021).
[278] Jin et al (2014), p. 115.
[279] See the Smart Citizen Kit initiative. https://www.seeedstudio.com/Smart-Citizen-Kit-p-2864.html. Accessed 13 December 2021.

purpose of identifying and sanctioning individuals[280]. In this latter case, applying the identifiability test appears to be more straightforward. Considering that sensor data is specifically processed with the goal of discerning who is violating noise pollution regulations, the personal nature of this data seems easier to establish.

5) Atmospheric profiling: Going beyond strict identifiability? Lastly, it should be considered that ambient intelligence environments are pushing scholars to come up with new ways to conceive identifiability in smart cities. In the case of Stratumseind, it has been argued that "persons are not to be affected as specific individuals or even algorithmic groups, but only as part of the general atmosphere on the street"[281]. In this sense, the operations implemented in the area have been labelled as a new kind of profiling called "atmosphere profiling":

> The SLL is therefore based on the detection of a positive or negative atmosphere, with the intention of directly affecting this atmosphere – rather than any particular individuals – so as to reduce aggression and violence. In other words, the SLL is based on the creation of profiles of atmospheres – *atmospheric profiles* – which are then translated into "everything alright" or "high risk" profiles within the *City-Pulse* project. Atmosphere can thus be described as a proxy to only indirectly affect and nudge people, who are reduced to a constitutive element of the atmosphere on the Stratumseind street[282].

Arguably, this creates further problems in conceptualising identifiability and personal data. Whereas the primary goal of these smart city initiatives is to affect the atmosphere, its indirect one remains nudging people towards certain behaviours. To do so, however, no individual needs to be identified: in the *De-escalate* project, for instance, the emotional status of people in Stratumseind is (presumably) moulded with an adaptive lighting system; individuals are not targeted as such, but only insofar as they form part of the bundle of moods, interactions and behaviours predominating in the street. As claimed by the involved actors, therefore, these data processing operations would fall outside the scope of data protection.

Nonetheless, the distinction between processing targeted individuals, and those that are not, is not always a neat one in environments like the Stratumseind[283]. As indicated above indeed[284], the processing of environmental data may at times impact on individuals. Also, blurred-video images may easily lead to the re-identification of individuals if they have caught the attention of law enforcement.

Overall, identification risks and the applicability of data protection seem difficult to discern in projects like the Stratumseind, which pursue multiple goals at the same time (e.g., security, environmental monitoring). In the end, much seems to depend on the concrete objectives of the surveillance put in place, which may be established only on a case-by-case basis even within the same smart city initiative.

2.4.2.3. Reasoned approaches to the scope of data protection

The dangers of an over-stretched notion of personal data. In general terms, this analysis highlighted that the scope of application of data protection in smart cities is potentially very wide. Opposing interpretations of the scope of data protection rules in intelligent environments respectively support or discourage an image of the GDPR that, according to some, is rapidly becoming "the law of everything"[285].

---

[280] See Poon (2021).
[281] Galič et al (2021), p. 11.
[282] Id.
[283] Id., pp. 11-12.
[284] See §2.4.2.
[285] See Purtova (2018a).

Importantly, an over-stretched notion of personal data is seen with fearful eyes by technology actors in terms of compliance obligations[286].

To the rescue of, or possibly to aggravate this situation, different proposals have been put forward as a remedy to the overly broad notion of personal data and identifiability. Some have proposed to abandon the concept altogether[287]. If the concept of personal data excludes safeguards for group or atmospheric profiling, it is advocated that a shift to "data protection *tout court*" could improve the level of protection[288].

From the American perspective, others see the concept of personally identifiable information as particularly problematic in a world dominated by information overflows[289]. With ubiquitous data processing, regulation boundaries are definitely needed[290]. Drawing inspiration from the European definition of personal data (which foresees both *identified* and *identifiable* information), Schwartz and Solove undertook a risk-based approach to scope data protection rules[291]. It was proposed to overcome rigid mechanisms, according to which the question of whether data protection law applies does not require unequivocal "yes or no" answers. Rather, legal protection should be conceptualised as a continuum revolving around increasing identifiability risks for individuals[292].

This spectrum would be articulated as follows: (i) identified; (ii) identifiable; (iii) non-identifiable person. Stronger safeguards would be required for personal information identifying individuals, moving to softer compliance obligations as the risks of identification diminish[293]. The domain of identifiable information comprises different risk-levels, from low to moderate. When the danger of re-identification is high, even identifiable information should be treated in the same way as information directly identifying individuals[294]. Notably, this option is also supported by European scholars aiming to keep a broad interpretation of personal data, while also diminishing the intensity of compliance GDPR obligations[295].

Rather than imagining alternative regulatory scenarios, European scholarship has also tried to leverage the existing legislation to achieve a more reasoned interpretation of the notion of personal data[296]. One first way to curb the expansion of personal data protection could be enhancing the interaction between the relational link ("*relating to*") and the identifiability test. It is contended that when data does not relate in *content* to an identified or identifiable individual, but just in *purpose* or *effect*, additional information will always be needed to satisfy the identifiability requirement[297]. Therefore, identifiability standards should logically be higher in these latter instances.

A more dynamic, rather than static, interpretation of the concept of personal data should also be emphasised. Indeed, data protection law "does not apply to personal data in a vacuum, but to its *processing*"[298]. Data has a lifecycle, and it is not necessarily personal throughout its entire lifespan[299]. For example, L-identifiers such as passport number relates to individuals in content for their entire lifecycle.

---

286 Id., pp. 75 ff.
287 De Hert et al (2008), p. 289. cf. Purtova (2018a), p. 80.
288 Id.;
289 Schwartz et al (2011), p. 1866.
290 Id.
291 Id., p. 1877.
292 Id.
293 Id.
294 Id., p. 1878.
295 Purtova (2018a), p. 79.
296 Dalla Corte (2019), pp. 9 ff.
297 Id., p. 10.
298 Id., p. 9.
299 Id., p. 11.

However, this is not the case for data relating to individuals in purpose or effect: these acquire a personal nature only in the phases in which they are processed to have an impact on individuals[300]. Lastly, the test of reasonable likelihood of identification should be interpreted in relation to the specific context and environment in which the processing occurs, rather than to the mere hypothetical technical possibility of identifying a person[301].

Speculating about regulatory scenarios in smart cities. Arguably, some kind of perimeter should be kept in order to circumscribe the scope of data protection rules. Giving up the notion of personal data and accepting that all data is personal may not be viable option, from both a practical and legal perspective. On the one hand, in fact, high-intensity compliance obligations could significantly curb technological innovation, while on the other, a different conceptualisation of data protection may be obstructed by its framing as individual right in EU primary law. Differently, the risks of processing impacting on groups could be addressed in different legislative instruments[302].

If the aim is to keep such boundaries, alternative approaches should be devised to counter the overly engulfing notion of personal data. Taking advantage of available provisions and interpretative tools can definitely be of help, as underlined above[303]. Nonetheless, enhancing a dynamic conceptualisation of personal data, excluding the application of relevant safeguards to bespoke phases of data lifecycle may not always be practicable. Indeed, *ex-ante* data protection obligations laid down by the GDPR may stand in the way of such an approach, imposing compliance obligations even where the risk of data becoming personal is foreseeable only for transitory phases. In practice, this means that controllers could be burdened with data protection obligations (e.g., performing a DPIA) even where the risk of data being personal is, from the outset, foreseen only for transitory processing operations. Sometimes, they could be bound to perform a DPIA just to exclude that any personal data is processed.

From a speculative perspective, a systematic interpretation of the GDPR highlights that the risk-based approach could provide for greater flexibility in the *intensity* of the obligations imposed on the controllers when data protection applies. This could lead to a diversified compliance regime, moulded according to the risk of re-identification. The layered regime distinguishing identified, identifiable and non-identifiable (i.e., anonymous) information described above, can be regarded as a useful representation of such regulatory regime.

Concrete examples in smart cities. In such a framework, the processing of weather data in Stratumseind would likely lead to very low risks for data subjects, insofar as they are not used to profile the general atmosphere in the neighbourhood. The processing of such data could then be associated with very few compliance obligations. Different might be the case of sound sensors which, even though not allowing a direct identification of the individual, can be combined with other data sources, such as Wi-Fi tracking and unmasked video-surveillance, to secure identification.

Of course, these arguments bear a highly speculative character, as definitive solutions can be put forward only with a contextual and technically informed analysis. Overtaking the claims of private and public actors about data processing in smart cities may often be necessary to discern if we are dealing with personal data at all, and if their collection is lawful.

---

[300] Id.
[301] Id, pp. 13-14.
[302] See e.g., the analysis made of the DGA, DA and AIA in Chapter VI.
[303] Cf. Dalla Corte (2019).

3. Grounds for data collection in public smart city environments

3.1. Issues with consent

Consent in the GDPR. Consent is identified as legal grounds for personal data processing in Art. 6(1)(a) of the Regulation. In addition, Art. 7 specifies the conditions under which consent is considered valid. Art. 4(11) GDPR, instead, provides for a definition of consent in EU data protection law:

> 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The building blocks of the notion of consent (freely given, specific and informed) are rooted in the legal history of the DPD[304]. The Working Party highlighted that consent requires an "*indication*" of the data subject's wishes. No further guidance was or is still provided on the form that such indication should take, leaving a wide margin of discretion to controllers on how to collect consent (e.g., written, orally, by ticking boxes, via *facta concludentia*)[305].

Firstly, to be valid, consent must be freely given, meaning that the data subject has been put in a position to exercise a real choice, with no danger of deception, threat, coercion of negative consequences if consent is rejected[306]. That is why the GDPR bars controllers from relying on consent as grounds of lawfulness in various situations (e.g., employer-employee relations)[307]. Recital 43 also specifies that "[c]onsent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case".

Secondly, consent must also be specific, which presupposes that the exact scope, purpose and consequences of the processing were communicated clearly and intelligibly[308]. Thirdly, consent must be informed: data subjects should be able to appreciate and understand the implications of agreeing to the processing of their personal data[309]. Logical precondition of such awareness is the compliance, by the controllers, of their information obligation under the Regulation. Lastly, consent must also be "unambiguous", i.e., there should be no doubts as to the data subject's intention of providing consent[310].

Difficult application in (public) smart city scenarios. Even before the advent of smart environments, much criticism had been directed at consent as lawful grounds for personal data processing. The "mythology of consent" was even identified as one of the main problems of data protection law[311]. In online contexts specifically, consent was not seen as a viable legal basis for processing. Inconvenience often discourages people from spending time reading overly long and obscure privacy policies[312]. A paradoxical trade-off between *practical* and *meaningful* consent was thus detected: the easier the consent procedure is made, the less informed data subjects' consent would be; on the contrary, the more thorough the consent procedure, the less practical it would be for controllers to obtain consent[313].

---

304 Article 29 WP (2011), p. 6. On consent in the GDPR, see Kotschy (2020), pp. 329-330; Kosta (2020a).
305 Article 29 WP (2011), pp. 11-12.
306 Id., p. 12.
307 Id., p. 13. Cf. Recital 43 GDPR.
308 Id., p. 17.
309 Id., p. 19.
310 Article 29 WP (2011), p. 21.
311 Koops BJ (2014a), p. 251; Moerel et al C (2016), pp. 8-9.
312 Koops BJ (2014a), p. 252.
313 Id.

Arguably, these issues have only been magnified in hybrid online-offline environments. Considering that the IoT is designed to be unobtrusive, it is extremely difficult for individuals to deliver specific, informed and unambiguous consent. For starters, data subjects may not always be aware that data processing is occurring at all, especially in public spaces. Moreover, even when they know about the processing, hectic urban lifestyle may not allow citizens to take the time to read and understand complex privacy policies underlying these operations *beforehand*. For instance, it was suggested that providers of smart city services may equip lampposts and trams with QR codes redirecting data subjects to privacy policies or information campaigns. However, it is dubious whether individuals would dedicate time to read them while rushing to work or to buy groceries[314].

The "freely given" requirement for consent is also rather problematic in the smart city context, because the public dimension of the data processing often compromises individuals' chances to deliver consent free of any external pressure. Also, systematic and indiscriminate monitoring of people in public is rarely compatible with consent[315]. Pervasive data collection in public areas may even affect people's free choice of enjoying these spaces and related services.

As *consumers*, individuals may rationally agree to the processing of their personal data in exchange for additional commercial services or advantages, although this assumption might be challenged[316]. In cities, however, people are first and foremost *citizens*, and their access to public spaces and services should not be made conditional upon the processing of their personal data[317]. As a matter of fact, the only way to bypass data collection would be avoiding certain areas, or taking alternative paths, which sounds unreasonable and unrealistic[318]. In addition, as indicated by Recital 43 GDPR, the fact that public authorities would act as controllers in several smart city projects would probably exclude consent as a viable legal basis. The same would be true if individuals were not able to express separate consent for multiple data processing operations.

Restricted applications in smart cities. In limited cases, some contextual factors would justify resorting to consent as lawful grounds in smart city processing[319]. Firstly, that would be the case of grass-root or crowdsourcing initiatives, where citizens decide to voluntarily share their data for the common good of the city. Secondly, consent would seem to be an appropriate legal ground in smart city pilot initiatives, where individuals can freely decide whether to contribute to the early development of a project[320].

In this regard, an IoT application implemented in a Dutch museum is brought forth as example[321]. The idea was to track visitors to understand how they interact with exhibited items. It was decided that visitors would participate only on a voluntary basis, and technologies that would not allow such consensual tracking were excluded (e.g., Wi-Fi, emotion facial recognition, EFR)[322]. Conversely, wearables were picked as the only suitable option to rely on consent as a legal basis, as they presuppose users' choice of wearing one[323].

---

314 Christofi (2021), p. 27.
315 Cf. EDPB (2019), p. 14.
316 See Chapter VI, §3.2.3.5.
317 Christofi (2021), p. 26; on the problematic relation between the labels of "citizens" and "consumers" in smart cities, see Ranchordás (2018).
318 Kitchin (2016a), p. 9.
319 Cf. Christofi (2021), p. 27.
320 Id.
321 Breuer et al (2019), p. 3.
322 Id.
323 Id.

Alternative legal bases. Therefore, consent appears to be a viable legal basis only in very limited smart city initiatives that rely on the voluntary participation of citizens. That is why it would make more sense to turn to other GDPR non-consensual legal bases in this context. Specifically, the public interest and legitimate interest lawful grounds seem the most apt to regulate big data processing in urban environments.

3.2. Public interest

3.2.1. Relevant provisions and interpretation

In the GDPR. The public interest ground is of the utmost importance in smart city initiatives, due to the pivotal role of public authorities. In the GDPR, it is laid down at Art. 6(1)(e):

> "Processing shall be lawful only if and to the extent that at least one of the following applies: (…) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

Art. 6(3) then adds:

> The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
>
> (a) Union law; or
>
> (b) Member State law to which the controller is subject.
>
> The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Subjective scope of application: private bodies and public tasks. Even if the public task basis is most relevant for public authorities, this does not prevent private actors from processing data under Art. 6(1)(e) GDPR. However, the English wording of Art 6(1)(e) GDPR is quite ambiguous on this matter. It is not clear whether the expression "vested in the controller" refers to the "exercise of a public authority" or to "a task"[324]. The meaning of the provision is actually clearer in the German version, which translates as: "Processing is necessary for the performance of a task, carried out in the public interest *or* in the exercise of official authority, vested in the controller"[325].

In this regard, scholars have contended that the task pursued through the processing should always be entrusted beforehand to the controller by a legal provision. This stricter interpretation would exclude from the scope of Art 6(1)(e) cases where the public tasks have been assigned to the (private sector) controller by contract[326]. This position would be corroborated by a systematic interpretation of Art 6, whose par. 3 underlines the need for an additional legal basis regulating all the conditions of the processing in the public interest, including "the general conditions governing the lawfulness of processing by the controller".

---

[324] Kotschy (2020), p. 335.
[325] Id. [emphasis added].
[326] Id. In this case, the most appropriate legal basis would be Art 6(1)(b) GDPR.

Nonetheless, others doubt that private bodies always need to be entrusted with an official authority to rely on Art 6(1)(e). Indeed, the provision employs the conjunction "*or*", rather than "*and*", meaning that the two conditions are alternative and not cumulative. Therefore, public authorities should be responsible for deciding whether to bestow an official authority upon the private provider by legislative provision, or by contract[327].

Private actors in the smart city can often find themselves in the position of processing data while managing public services on behalf of public authorities. These PPPs can give rise to different interplays, which may stem from contractual agreements only, without a broader legal framework[328]. This state of things does not appear to contradict a literal wording of Art.(1)(e). While a prior legal basis should always ground the public task, the attribution of an official authority to a bespoke private body should not be seen as a mandatory criterion under this provision.

The notion of public interest. An integrated reading of the relevant (para)constitutional provisions in EU law suggests that the notion of public interest should be interpreted broadly. First of all, the notion of public interest is recalled in both the CFREU and the ECHR as legitimate grounds for circumscribing the right to the protection of personal data. Still, a fundamental difference persists. While Art. 8(2) ECHR includes a closed (but broadly formulated) list of public interest goals that may ground limitations on the right at stake[329], Art. 52(1) CFREU only refers to "objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others". This leaves a wider margin of discretion to the interpreter in identifying possible public interest aims legitimising encroachments upon fundamental rights. Indeed, this requirement is examined by the CJEU on a case-by-case basis[330]. Specifically, the Court can take into consideration several objectives that EU Treaties consider worthy of protection, from security, to safeguarding the environment, as well as the economic, social and territorial cohesion. Even an (elusive) objective of promoting "good governance" could be invoked as a public interest to process personal data[331]. Moreover, Recital 46 of the GDPR lists some important grounds of public interest aimed at safeguarding vital interests of data subjects, like humanitarian actions or monitoring situations of natural and human-made disasters. Importantly, after the outbreak of the Covid-19 pandemic, the need to monitor epidemics and their spread is also identified as a possible instance of public interest legal basis.

The need for an additional legal basis. Art. 6(3) GDPR explicitly foresees the need for an additional legal basis grounding a public interest processing[332]. This is a novelty of the GDPR, as the Directive 95/46/EC did not comprise a similar provision. This clarification is a direct expression of the constitutional principles of legality and the rule of law governing the activities of the Public Administration, including at the informational level[333]. For the actions of the government to be restrained within predictable boundaries, the law must clearly define the scope of the powers of the

---

327 Id, p. 336.

328 Reynaers (2014), pp. 41-42.

329 These are: national security, public safety or the economic well-being of the country, the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

330 See CJEU, *Digital Rights Ireland*, §42. See also CJEU, *Heinz Huber v Bundesrepublik Deutschland*, judgment of 16 December 2008, Case C-524/06, §59 (referring to the application of legislation on the right to residence); CJEU, *Scarlet Extended*, §§31, 36 (referring to the fight against violations of intellectual property rights).

331 Kotschy (2020), p. 336.

332 Other instances where an extra-GDPR provision is needed for the processing to be lawful are Arts. 9(2)(g) and 23.

333 Principles derived from legal logic and the needs of material justice such as legality, the rule of law, legal clarity, legitimate expectations, effective judicial protections are general principles of EU law. See Kostoris (2018), p. 24.

State *vis-à-vis* individual citizens. This allows for greater transparency and democratic oversight of public administration activities.

Furthermore, Art 6(2) GDPR opens up to the possibility for Member States to introduce provisions at the national level to further detail the conditions of lawfulness for processing operations under the grounds of a legal obligation or public interest. The rationale behind this provision can easily be understood. In the field of the public sector – where it is reasonable that Member States are more "jealous" of their own legal traditions – the EU legislator decided to compromise between the desire to strengthen data protection harmonisation and the needs of Member States to preserve more specific rules in a domain that is more sensitive to how sovereign power is exercised. In any case, this is only optional for Member States, while the requirement for an extra-GDPR legal basis under Art. 6(3) is considered mandatory for processing under the public task legal basis.

3.2.3. The quality of the law requirement

The quality of the law requirement in the Convention and the Charter. Whenever the Regulation refers to an additional legal basis to legitimise the processing, we should deal with the question of *what kind of law* this should be. In line with the case law of the ECtHR and the CJEU, Recital 41 provides an answer by recalling the so-called "quality of the law" doctrine[334]:

> Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise, and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the "Court of Justice") and the European Court of Human Rights.

The ECtHR built the quality of the law doctrine in relation to Art. 8(2) of the Convention, which requires that any interference with the right to private life is "according to the law". The Court has developed an autonomous concept of the "law", opting for an anti-formalistic approach – which is also supported by the rather flexible wording of Art. 8(2)[335]. Legal measures that limit fundamental rights should not necessarily be the outcome of decision-making processes of Parliament, or of any other body holding legislative power. It suffices that the limitation is authorised by a rule acknowledged in the national legal order. This comprises both "written law", including different kinds of delegated legislation adopted by the government, and "unwritten law" as interpreted and applied consistently by the judges. This a-technical stance is justified by the need to include different types of legal traditions (i.e., both civil and common law systems) in the ECHR system.

Nonetheless, some caveats apply. The "law" in question must in fact abide by some quality requirements: accessibility and foreseeability[336]. It must be accessible to the individual and its consequences should be predictable. For instance, when case law serves as a basis to limit fundamental rights, the Court demands the jurisprudence at issue to be sufficiently solid and consistent, so as to allow individuals to easily predict the consequences of their actions. Also, the criterion of accessibility is not satisfied only if the measure was published on the Official Journal of the responding States. In *Zakharov*, the Court examined the question of accessibility of a regime of secret interceptions in

334 See Schabas (2017), pp. 402 ff; De Hert (2005), pp. 73 ff.; De Hert et al (2020), p. 8.
335 Schabas (2017), p. 402.
336 See, e.g.,ECtHR, *Roman Zakharov v Russia*, judgment of 4 December 2015, Appl. No.47143/06, §228; ECtHR, *Rotaru v. Romania*, judgment of 4 May 2000, App. no. 28341/95, §52, ECtHR, *S. and Marper v the United Kingdom*, judgment of 4 December 2008, App. nos. 30562/04 and 30566/04, §95; ECtHR, *Kennedy v. United Kingdom*, judgment of 18 May 2010, App. no 26839/05, §151.

Russia[337]. While most legal provisions had been published in the Official Journal, some addendums of a technical nature only appeared in a ministerial specialised journal, available in an online free database. Considering that this document was published in an official source and was fairly accessible to the public, the Court considered the law to be sufficiently accessible[338].

In the context of the Charter, however, a stricter approach might apply. It has been deemed that certain restrictions upon fundamental rights can be established by means of legislation only[339]. The CJEU implicitly looked at this issue in the *Bara* judgment. Under the regime of the DPD, the Court considered whether a national measure could prevent an administrative body from transferring personal data to another public entity and preclude further processing[340]. First of all, the Court reiterated that such processing operations could not occur without informing data subjects beforehand[341]. In the case at stake, however, some of the data transfers did not find a basis in the law, but on a stipulated protocol between administrative authorities that was not subject to official publication[342].

Under these circumstances, the Court concluded that the conditions of Art. 13 DPD permitting restrictions of data protection rights were not met, as data subjects had not been properly informed of the foreseeable use of their data[343]. Critically, it was not clear from the wording of the Court whether the protocol was inapt for grounding the processing because it was not a legislative measure, or only because it had not been officially published. Therefore, some ambiguity in this sense persists in the EU system.

Foreseeability. The consequences of a legal provision are foreseeable insofar as the latter is detailed and precise in its wording. Nonetheless, a distinction can be drawn between legislative measures legitimising data processing on the basis of a legal obligation and a public task, respectively. On the one hand, the standard of detail in the first case is much higher, as the legal basis should in itself be apt for clearly circumscribing the scope of the legal obligation[344]. On the other, the level of foreseeability required for processing under a public task seems to be lower. In this regard, the UK Information Commissioner's Office (ICO) stated that a specific statutory power to process personal data is not required, but the underlying task, function or power must have a clear basis in the law[345]. Processing under Art. 6(1)(e) GDPR is thus underlined by a greater level of flexibility. It was even argued that the relevant legal basis may simply result in a "more general authorisation to act as necessary in order to fulfil the task"[346].

Foreseeability issues in smart cities: Does the ECtHR's case law on secret surveillance apply? How does this all apply in the smart city? It has been argued that such broad legal authorisations under Art. 6(1)(e) GDPR can pose challenges in this context[347]. With increasingly complex processing, legal bases that do not even specify the categories of the processed data may not satisfy high foreseeability standards[348]. For instance, general laws only stipulating public authorities' tasks may leave them with an excessive

337 See Chapter IV, §3.2.
338 ECtHR, *Zakharov v Russia*, §242.
339 Peers et al (2021), p. 1626.
340 CJEU, *Smaranda Bara and Others*, judgment of 1 October 2015, Case C-201/14, §28.
341 Id., §34.
342 Id., §40.
343 Id., §41.
344 Cf. CJEU, *Digital Rights Ireland*, §§59-68; Article 29 WP (2014b), p. 19.
345 ICO (2018), p. 75.
346 Kotschy (2020), p. 336.
347 Christofi (2021), p. 49.
348 Id.

margin of appreciation in the choice of the data to be collected and the means to process it. This approach appears to be at odds with the standards of protection demanded by the Working Party, which specified that in the event of *extensive* privacy invasions, "the legal basis should be specific and precise enough in framing the kind of data processing that may be allowed"[349]. In this perspective, it has been submitted that a "municipality acting on its own is hardly an appropriate legal measure to ground public interest smart city processing, that deploys for instance the use of cameras and other sensors capturing personal data from public spaces"[350]. Recognising these dangers, some Member States (e.g., Belgium) have introduced special laws governing more sensitive processing operations, like the use of cameras by municipalities[351].

Scholars have also relied on the ECtHR's case law on secret surveillance to further argue in this sense. In *Huvig* for instance, the Court established a set of criteria to assess the foreseeability of secret surveillance laws: a definition of the category of persons whose communication may be surveilled or processed; limitations in time for the periods of the surveillance measure; a procedure for the use and storage or retention of the data (use of summary reports); precautions when the data is communicated to others; and the circumstances when the data must be deleted or destroyed[352]. These criteria are still valid to this day[353], and they have also been integrated in the case law of the CJEU since *Digital Rights Ireland*[354]. Nonetheless, Strasbourg judges also seem to apply these criteria in a diversified manner, demanding lower standards of protection in cases of less serious interferences with the right to private life[355]. In *Uzun*[356], for instance, only the grounds for ordering surveillance and the nature, scope and duration of those measures were required, while the Court remained silent on the conditions for storage and transmission of collected data.

The direct applicability of this case law may be questioned, as far as public task processing in smart cities is concerned. While the ECtHR has in time extended the scope of its argumentations across decisions, we should be careful not to excessively generalise the validity of its considerations in different settings[357]. At a closer look, it appears that the Court's arguments may rather regard, or be more pertinent to, hypotheses of data collection, disclosure or transfer based on a legal obligation (e.g., data transfers from the private sector to the police), or on a law enforcement basis (Art. 1(1) LED). It also concerns a field fraught with potential sensitive consequences for data subjects (e.g., covert surveillance measures).

On the contrary, the field of public task processing arguably features a higher degree of flexibility, which may result in more diluted standards of foreseeability. Certainly, these may vary according to the level of invasiveness of the processing. As underlined by the ICO, a law framing the general boundaries of the missions pursued by public authorities is certainly needed. Nonetheless, it could be wondered whether the mere definition of governmental tasks is enough for citizens to anticipate the reach of the data processing operations that may interest them in the city. To satisfy the foreseeability requirements under Art. 6(1)(e), the extra-GDPR legal basis should *at least* combine provision of the public task with

[349] Article 29 WP (2014b), p. 22.
[350] Christofi (2021), p. 50.
[351] Id.
[352] See Chapter IV, §3.2.
[353] See ECtHR, *Huvig v. France*, judgment of 24 April 1990, App. no. 11105/84, §34; ECtHR, *Weber and Saravia v. Germany*, judgment of 29 June 2006, App. no. 54934/00, §95.
[354] CJEU, *Digital Rights Ireland*, §§58-62.
[355] De Hert et al (2020), p. 9.
[356] ECtHR, *Uzun v. Germany*, judgment of 2 September 2010, App no 35623/05.
[357] Kostoris (2018), p. 47.

a general authorisation to process personal data for that purpose. Instead, higher standards of foreseeability should be satisfied in the case of high privacy-invasive operations (e.g., CCTV, facial recognition), or when the processing is grounded on a statutory obligation (see below).

3.2.4. Public task processing vs. processing under a legal obligation

Balancing in public task processing – ambiguities with a legal obligation basis. Legal obligation and public task grounds for processing may coexist in many instances of smart city processing[358]. Nonetheless, the same standards of foreseeability may not to apply to the legal bases.

At the outset, not all scholars agree on the nature of the balancing act enshrined in the public task legal basis. For instance, Gellert distinguishes two fundamental balancing tests in the GDPR: an implicit and an explicit one[359]. On the one hand, implicit balancing occurs when this is done *ex ante* the processing and is embedded in the (additional) legal basis. That would be the case of processing based on a legal obligation (Art. 6(1)(c) GDPR), public interest (Art. 6(1)(e) GDPR) and consent (Art. 6(1)(a) GDPR, where the consent is the result of a balancing made by the data subject prior to the processing). On the other, an instance of explicit balancing is the grounds of legitimate interest (Art. 6(1)(f) GDPR), where the controller carries out the relevant proportionality assessment only at the moment of proceeding with the processing.

In this reconstruction, the public task basis would be very similar to, if not coincident with, processing under a legal obligation. Nonetheless, it would be more useful and coherent with the overall GDPR structure to label public task processing as instances of *explicit* processing, as per the legitimate interest basis. A threefold reason supports this argument. Firstly, this approach would avoid any overlapping between Arts. 6(1)(c) and 6(1)(e) GDPR, distinguishing their rationale and mode of application. Indeed, a systematic interpretation of the Regulation suggest that requiring the same standards of precision for extra-GDPR legal bases under Arts. 6(1)(c) and 6(1)(e) would simply result in a substantial duplication of these two grounds for lawful processing. If the EU legislator decided to separate these grounds in Art. 6(1), this means that they should be interpreted in such a way as to avoid their complete overlap.

Secondly, Art. 6(3) GDPR does not require a mandatory specification of all the elements of the processing. The legal basis must indicate the purpose of the processing as a minimum, but *may* also include other specifications, such as "the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; and the purpose limitation".

This margin of freedom left to the controller opens up to the possibility that such elements may not be established beforehand in the additional legal basis, allowing the controller to make a balanced decision at the moment of initiating the public task processing. Inversely, when processing is based on a legal obligation, the balancing act should have already been performed by the legislator at the moment of adopting the legal basis. Higher "quality of the law" standards would thus apply.

This means that, in terms of foreseeability, the public task ground seems to stand in a "middle-way" between the legal obligation and the legitimate interest bases: on the one hand, public task processing shares a similar mode of application with legitimate interest, based on explicit balancing by the controller; on the other, it also requires an additional legislative basis defining the purpose of the processing as per the legal obligation ground. In other words, Art. 6(1)(e) is at the same time both *less*

[358] Article 29 WP (2014b), p. 21.
[359] See Gellert (2016).

flexible than Art. 6(1)(f) because of its underlying general interest basis (defined by the law), and *more* flexible than Art. 6(1)(c) in terms of the foreseeability standards attached to the extra-GDPR legal basis.

Also, this approach entails that the balancing operation may be performed by the controller in different moments, according to the chosen GDPR basis. In the case of Art. 6(1)(c), the balancing between competing interests occurs at the genesis of the extra-GDPR legal basis, where the legislator defines the exact scope of the data processing measures. Art. 6(1)(e) instead is more similar to the legitimate interest basis (Art. 6(1)(f))[360]. The balancing act, also implying the choice of the categories of data to collect, should not necessarily be made beforehand and set in stone in a separate legal basis. It should rather be a contextual choice of the data controller to determine the amount of data and the means of processing strictly necessary to pursue that kind of public task.

Implications for smart cities. Arguably, this interpretation better support the needs of flexibility of urban authorities transitioning towards greater digitalisation. Certainly, people living in smart cities incur increasing privacy and data protection risks. At the same time, however, overly cautious approaches to privacy and data protection safeguards may curb the potential of AI and other data-driven technologies when these can bring valuable societal advancements in the urban sphere[361].

Nonetheless, caution should be applied even in this approach. Sometimes, one should consider the seriousness of the privacy invasion entailed by the operation. In these cases, it may be appropriate to ensure that the legal basis for public task processing complies with higher foreseeability requirements, going beyond the mere specification of the purpose of processing. In smart cities, for example, gathering data to improve the efficiency of mobility services is not the same as keeping security cameras in public streets or processing personal data for tax checks.

3.2.5. The necessity link

The necessity link in public task processing: the Huber judgment. Art. 6(1)(e) legitimises data processing only if and to the extent it "*is necessary"* for the performance of a task carried out in the public interest[362]. As for other non-consensual bases in the GDPR, the necessity link averts the risk of undue recourse to Art. 6(1)(e).

Considering the hierarchy of EU legal sources, this requirement could be interpreted in light of the proportionality test laid down in Art. 52(1) CFREU. However, this is not necessarily the case in data protection law. The EDPS has clarified that "necessity of processing operations in EU secondary law and necessity of the limitations on the exercise of fundamental rights refer to different concepts"[363].

Previously, the Working Party had indicated that Art. 7(1)(e) DPD (Art. 6(1)(e) GDPR, today) requires a direct and objective link between the processing and the purposes[364]. In the proportionality assessments conducted by the CJEU, this would substantially coincide with the suitability (or appropriateness) requirement, which demands that the infringing measure is abstractly suitable to reach the stated objectives[365].

Further guidance can also be found in the CJEU *Huber* judgment[366], adopted under the DPD regime. In this case, the Court scrutinised the lawfulness of a database created by the German authorities,

360 Kotschy (2020), p. 336. *Contra* Gellert (2016), p. 486.
361 Moerel et al (2016), p. 7; Marsch (2020), p. 42 ff.; Custers et al (2016), p. 5.
362 Art. 6(1)(f) GDPR [emphasis added].
363 EDPS (2017a), p. 4.
364 Article 29 WP (2014a), p. 15.
365 See Chapter IV, §3.1.2.2.
366 CJEU, *Huber*.

which included personal data on third country nationals and other EU citizens that did not hold German citizenship. Such a database, according to national law, was established to support national authorities responsible for the application of the legislation relating to the right of residence.

In *Huber,* the CJEU clarified that "necessity" in Art. 7(1)(e) of the Directive had an independent meaning in European Union law, preventing Member States from relying on their own interpretations[367]. Also, it had to be interpreted "in a manner which fully reflects the objective of that directive"[368]. In the case at stake, the Court found that the establishment of a centralised (rather than decentralised) database of non-German citizens could not satisfy the requirement of necessity under Art. 7(1)(e), unless: "[i] it contains only the data which are necessary for the application by those authorities of that legislation; [ii] its centralised nature enables that legislation to be more effectively applied as regards the right of residence of EU citizens who are not nationals of that Member State"[369].

In this reasoning, the Court seems to refer to the strict necessity test as enshrined in Article 52(1) CFREU. This requirement demands that a measure limiting fundamental rights cannot be justified unless no less intrusive means to achieve the goal are available[370]. On the contrary, operations that are simply "useful" for reaching the stated objectives do not comply with the strict necessity requirement[371]. In *Huber*, in fact, only strictly necessary data could be entered in the database; additionally, the register could be made centralised only if the objective improving the efficiency of the legislation could not be achieved otherwise.

Therefore, it can be argued that necessity as enshrined in Art. 6(1)(e) is partially (but not completely) convergent with the proportionality test pursuant to Art. 52(1) CFREU[372]. Indeed, controllers must perform a suitability and strict necessity test to initiate processing under all non-consensual bases in Art. 6(1) GDPR.

On the contrary, a proportionality *stricto sensu* may not be required at the collection stage. The controller should identify all the means of processing according to strict necessity standards, but a strict axiological reasoning on the impact of the processing may be overburdening. Strict proportionality assessments should be carried out only when limitations to the core principles of the right to data protection are interfered upon, and Article 52(1) should be applied in its entirety, or when specifically requested by the Regulation (e.g., Arts. 6(1)(f)[373], 35(7)(b)).

Importantly, this approach is coherent with the overall premises of the analysis on the right to data protection. Indeed, a permissive rationale of this right entails that no data processing operation involves limitations that need to be justified in light of *all* the requirements of Art. 52(1) CFREU[374]. A more severe test (also implying proportionality in the strictest sense) should nonetheless be reserved only for interferences upon the core data protection principles (e.g., purpose limitation, information, access and rectification rights).

3.3. Legitimate interest

3.3.1. Relevant provisions and interpretation

Overview. The legitimate interest of a controller or of a third party is the basis of lawfulness provided for in Art. 6(1)(f) GDPR:

---

367 Id., §52.
368 Id.
369 Id., §66. Cf. CJEU, *Schwarz v Stadt Bochum*, judgment of 17 October 2013, Case C-291/12 § 46.
370 Cf. Clifford D, Auloos J (2018), p. 150.
371 EDPS (2017a), p. 17.
372 Christofi (2021), p. 43.
373 See below §3.3.2.2.
374 See Chapter I, §2.2.

> Processing shall be lawful only if and to the extent that at least one of the following applies: (…)
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
>
> Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

The concept of legitimate interest. The Working Party has clarified that the concept of interest is related to but distinct from that of "purpose" in Art. 5 GDPR. If the purpose is a specific objective pursued with the processing, the interest is the "broader stake" that a controller may have in the processing[375]. The nature of an interest may vary, with some being more compelling and socially beneficial (e.g., scientific research), others being more controversial (e.g., companies' economic interest to target their clients with bespoke adverts). If the interests of the controller are not widely accepted, they will not be able to override the rights and interests of the data subjects[376]. In order to justify processing under Art. 6(1)(f), the interest pursued by the controller should also be "legitimate" (i.e., acceptable under the law), as well as sufficiently specific, real and present for the controller (i.e., not speculative)[377].

Interests of third parties and rights of data subjects. Art. 6(1)(f) authorises the processing also for the legitimate interest of a third party. Art. 4(10) of the Regulation defines a third party as a natural or legal person, public authority, agency or body, other than "the data subject, controller, processor, and persons under the direct authority of the controller or processor", who is authorised to process personal data. In practice, it might be challenging to determine who the third party is. Experts suggest interpreting the notion of third party in a strict sense[378]. The latter cannot process data on behalf of the controller, or have its personal data processed by the controller. It needs to claim its own different legitimate interest to process the data, thus qualifying as a controller in its own right[379]. Actors qualifying as third parties could be public authorities pursuing law enforcement purposes or other public tasks, as well as subjects having legal claims against the data subject.

On the other hand, the interests and rights of data subjects are strongly protected. Indeed, while the interests of controllers and third parties can be taken into account only if they are legitimate, the data subject is entitled to the protection of any kind of interest, even those going against the law[380].

Criticism and appreciation. The legitimate interest grounds have long been subject to harsh criticism in literature for its elusive nature and broad wording. Some have even argued that it could constitute a loophole allowing controllers to escape data protection restrictions[381]. Specifically, criticism addressed the lack of useful guidance on the interpretation of this legal basis[382]. Attributing the balancing task directly to controllers without any clear indication could lead to undue restrictions of data subjects' rights and interests. Controllers' interests would always be destined to prevail[383]. That is why search

375 Article 29 WP (2014b), p. 24.
376 Id., p. 26.
377 Id., p. 25.
378 Kamara et al (2018), p. 14.
379 Id., p. 13.
380 Article 29 WP (2014b), p. 30.
381 Ferretti (2014), p. 845.
382 Kamara et al (2018), p. 9.
383 Ferretti (2014), pp. 856 ff.

engine operators and Internet service providers (ISPs) often relied on legitimate interest grounds to systematically process users' data for profiling purposes[384].

More recently, however, some scholars seem to have re-evaluated the role of the legitimate interest basis in EU data protection law. Since consent and purpose limitation are undergoing a severe crisis, it has been argued that a legitimacy test for data collection and processing could lead to a more effective level of data protection[385]. Contrary to what is often assumed, in fact, it is contended that such a proposal does not necessarily mean that more data would be processed[386]. If data minimisation were applied to *interests* rather than *purposes*, less or even no data at all could actually be collected and processed in many situations[387].

3.3.2. Balancing in the legitimate interest basis

3.3.2.1. The Working Party multi-factor assessment model

Controllers' interests and data subjects' rights and interests on a spectrum. The Working Party articulated a step-by-step process to apply the balancing test enshrined in the legitimate interest basis. Controllers' legitimate interests and the impact on data subjects' rights and interests should be viewed in a spectrum[388]. Controllers' stakes in the processing may go from being insignificant to more compelling. Depending on their significance, they may be more or less likely to override data subjects' interests and rights[389]. Four key factors should be considered in such an assessment: (i) the controller's legitimate interest; (ii) the impact on data subjects; (iii) provisional balance; (iv) additional safeguards applied by the controller to prevent any undue impact on the data subject[390].

(i) The controller's legitimate interest. The controller's legitimate interest may coincide with a fundamental right or freedom enshrined in the Charter or the Convention (e.g., freedom of expression, freedom of arts and sciences, right of access to documents, right to liberty and security, freedom of thought, conscience and religion, freedom to conduct a business, right to property, fair trial rights and right to effective remedy, or the presumption of innocence)[391].

Also, the controller may rely on a societal interest (e.g., medical research, publication of data to denounce government corruption). Generally speaking, the fact that the controller is acting not in pursuit of its own commercial interest but in those of society can "give more weight" to the interest[392]. Also, the controller may refer to interests that come close to those foreseen by other legal grounds, such as the performance of a contract, compliance with a legal obligation and pursuit of a public task. For instance, some processing may not be strictly necessary for the performance of a contract, but still occur within this framework. Private or public actors may decide to proactively transfer to law enforcement or tax agencies data that could have been subject to mandatory disclosure based on a legal

384 Id.
385 Prins, Moerel (2016), p. 2.
386 Id., p. 5.
387 Id., pp. 5-6.
388 Article 29 WP (2014b), p. 30.
389 Id.
390 Id., p. 33.
391 Id., p. 34.
392 Id., p. 35. See, in this regard, a decision of the Dutch Council of State, which considered that a sports TV did not pursue only a purely commercial interest in broadcasting amateur football matches, but also allowed football fans to enjoy themselves and be involved in the game. See Dutch Council of State, 27 July 2022, *VoetbalTV BV and the AP*, 20100045/1/A3. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2022:2173. Accessed 27 August 2022.

obligation. Of course, the distinction between these legal grounds is not always clear-cut, but the same rule applies: the more compelling the interest of the controller, the more likely it is to outbalance the rights and interests of data subjects.

Indeed, a legal, cultural or social acknowledgement of the legitimacy of the interest may also tip the balance in favour of the controller. For instance, it is relevant if the national or EU law authorises controllers to act in light of the public or private interest concerned. Compliance with guidelines provided by data protection authorities is equally important. Lastly, cultural and societal expectations about the processing of personal data, even if not mirrored in legislative instruments, may play a role in the assessment[393].

(ii) The impact on data subjects. This criterion takes into account the nature of the personal data processed, the way the information is being processed, the reasonable expectations of the data subjects and the status of the controller and data subject[394]. Broader emotional consequences for individuals shall be considered (e.g., chilling effects of blanket surveillance)[395]. The negative cumulative effects of linked or unrelated processing should also be examined[396].

Traditional risk assessment is an important methodology: both the likelihood that the negative event can materialise, and the severity of the consequences for the data subject should be discerned[397]. However, this should not be an exclusively mechanical and quantitative exercise. For instance, even those processing involving a minority of data subjects (or even one single individual) shall be treated with caution if the impact is potentially significant[398].

The nature of the data processed has salient implications, especially if belonging to special categories of data under Art. 9 GDPR. On the contrary, lower standards may apply if the data was already publicly available, as its further use could be reasonably expected by data subjects[399].

As for the way data are processed, various elements can be enhanced in the assessment: the fact that data was already publicly available, or whether large amounts of data are used and combined with other datasets, potentially uncovering sensitive information about data subjects[400]. Indeed, this kind of operations can lead to unforeseen and sometimes inaccurate predictions about individuals' private lives[401].

Importantly, the role of data subjects' expectations should be stressed[402]. This criterion is integrated in Recital 47 GDPR, which was positively received by privacy and data protection advocates, although not universally. This refers to the foreseeability and acceptance of the processing from the perspective of the data subject[403]. Specifically, while *foreseeability* needs to be clearly and objectively defined, *acceptance* of the processing can also be implied[404]. Also, reasonable expectations should not be interpreted

393 Article 29 WP (2014b), p. 36.
394 Id. These elements partially recall the parameters to evaluate the compatibility of secondary processing in Art. 6(4) GDPR. See Chapter II, §2.1.2.
395 Article 29 WP (2014b), p. 37.
396 Id.
397 Id., pp. 37-38.
398 Id., p. 38.
399 Id., p. 39.
400 Id.
401 Id., p. 40.
402 Id.
403 Kamara et al (2018), p. 16.
404 Id, p. 17. Otherwise, consent would be the relevant legal basis.

subjectively: the controller needs to refer to the average data subject in order to conclude whether further processing could reasonably be expected in the circumstances at hand[405].

Lastly, the status of the controller and the data subject should be examined to discern potential power imbalances[406]. Attention should be drawn to whether the controller is an individual, a small organisation, a large corporation, or a public sector body. It is important to consider whether the data subject is a child or if he or she belongs to some vulnerable segment of the population (e.g., elderly, mentally ill, asylum seekers)[407].

(iii) Provisional balance and (iv) additional safeguards applied by the controller. If controllers comply with GDPR obligations, this can help them to meet the requirements of Art. 6(1)(f)[408]. However, this alone does not ensure the legitimacy of the processing[409]. Therefore, the controller should think of introducing further protective measures, e.g., user-friendly mechanisms providing unconditional possibility for data subjects to opt-out of the processing. Additional safeguards for the security of the processing may help the controller to tip the balance in their own favour (strong data minimisation measures, immediate erasure after use)[410]. Technical and organisational measures should be considered: strategies ensuring respect of purpose limitation; anonymisation techniques; aggregation of data; privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments; increased transparency; general and unconditional right to opt-out; data portability and related measures to empower data subjects; pseudonymisation and encryption [411].

3.3.2.2. Balancing in the CJEU case law

A three step assessment. The CJEU follows a more literal interpretation of Art. 6(1)(f) GDPR. It appreciates the legitimacy of the interest claimed by the controller (step 1), the necessity of the processing (step 2), and how the interests of the controller are balanced with the rights and interests of the data subject (step 3)[412]. In the *ASNEF* judgment, the Court confirmed the exhaustive and restrictive nature of these criteria, meaning that Member States cannot add further requirements[413].

Necessity and balancing. This requirement is integrated in all the grounds of Art. 6(1) GDPR, except for consent. As outlined above for public task processing[414], necessity should be interpreted in line with its meaning in Art. 52(1) CFREU. This means that necessity is here intended as "strict necessity". The processing of personal data must be the least intrusive measure to achieve the goal pursued by the controller[415].

---

405 EDPB (2019), p. 12.
406 Article 29 WP (2014b), p. 40.
407 Id, p. 41.
408 Id.
409 Id.
410 Id.
411 Id., p. 42.
412 CJEU, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado,* judgment of 24 November 2011, Joined Cases C-468/10 and C-469/10*,* §38.
413 Id., §32.
414 See Chapter I, §3.2.5. While the CJEU explained in *Huber* the meaning of necessity within public task processing, it did not take advantage of the same opportunity in *ASNEF* with regard to legitimate interest processing. Nonetheless, taking into account the similarities between these two lawful grounds, the considerations made in *Huber* can be easily transposed in this case as well.
415 Kamara et al (2018), p. 14.

The balancing exercise in Art. 6(1)(f) adds on to the necessity test and resembles more a proportionality *stricto sensu* assessment, within the meaning of Art. 52(1) CFREU. The controller makes a value judgement as to whether its legitimate interests can override the rights and prerogatives of the data subject. To avoid sheer arbitrary decisions and abuses, different contextual circumstances can be taken into consideration[416]. Those listed by the Working Party in its Opinion can prove to be useful in this respect (e.g., nature of the data, weight of the controller's interest, impact of the data subject)[417].

3.3.3. Smart city scenarios

Who can rely on legitimate interests? For the flexibility it affords, the grounds of legitimate interest can be very useful in smart cities. Firstly, private actors can take advantage of this legal basis to pursue commercial or more widely accepted interests (e.g., research). These can indeed play a major role in smart city development, acting as urban technology providers[418]. On their side, public authorities processing data as controllers cannot in principle avail themselves of this legal basis. However, this prohibition only applies when they act "in the performance of their tasks". This should allow public authorities to rely on the legitimate interest basis outside the strict purview of their mission, e.g., to conduct smart city piloting projects. Some concrete scenarios will be analysed below to substantiate this argument.

Wi-Fi tracking: The case of the esplanade of La Défence. With the IoT, sensor tracking through Wi-Fi or Bluetooth are becoming increasingly widespread in smart cities. They can measure fluxes and concentrations of pedestrians, and serve varied purposes, ranging from the enforcement of anti-Covid social distancing measures[419] to marketing research[420].

Data protection authorities and national jurisdictions have started to deal with the privacy and data protection issues of Wi-Fi tracking. In 2015, the advertising company JCDecaux France lodged an authorisation request before the national data protection authority (*Commission nationale de l'informatique et des libertés*, CNIL) for the installation of six Wi-Fi tracking devices in the esplanade of La Défence, in the vicinity of the most visited mall in the country. The project had a strong commercial connotation. The company aimed to make automated measurements of pedestrian fluxes and people's trajectories in the esplanade. The tracking devices would be embedded in JCDecaux's smart billboards to collect the MAC addresses of any mobile device having their Wi-Fi switched on in the range of 25 metres for a period of four weeks.

The request was filed pursuant to paragraph 4 of Art. L. 581-9 of the French Environmental Code (*code de l'environnement*), which provides that each automated measurement system of the audience of an advertising device, as well as of automated analysis of a user's behaviour before an advertising device, must be authorised by the CNIL.

In its decision, the CNIL firstly stated that the data processing could not be based on users' consent. Therefore, the only legal basis that could justify the processing was the legitimate interest of the controller (i.e., JCDecaux)[421]. The latter described the esplanade of La Défence as a complex space,

---

[416] On the contextual nature of the balancing exercise, see CJEU, *ASNEF*, §40; CJEU, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González,* judgment of 13 May 2014, §74.
[417] See §3.3.2.1.
[418] Christofi (2021), p. 29.
[419] Aldegheri (2021).
[420] Centre de recherches routières – Service public régional de Bruxelles (2018), p. 6.
[421] CNIL, *Délibération n° 2015-255 du 16 juillet 2015 refusant la mise en œuvre par la société JCDecaux d'un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de La Défense*

where the traditional means of audience measuring could not be considered satisfactory due to the high presence of tourists in the area. The Commission accepted that to promote their advertisement devices and optimise their prices it was necessary to have adequate knowledge of the potential audience (that is of the number of people that could be reached by the advertising message).

Hence, the Commission found that the purpose of the processing was sufficiently defined and determined, explicit and legitimate. Importantly, it also highlighted that no targeted decision could be taken with regard to individuals concerned by the processing. Furthermore, the Commission considered the initiative to be limited in space and time, in an adequate, pertinent and non-excessive manner. In other words, the Commission esteemed the necessity requirement to be satisfied[422].

However, the data security measures implemented were deemed problematic. At the end of the four-week period, raw data collected were supposed to be aggregated and then destroyed. The CNIL considered that JCDecaux would not employ techniques that could qualify as a real anonymisation measure, as they easily allowed the re-identification of individuals. In addition, such risks were heightened because the initiative was meant to measure not only the volume of visitors in the esplanade, but also how many times individuals would pass in the vicinity of a smart billboard. Therefore, the only way for people to escape surveillance in the esplanade would have been to stop connecting to a Wi-Fi network altogether. In addition, the controller had not predisposed suitable methods to inform individuals about the data collection, nor to allow them to exercise their rights to access, rectification and objection.

As a result, the CNIL found that strict proportionality requirements were not satisfied and rejected the request. In 2017, the French Council of the State (*Conseil d'Etat*, the highest administrative court) upheld the decision of the CNIL confirming the legal soundness of its reasoning[423].

(continues): The case of the Municipality of Enschede. Between 2018 and 2020, the Dutch Municipality of Enschede set up a Wi-Fi tracking initiative in the inner city centre to monitor the responsible use of public investments in the area. The instalment and exploitation of eleven sensors working 24/7 was awarded to a private service provider, Bureau RMC. Following the complaint of a citizen, the national data protection authority (*Autoriteit Persongegevens*, AP) conducted an investigation and rendered a decision on the legality of the project[424].

At the outset, the AP analysed the personal nature of the data at stake to establish the applicability of data protection law. Although Bureau RMC and the Municipality claimed that they were processing non-personal data[425], the AP underlined how weak the anonymisation techniques employed were. Therefore, the data had to be deemed personal and collection had to be supported by a legal basis under the GDPR. The AP considered that there were three possible legal bases for the processing in that scenario: processing required to comply with a legal obligation (Art. 6(1)(c) GDPR); processing necessary for the performance of a public task (Art. 6(1)(e) GDPR); processing justified by a legitimate interest (Art. 6(1)(f) GDPR)[426].

(demande d'autorisation n° 1833589). https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000031159401/. Accessed 19 December 2021.

[422] Cf. Arts. 5(1)(c) and 6(1)(f) GDPR.

[423] Conseil d'État, 10ème - 9ème chambres réunies, 08/02/2017, 393714. https://www.legifrance.gouv.fr/ceta/id/CETATEXT000034017907/. Accessed 21 December 2021.

[424] Autoriteit Persongegevens, 11 March 2021, *Gemeente Enschede.* The analysis was carried out on an English machine translation of the decision. An English summary of the of the case is available at the GDPRhub database. https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_Gemeente_Enschede. Accessed 20 December 2021.

[425] Autoriteit Persongegevens (2021), § 3.1.

[426] Id., § 3.3.2.

Firstly, the AP excluded that Art. 6(1)(c) could serve as a viable lawfulness ground. The Municipality claimed that the processing operations were justified in light of its broad city management powers, set out in Art. 160 of the Municipalities Act. However, the AP considered that neither this piece of legislation, nor others in national or EU law, *precisely* laid down an obligation for urban authorities to perform Wi-Fi tracking[427]. Nor was the processing of personal data mentioned in any source as a possible statutory obligation or broader duty of care of municipal authorities.

Art. 160 of the Municipalities Act, framing general government tasks, could not be invoked either to ground the processing on Art. 6(1)(e) GDPR, as claimed by Enschede Municipality. The AP provided an interesting assessment of the foreseeability standards that should be met in public task processing (an issue that was discussed above)[428]. It recalled that Recital 41 GDPR requires a certain degree of clearness, precision and predictability to the additional legal basis justifying the processing under Art. 6(1)(e). The legality requirement enshrined in Art. 8 ECHR sets the same conditions. This meant that mere provision of a general mission of daily city management could not always serve as a legal basis for data processing, due to its very broad formulation[429].

Lastly, the AP ruled out that Wi-Fi measurements in the city could be justified in light of a legitimate interest of the Enschede municipality[430]. On the one hand, it did not exclude altogether that public authorities could rely on Art. 6(1)(f) for operations falling outside the scope of their statutory obligations. These might be "typical business operations", for which the government is no different from a private entity (e.g., processing employees' data for the security of buildings). On the other, the AP stated that the Wi-Fi tracking initiative did not have the features of a typical business operation. The whole project had the goal of monitoring the responsible use of public funds, which indicated that the processing was carried out in the context of municipal government duties[431]. Hence, the AP concluded that the Municipality could not invoke Art. 6(1)(f) either as the basis of lawfulness for the processing.

It is interesting to highlight once more how the level of foreseeability in public task processing may be subject to diverse interpretations in the smart city. Indeed, compared to processing under a legal obligation, there is less guidance in case law about the standard of precision that the legal basis should comply with in this case. Nonetheless, it should be considered that a provision of general city management powers, combined with an explicit authorisation for data processing, should serve this purpose[432]. In this way, citizens may anticipate for which tasks and in which situations public authorities may process their personal data for daily administration of the city.

Analysis: Lawfulness, necessity and balancing of legitimate interest processing in smart cities. The considerations made by the CNIL and the AP can be critically analysed under different profiles. Firstly, it seems that the AP relies on the excessively strict notion of what could be considered a legitimate interest by public authorities. It is generally acknowledged that legitimate interest, pursuant to Art. 6(1)(f), does not only include commercial stakes. For instance, stakes bearing significant weight in society include research and innovation. In smart cities, it is difficult to imagine which other entities could have more interest in upgrading urban environment and services rather than local authorities. Research and knowledge acquisition are crucial to smart city development. Denying public authorities the chance to resort to the

[427] Id., § 3.3.2.1.
[428] See Chapter I, §3.2.3.
[429] Autoriteit Persongegevens (2021), § 3.3.2.1.
[430] Id., § 3.3.2.2.
[431] Id.
[432] See § 3.2.3.

legitimate interest ground may prevent them from exploring paths to improve the well-being of city dwellers through new technology applications. In this sense, legitimate interests for public authorities should not be circumscribed only to regular administration tasks that have no public dimension, as prospected by the AP. They should also ground processing that falls within its governmental competences, when no associated research/innovation task is explicitly foreseen[433].

This is not to say that the legitimate interest basis should be seen as a loophole for public authorities to conduct surveillance initiatives whose boundaries are not clearly defined by the law. Research objectives could be invoked only for *embryonal* or *transitional* phases of smart city pilot projects[434]. More stable projects – a harbinger of potential consequences on individuals – could only be based on other legal bases, such as public task processing. In any case, these should be implemented with strong security measures.

Another interesting factor to examine in both decisions regards the assessment of the necessity and proportionality *stricto sensu* criteria in Art. 6(1)(f). At the outset, it is interesting to appreciate how broader commercial goals are not dismissed as legitimate grounds to carry out smart city initiatives. Economic attractiveness is indeed one of the pivotal aspects of the smart city. Nonetheless, it emerges from the decisions of both the CNIL and the AP how commercial purposes remain less compelling interests in the system of the GDPR. On the one hand, the CNIL seems to accept JCDecaux's marketing research goals only in light of the restricted geographical and temporal scope of the tracking experiment[435]. On the other, the AP considered that the interference on the right to privacy (and data protection) entailed by the Wi-Fi tracking initiative in Enshede could not be seen as proportionate in light of the processing purpose, which was testing the effectiveness of the investments in the inner city centre[436].

Both the AP and the CNIL follow a fact-based approach in assessing the necessity requirement[437]. In the *Enschede* case, the AP considered that the aims pursued by the municipality could be reached in less far-reaching ways, suggesting the use of infrared beams to count visitors[438]. As for *La Défense*, the CNIL accepted that the area had complex features that made traditional techniques of audience monitoring ineffective, especially due to the high presence of tourists[439]. Hence, one may wonder if more intrusive measures such as Wi-Fi tracking should be reserved for busier cities or neighbourhoods, excluding their use for small or middle-sized urban centres. Another factor that seemed to make the difference in both cases concerns the type of measurement to be performed. Both DPAs found the collection of absolute figures representing the number of visitors to be more acceptable and less intrusive. On the contrary, techniques suitable for reconstructing the trajectories of data subjects were considered to be more privacy-invasive and therefore not justified in light of the goals pursued.

Lastly, it important to underline how the use of sound anonymisation techniques was seen as crucial in both the French and the Dutch cases. Especially for the CNIL, the weakness of the chosen measures made the balance of interests tip against the controller. Therefore, it seems that such urban large-scale processing, if supported by (mere) economic interests, can be imposed only if such serious interferences are counterbalanced by strong security measures. While the Working Party accepts at the abstract level that legitimate interest processing may result in some negative consequences for data

[433] See Christofi (2021), pp. 37-38. Certain data protection authorities maintain a restrictive notion of what should be meant by public tasks. These should coincide only with *substantive* tasks attributed to authorities by law, excluding research interests.
[434] See Chapter II, §2.2.2.
[435] CNIL (2015).
[436] Autoriteit Persongegevens (2021), § 3.3.2.1.
[437] EDPS (2017a), p. 8.
[438] Autoriteit Persongegevens (2021), § 3.3.2.1.
[439] CNIL (2015).

subjects, the CNIL believes that such intensive data collection measures can be implemented only if data subjects are shielded from any further consequences. Controllers' commercial-oriented interests may have arguably a legitimate place in the smart city; what must be avoided, however, is that citizens "pay" from a privacy perspective.

Balancing exercises in smart city processing (permissive rationale)			
	Art. 6(1)(c) GDPR	**Art. 6(1)(e) GDPR**	**Art. 6(1)(f) GDPR**
Objective of the processing	defined by the law (Art. 6(3) GDPR)	defined by the law (Art. 6(3) GDPR) + provision of processing powers	defined by the controller
Necessity (=strict necessity in Art. 52(1) CFREU, referred to the data and means of the processing)	defined by the law (Art. 6(3) GDPR)	defined by the controller, defined by the law only for more invasive processing (e.g., CCTV)	defined by the controller
Balancing (=proportionality *stricto sensu* in Art. 52(1) CFREU)			made by the controller
Smart city uses for public authorities	mandatory collection of citizens' data by the administration, case-by-case transfers to LEAs	running city services relying on data processing (e.g., transportation)	pilot and experimental projects, general interest processing where no research competence is explicitly foreseen (only embryonal stage)

Fig. 1: Balancing exercises in smart city processing

4. Interim conclusions

This chapter addressed the following research question: *Which legal grounds legitimise data collection in smart cities and what balancing exercises do they entail?*

Preliminarily, a literature review was carried out to identify major data issues in smart cities and provide background for the investigation. Subsequently, the roots and rationale of the right to data protection were examined. This analysis showed that a permissive conceptualisation of the right at stake is more apt for tackling the challenges of urban digitisation. Indeed, seeing data protection as completely overlapping with privacy and informational self-determination does not take into due consideration the specificities of the urban context, ranging from the limited relevance of consent, the restrictions to data protection rights in the public sector, and the blurring dichotomy between private/public spaces. While privacy and data protection remain closely interrelated, these reasons justify a separate analysis of the two rights with regard to smart cities.

Another preliminary question to examine was the very applicability of data protection law in smart cities. Contrary to the claims of the proponents of many initiatives, many projects can be found to process personal data and should thus be subject to data protection law. Identifiability remains a highly debated matter in smart environments, but efforts to enlarge the scope of EU data protection law may

also be fraught with negative consequences for technology operators, which may be overburdened with compliance obligations. An old-fashioned notion of personal data seems to be misaligned with the complexity of modern big data processing, where identifiability depends on multiple factors (e.g., intentions of the actors involved, combination of different datasets, available technical means of anonymisation or re-identification). This co-existence of different "ifs" and "buts" in the qualification of personal data suggests that such question cannot be answered by means of a strict "yes" or "no". Rather, a layered approach would appear more useful, especially in smart cities. The premises for such a model may already exist in the GDPR. An explicit application of the risk-based approach to the notion of personal data may indeed suggest a differentiated compliance regime, with intensifying data protection obligations as the risks of re-identification and impacts on data subjects increase.

Afterwards, the analysis delved into the main research question for this chapter, i.e., legal bases for data collection in smart cities. Having excluded the wide applicability of consent, the attention was drawn to more pertinent legal bases: legal obligation (Art. 6(1)(c) GDPR), public task (Art. 6(1)(f) GDPR) and legitimate interest (Art. 6(1)(e) GDPR). Different requirements concerning quality of the law and balancing exercises were analysed (see Fig. 1). It emerged that varied foreseeability and proportionality requirements could be required according to the chosen legal basis and implications for data subjects. Examples of concrete smart city scenarios were also scrutinised.

Because balancing exercises are directly performed by controllers, diverging interpretations and practices with regard to data collection should be countered as much as possible to avoid arbitrary value-judgements. This analysis offered guidelines in this direction and provided a first part of the analysis on data protection issues in smart cities. Moving on from the stage of data collection, the next chapter will study another set issues, focusing on the proper management of data flows within smart cities.

II. Data Protection Issues in Smart Cities: Managing Data Flows

1. Introduction

Complex data flows in smart cities. Chapter I already provided an overview of privacy and data protection issues in smart cities. After examining grounds for data collection, this chapter will deal with further data protection principles and instruments, which are essential to manage data flows within the city. Indeed, smart cities function also thanks to seamless data repurposing among various actors, from public authorities to private companies and law enforcement. Although this may be an unavoidable consequence of urban digitisation, changes of context in data processing may betray data subjects' expectations and trust in the processing. The principle of purpose limitation is designed to counter these risks, but its application in smart city scenarios faces many challenges.

Moreover, these data exchanges often occur in the framework of PPPs, which may be inspired by different architectures. Through the lens of data protection, these agreements pose questions of data controllership. Public authorities lacking expertise and budget resources may rely on private service providers, which may in turn attempt to maximise the commercial value of the data collected. Both public and private actors participating in the processing may also try to discard their responsibilities over data, which become increasingly difficult to pin down in complex IoT environments. The GDPR already provides for instruments to address these issues, but significant power imbalances may impede a fair balancing between public and private interests.

Lastly, DPIAs can be crucial to address individual and societal risks associated with large-scale processing in urban environments. Prior to smart city projects, these can function as an arena for different actors, including citizens, to have a say on how (surveillance) technologies should be implemented. Although this could counter technocratic and top-down approaches in smart city development, integrating data subjects' views in DPIAs is not currently mandatory in the GDPR. Regrettably, this excludes community-based insights from the process of integrating technologies in the city, thus increasing power gaps between the wider public and private technology vendors.

Outline. Against this background, this chapter will analyse how to best manage data flows within the smart city, drawing on the EU data protection legislation. The addressed research question is: *What are the issues that arise from personal data flows in smart cities and how should these be addressed?* To this end, the application of purpose limitation will firstly be examined in this context. Afterwards, issues of data controllership will be studied to ensure fair data processing among private, public and law enforcement bodies participating in PPPs. Lastly, the role of DPIAs will be explored to understand how citizens could be involved in large-scale smart city initiatives, thus providing a tool for citizens to rebalance the asymmetries of power present in highly technocratic smart cities.

2. The principle of purpose limitation in smart cities

2.1. The role of purpose limitation in EU data protection law

Overview. Purpose limitation is one of the cornerstones of EU data protection law (Art. 8(2) CFREU)[440]. Its main function is to set boundaries on what controllers can do with the data they collect,

[440] De Terwangne (2020), p. 509.

while offering them some degree of flexibility[441]. The principle is made up of two building blocks. On the one hand, *purpose specification*, which obliges controllers to collect data only for specified, explicit and legitimate purposes. On the other, *compatible use*, which implies that once data are collected, they must not be further processed in a way incompatible with the initial purposes. Importantly, this principle applies to data processing in both the private and public domain[442]. Therefore, private and public entities alike are called on to balance needs of predictability of the processing with needs of flexibility[443].

2.1.1. Purpose specification

Requirements. Purpose specification is an essential step in data processing operations, and a precondition for applying other data quality requirements (e.g., adequacy, relevance, proportionality, accuracy, data retention, accountability)[444]. It determines what kind of data needs to be collected, and for how much time it is stored, based on the predetermined aims. The assumption behind this principle is that when someone shares his or her data, he or she usually has an expectation about how these will be used: respecting those expectations is vital to preserve crucial values such as trust and legal certainty[445].

Art. 5(1)(b) GDPR provides that data shall be "collected for specified, explicit and legitimate purposes". To be "specified", purposes should be sufficiently defined to enable the application of any necessary data protection safeguard and circumscribe the scope of the processing[446]. The Working Party clarified that the purposes must be specified *prior to*, or *not later than*, the time when the data collection occurs. Moreover, the purpose should be explicit, that is clearly revealed, expressed and explained in an intelligible form, contributing to the transparency and predictability of the processing[447]. Lastly, data must be collected for legitimate purposes. This requirement is not simply satisfied by providing a legal basis for the processing[448]. Legitimacy implies that the processing is "in accordance with the law" in the broadest sense, meaning that it complies with all applicable data protection safeguards, as well as other applicable laws, such as employment law, consumer law, contract law, whether written or not[449].

2.1.2. Compatible purpose

Legitimate repurposing and compatibility assessment criteria. Purpose specification does not impede, however, that collected data can never be reused for other purposes that were not initially indicated. Indeed, the law tempers the strictness of this principle and allows the reuse the data for new but compatible goals. The principle of compatible use prescribes that anytime additional uses are considered, compatible and incompatible processing operations should be discerned.

To this end, the Working Party has put forward different criteria to assess the compatibility of further processing, devising a proper "multi-factor assessment"[450]. With the enactment of the GDPR, these have been incorporated into Art. 6(4)[451]. When further processing is not based on the consent of

---

441 Article 29 WP (2013a), p. 3.
442 Id., p. 9.
443 Id., p. 5.
444 Id., p. 11.
445 Id., p. 4.
446 Id., pp. 12, 15 ff. The Working Party stated that vague purposes like "improving users experience", "marketing purposes", "IT-security purposes" or "future research" would not usually meet the requirement of specificity.
447 Id., p. 17.
448 Art. 6 GDPR.
449 Article 29 WP (2013a), p. 20.
450 Id., p. 21. The Working Party defines "further processing" with an "atomistic" approach, distinguishing data collection from any other operation.
451 On the genesis of this provision, see De Terwangne (2020), p. 316; Article 29 WP (2013a), p. 41; Rauhofer (2014), p. 152.

the data subject or another legal basis under EU or national law, these criteria should be applied to evaluate the additional processing:

(a) *any link between the purposes for which the personal data have been collected and the purposes of the intended further processing*. There should be a substantial link between the purposes of the collection and the further processing. This criterion easily covers situations where the further processing was "more or less implied" in the original purposes, or that are considered to be the "next logical step in the processing". Certainly, the more this relationship is blurred, the more difficult proving compatibility will be.

(b) *the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller*. This entails considering the customary and generally expected practises in a given environment or relationship. Power imbalances between the controller and the data subject should be looked for. Reasonable expectations of data subjects are to be evaluated against a number of factors: the status of the data controller (e.g., attorney or physician), the nature of the relationship and the service provided, the contractual obligations or the promises made at the time of collection if further processing is required by the law. Generally, the more *specific* and *restrictive* the context of the collection is, the more limitations are likely to be placed on further use[452]. The assessment should also focus on the transparency of the processing, as well as on whether further processing was required by the law (in this latter case, further processing is usually predictable).

(c) *the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10*.

(d) *the possible consequences of the intended further processing for data subjects*. Both positive and negative impacts should be considered. These may comprise potential future decisions by third parties, risks of exclusion or discrimination of individuals, emotional impacts on data subjects (e.g., irritation, fear, distress) resulting from losing control over their personal information. The assessment should also focus on whether additional operations will be carried out by a different controller with unknown consequences, if data are publicly disclosed or made accessible to a large number of persons, large amounts of personal data are processed or combined with other data sources.

(e) *the existence of appropriate safeguards, which may include encryption or pseudonymisation*. Like in any other balancing operation, the existence of additional safeguards may compensate for an initial infringement of purpose specification. These may include technical and/or organisational measures (e.g., full anonymisation, pseudo anonymisation, data aggregation). Other initiatives may involve heightened transparency and the possibility for data subjects to provide consent or opt-out of the new processing[453].

Reuse for historical, scientific or statistical purposes. The GDPR bestows a presumption of compatibility in the case of further processing for "historical, scientific or statistical purposes"[454]. This provision should not be regarded as an exemption from the requirement of compatibility, nor as a general authorisation to further processing for these goals. The above-mentioned contextual factors and circumstances should also be taken into account here for a case-by-case assessment. Specifically, technical and/or

[452] Article 29 WP (2013a), p. 25.
[453] Article 29 WP (2013a), p. 27.
[454] Arts. 6(1)(b) and 89 GDPR.

organisational measures should be aimed at preserving the so-called "functional separation". While this provision often supports public interests (e.g., research, improvement of public services), it may also be leveraged by private actors for commercial purposes (e.g., cookie tracking for websites and big data applications for market research).

2.1.3. Limitations to the purpose limitation principle

Article 23 GDPR and the proportionality assessment. Article 23 GDPR provides that restrictions can be imposed on the rights and obligations under Article 5 (including purpose limitation), when these are necessary to pursue objectives of: national security; defence; public security; law enforcement; other important objectives of general public interest of the Union or of a Member State, among others. In any case, these measures need to respect "the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society". This wording clearly recalls the proportionality test foreseen, respectively, in Article 52(1) CFREU and Article 8(2) ECHR, and should be interpreted according to the relevant case law.

Again, this suggests that a strict proportionality test should be required only when one of the core principles of the right to data protection is impinged. A stricter approach should thus be applied to data *repurposing*. Indeed, further and incompatible processing cannot be authorised with any legal basis under Art. 6(1) GDPR[455]. Only consent or a new national or EU legal basis can authorise it (Art. 6(4) GDPR). In the latter case, the law should satisfy all the proportionality requirements under Art. 52(1) CFREU (quality of the law, general interest objective, strict necessity, proportionality *stricto sensu*)[456].

2.1.4. The reality of the purpose limitation principle

A difficult application. Undoubtedly, the principle of purpose limitation is at odds with how big data processing occurs in the big data era[457]. Especially after the pandemic, many daily (and even essential) activities have transmigrated to the digital world. People live *onlife,* that is in a persistent hybrid state between the digital and analogue worlds[458]. Therefore, data collection becomes so pervasive that it is impossible to think that data subjects can actually keep track of when, why and how their personal data are used. Reading long and obscure privacy policies is at best utopian[459]. As collected data are fed to profiling systems, matched with different databases and exchanged in bulk by data brokers, data subjects often loose complete control of their personal data.

In information societies, data is a fundamental source of knowledge and power. Data collection is now a goal *per se*, and not a necessary by-product of day-to-day mundane activities. In other words, data is not simply collected to provide specific administrative and commercial services, but also to be analysed by AI algorithms which are able to uncover previously unspotted correlations.

This creates a problem also with regard to data minimisation. Whilst this principle prescribes to limit the processing to the data that are strictly necessary for the purposes, corporations and highest political pursue a "data-hungry" agenda. In the big data paradigm, "data collection and analysis *are themselves the purposes* for collecting data"[460], and the reuse of data becomes an indispensable component of this new way of processing[461].

---

455 Article 29 WP (2013a), p. 37.
456 Id., pp. 37-38.
457 For a critical perspective on the matter, see von Grafenstein (2020), pp. 511 ff; Hahn (2021), p. 39.
458 Floridi (2014), p. 43 ff.
459 See Madrigal (2012).
460 Moerel et al (2016), p. 7.
461 Id., p. 14.

Proposals for reform. Given this huge gap between the "law in the books" and the "law in action"[462], the scholarship is torn between calls to reinforce purpose limitation, or to abandon it. Among the latter group, Moerel and Prins observe that in contemporary data-driven societies the *purposes* of data processing are not the primary consideration: the *interests* that are served by the processing are[463]. And yet, purposes still play a primary role in the GDPR, while interests are subsidiary[464].

When collection becomes a purpose in itself, and its real value of lies in the *new* and *unknown* correlations the data might reveal, the original purpose of the processing becomes meaningless. That is why the two scholars propose to centre the compatibility test not on the purpose, but rather on the interest pursued with the secondary processing. Indeed, the requirements stemming from purpose limitation are practically coincident with those foreseen for processing data on the basis of legitimate interest (Art. 6(1)(f) GDPR)[465]. Given this "duplication" of criteria, regulatory requirements could be significantly simplified by merging the two tests.

Importantly, opting for a legitimate interest test does not necessarily lower the standard of protection. In situations where the processing has been grounded on meaningless consent, data collection would not likely pass a legitimate interest test. In the smart city context, where processing cannot be easily based on consent, factual assessments revolving around legitimate interest criteria may be a very useful tool to regulate further processing.

2.2. Data sharing: Legitimate expectations in different smart city contexts

Structural public-private data sharing in smart cities. Smart cities are populated by multiple actors with different goals, participating in the functioning of urban life. This co-presence of players is clearly problematic for the application of the principle of purpose limitation. Cities are often in need of considerable amounts of data to step up the efficiency of urban services, and usually turn to private companies for this.[466] Also, they usually need to partner with tech companies to digitalise urban services, from mobility to the security domain. In these settings, data flows seamlessly across public and private domains and processing operations take turns that data subjects would not easily expect.

Distinguishing the actors at play. In smart cities, the actors involved in the processing should be discerned more accurately. For instance, while the public is mostly depicted as a unitary, rock-hard element in literature, this is not necessarily true at the informational level. In examining different data sharing scenarios, therefore, three main figures could be taken into consideration: private companies, the public administration, and law enforcement agencies (LEAs). This three-fold partition reflects the institutional differences between these actors, and how individuals and groups could be affected by their activities. In particular, the fundamental distinction between the Public Administration in general and law enforcement agencies appears to be often overlooked. However, their missions can impact very differently on data subjects, even if they both belong to the State apparatus, work towards goals of general interest, and see their actions regulated by the law. With respect to law enforcement, many of their activities aim at identifying individuals[467]. Also, processing in this domain is subject to the specific regime of the LED.

---

462 Koops (2014a), p. 256.
463 Moerel et al (2016), p. 2. Cf. Article 29 WP (2014b), p. 24.
464 Id.
465 *Compare* Article 29 WP (2013a), pp. 23 ff., Article 29 WP (2014b), pp. 25 ff., and Moerel L, Prins C (2016), pp. 49-50.
466 Bass et al (2018), p. 12; Richter (2020), p. 532; High-Level Expert Group on Business-to-Government Data Sharing (2020), p. 7.
467 Although this is not always true for every law enforcement activity relying on AI (e.g., crime mapping software).

In light of these considerations, the application of the purpose limitation principle will be examined in three smart city scenarios: data sharing between the Private and Public sector[468]; data sharing within the Public sector[469]; data sharing from the Private or Public sector towards law enforcement authorities[470].

2.2.1. Private sector – public administration

Premise: terminology and variables in private-public sector sharing. Preliminarily, the meaning of the terms "repurposing" and "reuse" in this context should be understood. In their work, Custers and Uršič provide a taxonomy of possible data reuses. They distinguish data recycling, data repurposing and data contextualisation. Firstly, data recycling is defined as "using the same data in the same way more than once" (e.g., clients' billing addresses kept by private companies)[471]. Secondly, "data repurposing" entails "reusing the data for a different purpose (e.g., clients' billing addresses are used to determine risk-based insurance premiums or send advertisements)[472]. Finally, "data recontextualisation" identifies a specific kind of data repurposing, where data are reused in a completely different context (e.g., health insurance companies selling customers' data to other companies carrying out targeting advertising)[473].

The Authors add that, from a legal perspective, there is no real difference between mere data repurposing and data recontextualisation, as they both define instances of function creep[474]. Indeed, the GDPR does not formally distinguish between data repurposing and recontextualisation). At the same time, the Regulation considers the change of context as a factor that must be taken into account to assess the necessity and proportionality of a specific data reuse operation[475]. When data is reused in a new setting, data subjects' expectations are more likely to be betrayed.

In the analysis, the terms reuse, repurposing and recontextualisation will be used interchangeably, as it is often the case in relevant literature (where repurposing is often an umbrella term to define all instances of data reuse). Nonetheless, it remains important to distinguish, at least the theoretical level, instances of mere repurposing and data recontextualisation, as the latter may entail more serious interferences for the rights of data subjects.

Lastly, it should be considered that private-public data sharing might be articulated differently. In this section, data flows from private companies to the administration (business to government, B2G) and vice-versa (government to business, G2B) will be examined. While these processing operations are all subject to EU data protection law (where applicable) they may be subject to different legislation depending on whether data travels towards the private or public sector.

G2B transfers: The Open Data legislation. Government to business data sharing is a long-standing policy of the EU[476]. In 2003, the Public Sector Information Directive (PSID)[477] first regulated the field of open data, with the aim of unleashing the full economic potential of publicly-held information. The Directive removed major obstacles to data sharing and laid down uniform rules on pricing, licensing and exclusive arrangements (Art. 1(1) PSID). The right to reuse of public sector information was

468 See §2.2.1.
469 See §2.2.2.
470 See §2.2.3.
471 Custers et al (2016), p. 8.
472 Id.
473 Id., p. 9.
474 Id.
475 Cf. Art. 6(4) GDPR.
476 On open data legislation and smart cities, see Dalla Corte (2020). See also Catanzariti, Curtin (2023a), p. 23.
477 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

established in Article 3: where the reuse of public documents was allowed under domestic legislation, these had to be made available, through electronic means, for commercial and non-commercial purposes.

The PSID was then recast in 2013 and its scope was significantly extended to include data held by public undertakings in the transport and utilities sector[478]. Later, the 2019 PSID recast (the Open Data Directive)[479] introduced the notion of high-value datasets, i.e., "documents, the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and of the number of potential beneficiaries of the value-added services and applications based on those dataset" (Art. 2(10) PSID)[480]. For those datasets, the 2019 PSID established a legal basis for mandatory data disclosure[481].

Lastly, as a deliverable for its *European Strategy for Data*, the European Commission adopted a proposal for a Data Governance Act (DGA) in February 2020, which was finally adopted in May 2022[482]. This piece of legislation aims to set forth an ambitious mechanism for the exchange of all kinds of digital resources, including personal data. It thus also overlaps with the GDPR and covers data that escaped the previous legislation on open data[483]. The structure and the implications of the DGA will be analysed further on in Chapter VI.

B2G transfers in smart cities and the Data Act. While G2B sharing is strongly supported in the EU, the interest in B2G transfers is quite new. This paradigm shift follows the growth of the data economy, which has seen private corporations harvesting huge amounts of data, unseating the public sector as the main keeper of data resources. In G2B, data transfers occur in different frameworks, like public tendering agreements or licensing schemes[484]. Different municipalities now frequently impose data disclosure as a mandatory condition to participate in public tendering procedures, or to conclude PPP agreements where private companies are tasked with running public services. Others ask businesses to disclose their data in order to be awarded a licence to conduct their business in the city[485]. In further cases, cities even purchase data from companies[486]. At the legislative level, B2G will soon be regulated by the forthcoming Data Act (DA), which will be examined in Chapter VI.

Balancing in public-private sector data repurposing. It should be highlighted that data transfers between the public and private sectors remains subject to data protection law, and thus to purpose limitation[487]. Therefore, these operations entail complex balancing.

For instance, this principle also applies to publicly available data: the fact that personal data has been made open for one purpose does not mean that it can be reutilised for whatever goal[488]. Public sector

478 See European Commission (2018b).
479 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.
480 These are: geospatial; earth observation and environment; meteorological; statistics; companies and company ownership; mobility.
481 See Arts. 5(8), 14(1)(a); Dalla Corte (2020), p. 91.
482 European Commission (2020) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) COM/2020/767 final; European Council of the European Union (2022).
483 See de Hert (2023), pp. 107 ff.
484 See further Chapter VI, §5.2.2.
485 See Marshaal (2019).
486 Bass (2018), p. 12.
487 Article 29 WP (2013b), p. 6; Article 29 WP (2003).
488 Article 29 WP (2013b), p. 20.

agencies that are required to disclose data must perform a compatibility assessment. When there is no legal obligation to share data, they should cautiously check whether the conditions legitimising data repurposing are met, e.g., if the third party can invoke a legitimate interest[489]. Alternatively, public authorities may seek the data subjects' consent when they want to share personal data that have been collected for conducting a survey or concluding a contract (e.g., if public bodies want to use data collected from university students upon enrolment for direct marketing purposes)[490].

In particular, the reuse of publicly held information requires the right to data protection to be weighed against different values, from the interest to good administration, the freedom of business and expression. Various data sharing mechanisms may prioritise certain interests over others. For instance, open data regimes imply the highest degree of interference with the right to data protection, to the benefit of innovation needs[491].

Preliminary proportionality assessment for smart city repurposing. Unfettered data repurposing through open data among smart city actors seems at odds with EU data protection, especially with the principle of purpose limitation[492]. Because purpose limitation is a fundamental element of the right to data protection (Art. 8(2) CFREU), any kind of processing that interferes with it should be subject to the proportionality test of Art. 52(1) CFREU.

In this exercise, the intensity of the assessment should be established preliminarily according to the factors identified in the CJEU case law: the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference[493]. Afterwards, if the repurposing is not grounded on consent or on another legal basis, Art. 6(4) GDPR sets five criteria that provide further guidance in the balancing exercise[494].

Proportionality assessments are designed to be applied to concrete, factual situations[495]. Nonetheless, suggestions tailored to smart cities can be proposed. Generally, the intensity factor to be taken in the proportionality assessment would be impacted by:

I. *The area concerned*[496]. Smart cities data can flow between the public and private sector, two areas that feature different and often opposing logics. For instance, private companies frequently run public services on behalf of the administration, and public bodies are ever more "contaminated" by corporate strategies aiming at making their functioning more efficient. Hence, the boundaries between the two areas are increasingly blurred, which complicates the task of identifying the precise context of the processing. Clearly, this criterion poses difficulties in smart cities and requires careful consideration.

II. *The nature and seriousness of the interference.* In smart cities, private-public sector data sharing can occur occasionally, in the form of disclosure of specific data or datasets, or structurally, in the framework of agreements. Also, data sharing can steer innovation when data is used to inform machine-made decisions on how to manage public services[497]. Therefore, the interference with data subjects' rights can have different levels of seriousness. Firstly, the degree of significance of

489 Article 29 WP (2003), p. 8.
490 Id. Here, legitimate interest under Art. 6(1)(f) could be invoked as a basis to repurpose the data.
491 Dalla Corte (2020), pp. 207, 261-262.
492 Dalla Corte (2020), p. 207.
493 CJEU, *Digital Rights Ireland*, §47 (citing also ECtHR, *S. and Marper v the United Kingdom*, § 102).
494 See Chapter II, §2.1.2.
495 EDPS (2017a), pp. 8 ff.
496 This criterion is similar to that of "context" in Art. 6(4)(b).
497 This is acknowledged also by the EDPS (2020), §§ 21-23.

the restriction may be higher as much as the volume of data repurposed[498]. Additionally, the seriousness of the limitation upon the right to data protection can be even higher if the transfers are programmed on a systematic basis, e.g., in the case of structural agreements like PPPs).

III. *The object pursued by the interference.* Given the multiplicity of actors in smart cities, data transfers between the private and public sector can serve several goals. Data can be repurposed for research reasons, to improve public services, inform on decisions in emergency situations, be commercialised (e.g., for targeted advertising), or otherwise support the economic development of the company (i.e., statistical repurposing).

Arguably, processing directed at public interest goals should be subject to a lighter proportionality assessment[499]. For example, the need to use the data to organise effective responses in emergency situations should carry an even higher weight on the test. In other words, the reuse of data for the "common good", or to benefit larger societal groups, should generally favour data repurposing. If this trend has not been explicitly supported by data protection consultative bodies at the EU level, a double standard approach towards commercial and non-commercial data repurposing can be observed through a systematic reading of the opinions of the Article 29 Working Party, the EDPS and the EDPB. Indeed, they seem to adopt a double standard approach towards commercial and non-commercial data reuse. With regard to public interest repurposing specifically, EU data protection bodies seem to advocate a lighter approach, compared to for-profit processing of publicly held data[500].

Instead, data transfers to the private sector should be assessed differently. On the one hand, data reuse for statistical and research purposes appears less problematic. Indeed, the development of the internal market is one of the established objectives of the EU (Arts. 26 and 114 TFEU), and economic flourishment is one of the pivotal aspects of the smart city paradigm[501]. Often, private companies in the tech sector are actively involved in the provision of services and the improvement of the urban environment, meaning that research repurposing can indirectly pursue some goals of general societal benefit. In this case, the proportionality assessment could take a more lenient form.

On the other, many more criticalities emerge when data is transferred to private companies for commercialisation purposes. These issues were approached inconsistently by the Working Party, which once stated: "The distinction between re-use for commercial or non-commercial purposes should not be decisive when considering the compatibility of further use of personal data. The assessment of compatibility should not be primarily based on whether the economic model of a potential re-user is based on profit or not"[502]. On other occasions, it also declared: "If personal data are to be re-used for commercial purposes, this secondary purpose may be considered as incompatible and thus the information not be disclosed"[503]. The EDPB and EDPS reiterated this latter position in the 2021 Joint Opinion on the DGA: "Any subsequent use of data, collected and/or shared in pursuit of a public task (e.g., for improving transport/mobility or tackling serious cross-border threats to health), for commercial for-profit purposes (for instance

498 Cf. CJEU, *Digital Rights Ireland*, §48.
499 See the arguments proposed in Chapter IV (with regard to environmental objectives) and VI.
500 See, e.g., EDPS (2020), § 21.
501 See Introductory Chapter, § 3.2.3.
502 Article 29 WP (2013), p. 21.
503 Article 29 WP (2003), p. 9.

insurance, marketing, etc.) should be avoided"[504]. The same arguments were also put forward in the EDPS Opinion on the *European Strategy for Data*[505].

Art. 6(4) criteria in the smart city context. Having assessed the intensity of the interference, the criteria listed in Art. 6(4) GDPR should be applied if there is no consent or additional legal basis to repurpose data. These requirements can be translated in the smart city context and applied to both G2B and B2G transfers, as follows:

I. *The context*. In smart cities, expectations and changes of context should be gauged not so much on the subjective nature of the actors involved, but rather on the specific use or purpose sought with the processing. Therefore, the contexts of the processing should be established mainly through objective criteria, rather than the subjective nature of the recipients of the data. In this sense, data repurposing may be proportionate if, for instance, private actors intend to use the data in the public interest.

II. *The nature of the data.* the nature of the data to be repurposed is relevant in different aspects. Of course, special categories of data under Art. 9 GDPR benefit from reinforced protection in the Regulation. Therefore, their repurposing should be underpinned by pressing needs to pass the proportionality assessment. Nonetheless, identifying what sensitive data is may not be easy in smart urban environments[506]. Here, data may not be sensitive *per* se, but become so in light of the processing[507]. Certain data points, that are "innocent" at a first glance, can actually reveal pretty sensitive aspects of individuals' private lives if combined together through analytics[508]. Therefore, attention should be paid to the ultimate goal of the processing, e.g., whether data is meant to be combined with different datasets for profiling purposes.
Moreover, the Working Party has warned about cases of mandatory data disclosure: "a data subject that has been co-opted to provide his or her personal data to the administration will not usually expect reuse of such data for different purposes. Thus, this kind of processing may actually be unfair, especially if third parties mean to commercialise the data"[509]. This should be kept in mind when data is to be repurposed by the public sector to the private domain.
On a different note, specific datasets can present a particular value for society, thus making the balance lean towards the repurposing solution. This is the case of "high-value datasets". In this case, the legislator seems to have embedded the balancing test in the legislative basis, making availability of those datasets mandatory in every case. The underlying rationale, again, seems to focus here on the crucial contribution that these resources could bring to society as a whole.

III. *The consequences for data subjects*. The right to data protection is closely interconnected with other fundamental rights (see, e.g., Recital 75 GDPR). Coherently with the risk-based approach informing the Regulation, the higher the risks for data subjects, the higher the caution that should be employed in assessing the proportionality of the repurposing.

---

[504] EDPB, EDPS (2021a), § 74.
[505] See EDPS (2020), §§ 21-25.
[506] The definition of sensitive data is often seen obsolete in the scholarship. See Moerel L, Prins C (2016), pp. 11 ff ; De Hert et al (2009b), p. 439.
[507] Moerel et al (2016), p. 11.
[508] CJEU, *Digital Rights Ireland*, §27; CJEU, *Tele 2 Sverige AB/Watson*, judgment of 21 December 2016, Joined cases C 203/15 e C-698/15, §99. In the United States, see *Carpenter v United States*, 585 U.S. ___ (2018), pp. 10 ff.
[509] Article 29 WP (2003), p. 9.

In the smart city context, the pervasive nature of data collection and automated decision-making makes all the above-mentioned risks very relevant. There are countless scenarios that could be postulated. In some instances, there are processing operations whose likely impact on individuals is very remote, such as the use of data on weather, park irrigation or noise levels. In such instances – even assuming that one considers this data to be personal[510] – the potential consequences of the processing have no great effect on citizens, and repurposing may actually be allowed on very loose conditions.

In other cases, repurposing could actually affect the legal and material situation of data subjects living in smart cities, e.g., when the processing could result in denying access to a public service or social benefit to citizens. This might be the case in which RFID-equipped cards (even with embedded biometric information) function as identity verification instruments, unlocking access to essential services or government funds[511].

Conclusion on the balancing test. This section presented guidelines for data repurposing applicable to smart city scenarios. Hopefully, these bear a potential for generalisation. The given methodological indications could make balancing exercises on data repurposing more granular and accurate in smart cities. This two-step methodology – comprising a preliminary assessment on proportionality approach, and one on compatibility – can prove to be effective also in other repurposing scenarios, as will be shown in the following subsections.

	Preliminary proportionality assessment *(the area concerned, the nature and seriousness of the interference, the objective pursued)*	
Consent (balancing made by the data subject)	**New EU or national legal basis (Art. 23 GDPR)**	**Compatibility assessment (Art. 6(4) GDPR)**
	Art. 52(1) CFREU: • *quality of the law* • *suitability* • *necessity* • *proportionality* stricto sensu	• *contexts and links between the processing* • *nature of the data* • *consequences for data subjects* • *appropriate technical and organizational safeguards*

Fig. 2. Balancing exercises in public-private sector repurposing

2.2.2. Public administration – public administration

Informational division of powers in the Public Administration. An important thing to consider in data sharing within the public sector is that the administration cannot be identified as one *informational unit*. In this domain, in fact, the principle of legality imposes an "informational division of powers" (*Informationelle Gewaltenteilung*) between public bodies[512]. This principle, firstly rooted in the German system, entails that the law must regulate beforehand which authority may collect or process which type of information, in the same way it does with all other functional activities of the State[513]. With the development of information technologies, the informational separation of powers was conceived to discourage pervasive data collection by the government and reckless data sharing across different departments.

[510] Cf. Purtova (2018a).
[511] See, e.g., MacDonald (2020); Financial Post (2020).
[512] See *Urteil des BVerfG* v. 15.12.1983 zum VZG 83 (1 BVerfGE 65), §§ 46, 69.
[513] Brouwer (2011), pp. 273-294. Article WP (2013b), p. 6.
[513] Article 29 WP (2013b), p. 19.
[513] Brouwer (2011), p. 280; von Grafenstein (2020), p. 515.

In the public sector, therefore, the normative rationale of purpose limitation is reinforced by the constitutional principles of legality and the rule of law[514]. Purpose specification is complied with only where the law defines the goals of the processing with a certain precision and clarity. In this regard, the Belgian Data Protection Authority (*Commission de protection de la vie privée,* now *Autorité de protection des données*) stressed that the purpose of the processing needs to meet "organisational" and "functional" requirements, determining which administration is entitled to process the data and ensuring that the processing falls within the missions of said administration[515]. Importantly, setting up networks of data sharing is allowed, being mindful of the plurality of purposes pursued with the processing. In that case, the law should delimit the scope and goal of each processing activity clearly[516].

What are the possible alternatives? As outlined above[517], this rigid separation between administrative departments and authorities at the informational level stands in stark contrast with the need to ensure efficient data flows within the smart city. Therefore, alternatives to enable seamless data processing should be explored. In this context, three possible choices seem to be available: (i) research repurposing; (ii) multi-factor assessment (Art. 6(4) GDPR); (iii) the enactment of broader legislative frameworks allowing data sharing within the public administration.

(i) Research repurposing. The reuse of data for research purposes can be of extreme importance for smart city development. Research can entail the development of testbed and pilot projects aimed to improve the efficiency of smart city services, or to initiate new projects for the common good of the city. Sharing of information can thus be beneficial to leverage past experiences in urban development.

When research is identified as the goal of the processing, public or delegated private entities involved in the project could share smart city research data with each other pursuant to Art. 89 GDPR[518]. In this case, the processing shall be subject to appropriate safeguards to protect the rights and freedoms of the data subject (e.g., data minimisation). Pseudonymisation and anonymisation measures should also be implemented as long as the purpose of the processing can be fulfilled.

(ii) Leveraging Art. 6(4) GDPR. Where there is no legal basis to share the data, public authorities may simply rely on consent (which may be a burdensome option), or on Art. 6(4) GDPR[519]. In this assessment, the power imbalances existing between public authorities and citizens may not weigh in favour of repurposing, considering the potential vulnerable position that data subjects have in relation to the State.

However, some surveys reveal that citizens generally have higher confidence rates in how public, rather than private bodies, manage their data[520]. Indeed, as far as potential consequences for data subjects are concerned, the balancing exercise may lean towards data sharing when this is mainly aimed at improving public services and is not likely to have an immediate negative impact on citizens concerned (e.g., uncovering of criminal offences or tax irregularities). Technical and organisational precautions should also be taken into consideration, especially when sensitive data is at stake.

514 Degrave (2009); von Grafenstein (2020), p. 515.
515 Degrave (2009), p. 50.
516 Id., p. 52.
517 See above §2.2.
518 On Art. 89 GDPR see §2.1.2.
519 See above §2.1.2.
520 Moerel et al (2016), p. 16 note 62. Other surveys confirm that people are most comfortable when their data is used for the public good and least comfortable when the processing is profit-driven, Schmit et al (2021).

(iii) Data sharing schemes. Another alternative for more fluid data flows between public administration bodies are data sharing laws. This solution is allowed by Art. 23 GDPR, which foresees the possibility to restrict some data protection principles, including that of purpose limitation[521]. Among the objectives that justify this kind of operation, there are those "of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State" (Art. 23(1)(e) GDPR). The national or EU legal basis should set the boundaries of general interest goals pursued and abide by the principle of proportionality.

Two fairly recent examples of such data sharing initiatives are the UK's Digital Economy Act (2017)[522] and Ireland's Data Sharing and Governance Act (2019)[523]. These pieces of legislation serve as general frameworks enabling smoother data transfers within the Public Administration, when this is aimed to improve public service delivery. A third noteworthy data sharing scheme is established by Art. 17 of the French Law no. 2016-1321 (*Loi Lemaire*)[524].

First of all, the UK Digital Economy Act is aimed to "improve public services through the better use of data, while ensuring privacy, clarity and consistency in how the public sector shares data"[525]. Specifically, various public service delivery objectives are identified as legitimate aims of data sharing: assistance of people experiencing multiple social or economic disadvantages, or living in fuel or water poverty; reduction and management of debt owed to the public sector; and combatting fraud against the public sector[526]. Section 35 of the Act authorises public authorities to disclose information about an individual to another authority for "specified objectives". To be specified, an objective must meet three cumulative conditions. Firstly, it should seek (a) the improvement or targeting of a public service provided to individuals or households, or (b) the facilitation of the provision of a benefit (whether or not financial) to individuals or households. Secondly, it should be aimed at improving the "well-being of individuals or households", including (a) their physical and mental health and emotional well-being, (b) the contribution made by them to society, and (c)their social and economic well-being. Thirdly, the objective should support (a) the delivery of a specified person's functions, or (b) the administration, monitoring or enforcement of a specified person's functions.

Furthermore, data sharing among public bodies in Ireland is regulated by Section 13 of the Data Sharing and Governance Act (DSGA). This provision lays down the general conditions allowing public authorities to disclose citizens' data to another public body when such transfers are not already grounded on another basis in EU law. Data sharing under Section 13 can occur only to allow public authorities to pursue their goals or for legally predetermined objectives. Some of these are worth mentioning: facilitating the administration, supervision and control of a service, programme or policy (Sec. 13(2)(a)(ii)(V) DSGA); facilitating the improvement or targeting of a service, programme or policy delivered (Sec. 13(2)(a)(ii)(VI) DSGA); enabling the evaluation, oversight or review of a service, programme or policy (Sec. 13(2)(a)(ii)(VII) DSGA); analysing the structure, functions, resources and service delivery methods of one of the two public bodies involved (Sec. 13(2)(a)(ii)(VIII) DSGA).

These legislative initiatives should be welcomed because they provide citizens with greater legal clarity on which kind of data sharing they should expect within the public administration. Certainly, the

---

[521] See above §2.1.3.
[522] The UK Digital Economy Act (2017) (c. 30).
[523] The Irish Data Sharing and Governance Act (Act No. 5 of 2019)
[524] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (1), JORF n°0235 du 8 octobre 2016.
[525] ICO (2020), p. 66.
[526] Id., p. 69.

level of specificity of these provisions is not high, as they simply refer to expressions such as "facilitating" or "improving" the provision of a public service. Still, it could not probably be otherwise: the legislator (and arguably anybody) is not in a position of foreseeing all possible situations where the administration will need to process data for such aims. Indeed, this goes back to the "more general" nature that legal bases grounding public task processing inevitably have[527]. That is why it is appreciated that Section 13 of the Irish DSGA explicitly recalls the necessity principle as a guiding principle for controllers that decide whether or not a specific operation is strictly needed to pursue the public interest goal. Also, it is important to underline how data sharing is explicitly circumscribed to instances where the processing can have a positive effect on individuals as beneficiaries of public services.

The UK regime however includes some exceptions, as data sharing is allowed also for "combatting fraud against the public sector". In this regard, the Working Party believes that public tasks can be leveraged by controllers to proactively transfer data which may suggest the occurrence of a criminal offence (e.g., tax evasion), even when there is no obligation to do so[528]. Hence, the provision should not be seen as highly critical. However, when the processing risks transhipping to the law enforcement domain, clearer and more specific legal bases would be required[529]. Indeed, the Working Party also admits that, even when public task processing is involved, if the operation entails (a significant) invasion of privacy, a more specific and precise legal basis should be provided for[530].

Lastly, in France, Art. 17 of the *Loi Lemaire* lays down a mandatory data sharing scheme between private companies running public services and the administration in the framework of public-private partnerships. This provision states that private companies tasked with running essential public services must provide the delegating public administration with the datasets (in open and readable format) that have been generated while managing the service. It also adds that the public administration remains free to process, extract information from and reuse the data at its disposal. Even if the provision targets PPPs, these transfers should be labelled as processing operations within the public administration. Indeed, when private bodies run services on behalf of the public sector, they are usually equated to a public body while exercising their functions. Also, compared to the English and Irish cases, Art. 17 of the *Loi Lemaire* does not address instances of one-time data disclosure between public sector bodies. It rather aims to establish structural data sharing flows between such entities. This kind of regime seems thus more apt to unleash the potential of urban data in smart cities.

Concluding remarks on intra-administration data sharing. Within the public administration, data flows need to accommodate opposing interests, between the need to uphold the principle of informational division of powers and those of urban innovation. Different legal instruments can ensure a higher level of flexibility for data sharing in this domain, while respecting citizens' rights to privacy and data protection. Firstly, public authorities may rely on Art. 89 GDPR. Secondly, when there is no legal basis to share data across public departments, authorities can also rely on the multi-factor test under Art. 6(4) GDPR. In this case, nonetheless, a careful balancing test is required. Finally, from the perspective of citizens, the provision of explicit data sharing schemes probably affords the highest degree of foreseeability in terms of data repurposing within smart city authorities. Therefore, a proliferation of such regimes is desirable at the European level.

[527] See Chapter I, §3.2.3.
[528] Article 29 WP (2014b), p. 21.
[529] See below §3.2.3.
[530] Article 29 WP (2014b), p. 22.

2.2.3. Private sector/public sector – law enforcement

Preliminary distinction between case-by-case and structural sharing. Data repurposing towards the law enforcement sector can take many forms. On the one hand, there might be on-point, case-by-case data disclosures relating to specific criminal investigations. On the other hand, structural data flows between the police and non-law enforcement bodies can occur within the framework of PPPs. In smart cities, for instance, private technology providers (e.g., companies marketing facial recognition software) enter into partnership with local police departments. It is important to distinguish these two scenarios as processing in the law enforcement sector is regulated by the special regime of the LED, which has a particular interplay with the GDPR[531]. Indeed, if case-by-case repurposing seems to fall within the scope of Art. 23 GDPR, in PPPs the applicable legislation appears to be the LED[532].

Case-by-case disclosure: Applicability of Art. 23 GDPR and higher quality of the law standards. Data that is transferred to law enforcement in these instances was originally collected under the GDPR, and the first controllers (public and private entities alike) cannot qualify as "competent authorities" under Art. 3(7) LED. They have not been entrusted by national or Union law with a law enforcement mission, and they only process data for their own commercial, statistical and general interest goals pursuant to the GDPR[533]. Disclosure to the police is not initially foreseen, but purely contingent. This makes the regime of the Directive inapplicable. That is because two cumulative conditions need to be satisfied for the regime to be triggered: processing is carried out for a law enforcement objective and performed by a competent authority pursuant to Art. 3(7) GDPR.

Therefore, the legal basis for data repurposing in these scenarios is Art. 23(1) GDPR. This provision authorises necessary and proportionate restrictions of the rights granted by the Regulation for reasons of public security (letter c) and prevention, investigation, detection or prosecution of criminal offences (letter d). Another relevant provision in this domain is Art. 15 of the e-Privacy Directive, which obliges providers of electronic communication services to retain users' data and disclose them to LEAs upon request, where this is proportionate to safeguard national security, prevent, investigate and prosecute crime, and address threats to public and national security.

High "quality of the law" standards would be needed here to legitimise processing involving such a strong invasion of privacy for data subjects, as required by the ECtHR's case law on the foreseeability of surveillance measures[534]. Such standards have also been integrated into the case law of the CJEU in *Digital Rights* cases, which concerned on-point disclosure of communication data from service providers to law enforcement. The legislator should embed a proportionality assessment in the legal basis, making sure that repurposing operations are restricted to what is strictly necessary in terms of the categories of data to be repurposed and the means of the processing. A pertinent criterion in this sense would be allowing transfers of GDPR data to law enforcement authorities only for the fight against serious forms of crime[535].

Moreover, in *Spetsializirana prokuratura*, the Court highlighted an additional criterion for the legitimacy of data transfers from the private to the law enforcement sector. It clarified that a decision of an independent or judicial authority authorizing the data disclosure is not, by itself, enough to comply with the rights to privacy, data protection, and effective remedy as enshrined in the CFREU. It is also necessary that national legislation foresees the possibility for data subjects to be informed of such

531 See Purtova (2018b).
532 Neroni Rezende (2020), pp. 381 ff.
533 Cf., for the Clearview case, Neroni Rezende (2020), pp. 378 ff.
534 Cf. Chapter I, §3.2.3.
535 Cf. CJEU, *Digital Rights Ireland,* §§ 57-59; CJEU, *Tele 2/Watson,* §§102, 106.

processing and object to it before the authorizing body[536]. The Court grounds this requirement on the right to information about the processing, which is explicitly foreseen in Art. 13 LED[537] and constitutes the precondition for the exercise of the right to an effective remedy. Nonetheless, paragraph 3 of this provision indicates that this right can be delayed, restricted, or omitted to avoid prejudicing the prevention, investigation, and prosecution of criminal offences, or to protect public security, national security, and the rights and freedoms of others. Neither this legislation nor the Court give precise indications on how such derogations should be implemented in national systems, e.g., if competent authorities should justify on a case-by-case basis their decisions not to inform data subjects that their data has been transferred to law enforcement. The CJEU was ambiguous about this obligation in *Spetsializirana prokuratura*. While the Court requires that the right to information is foreseen in national legislation, it does not clarify if and how competent authorities can take advantage of the related exception[538]. Specifically, it is not clear whether the right to information should be effectively "guaranteed" in *each* proceeding at some point[539], or if it is enough that this is only foreseen in national legislation, allowing competent authorities to derogate from it on a case-by-case basis, possibly without having to justify it to data subjects.

Therefore, as things stand, the obligations to be fulfilled by competent authorities in data repurposing from the private to the law enforcement sector are not clear-cut, and this may arguably hamper the possibilities for data subjects to exercise their right to an effective remedy in this context.

Structural agreements (PPPs): Purpose limitation issues? Structural agreements between the police and the non-law enforcement parties pose different privacy and data protection issues[540]. However, purpose limitation is probably not the most urgent one. In these interplays, only the special regime of the LED applies[541]. In this case in fact, the entities cooperating with the police could qualify as controllers or processor under the LED.

The interrelationship between different cooperating entities is clarified by Recital 11 LED. It indicates that when private entities or bodies are bound "by a contract or other legal act" to law enforcement agencies, they process data *on behalf* of competent authorities and become processors under the Directive. On the other hand, when they determine the objectives of the processing as equals, a situation of joint controllership is established[542].

In the LED, the principle of purpose limitation is enshrined in Arts. 4(1)(b) and (2). Nonetheless, this principle does not seem to be put under severe stress in this context. Here, public or private entities collect data for the specific purpose of making them available to law enforcement agencies, being directly involved in their security activities in the first place. Therefore, the collection of data is already underlined by a law enforcement purpose, which is the same as, or should be deemed compatible with, the one pursued by public security authorities. Whether the cooperating private party is acting as a processor or as joint controller, indeed, the purpose underlying the processing can be considered to be the same (e.g. preventing crime in a specific area). There is arguably only one purpose legitimising the collection and further analysis, detailed in light of the goals laid down in Art. 1(1) LED.

536 CJEU, *Spetsializirana prokuratura*, judgement of 17 November 2022, Case C-350/21, §§70-75
537 CJEU, *Spetsializirana prokuratura*, §§70-71.
538 Id., §§75-77.
539 As it may appear from the wording of the ruling at §77.
540 See Purtova (2018b).
541 Id., p. 65; Neroni Rezende (2020), pp. 381 ff.
542 Art. 21 LED. See Purtova (2018b), pp. 65-66; Neroni Rezende (2020) p. 382.

Differently, any further processing of the data (e.g., transfer to another LEA or use in another criminal proceeding) should be surrounded by greater caution. That is the case where LEAs share data, with other LEAs in the framework of data disclosure requests or interoperable databases at the EU level. Data may be used to investigate or prosecute rather different crimes (e.g. in terms of seriousness), or tackle situations in different Member States. Usually, the LED merely distinguishes between "law enforcement" and "non-law enforcement" purposes, rather than focusing on how various law enforcement objectives might be different and incompatible[543]. Actually, in these scenarios, the *interest* underlying the first and the secondary processing might be similar, as it relates to law enforcement in general, but the specific *purposes* of the two processing might be slightly different and not necessarily compatible. Despite this gap, interpreters should conduct a proportionality assessment even within the security domain, for instance by taking into account the seriousness of the offence for which data should be reused.

Concluding remarks on data repurposing towards the law enforcement sector. Because of the sensitivity of the interferences at stake and the potential consequences for data subjects, repurposing towards law enforcement actors should be handled with the utmost caution. To address purpose limitation issues in this domain, a preliminary distinction between case-by-case data disclosures and data sharing in PPP scenarios was made. The first case entails an interplay between the GDPR and the LED regimes, as the data transfer is subject to the criteria set out in Art. 23 of the Regulation, before moving into the scope of the Directive. Disclosure under a legal obligation in this case requires higher "quality of the law" standards, which should be gauged in light of the relevant ECtHR and CJEU case law. On the other hand, PPPs only entail application of the LED. Private companies and public bodies alike can qualify as controllers or processors under the Directive, processing data for law enforcement goals right from their initial collection. While these agreements may not pose serious issues in terms of purpose limitation, granular compatibility assessments should always underpin further data reuse within the security domain.

3. Controllership in public-private partnerships

3.1. What are public-private partnerships?

Conflicting definitions. Numerous – and sometimes conflicting – definitions of PPPs exist today. On general terms, Savas identifies PPPs as "any arrangement between government and the private sector in which partially or traditionally public activities are performed by the private sector"[544]. In PPPs, the public sector's goals of delivering services meet profit objectives of private companies, which (partially) assume the risks of the undertaking[545]. In turn, public authorities can benefit from the expertise, increased flexibility and competitiveness brought by the private sector[546].

The concept of PPP may be subject to more technical analyses and is not always consistent in the economy and administrative law literature[547]. Nonetheless, two significant aspects of PPPs are worth mentioning. Differently from occasional outsourcing, PPPs feature a fair stability of the agreements between the public and private parties[548]. Also, a variety of interactions may stem from contractual

[543] Emanuilov et al (2020), p. 29.
[544] Savas (2000), p. 4; see also Bexell et al (2010), p. 6; Bevir (2009), p. 161; Vutsova et al (2014), p. 85.
[545] Vutsova (2014), p. 85; Ross et al (2015), p. 449.
[546] Linder (1999).
[547] Reynaers (2014), p. 41.
[548] Id., p. 42; Bevir (2009), p. 161. See also European Court of Auditors (2018), p. 12.

schemes, which can be significantly formal and hierarchical or more informal and horizontal[549]. From a data protection standpoint, this means that different configurations in terms of who is the controller, and who is the processor of a given processing can be possible, as will be shown down below[550].

PPPs in smart cities. As already indicated, PPPs constitute a key feature of the smart city paradigm[551]. The increasing involvement of private corporations in public urban development indeed fits within a broader shift towards more decentralised and pluralistic models of (local) governance[552]. For private companies, the smart city has represented a promising, untapped market since the 2000s. By grasping it, big tech corporations such as IBM and Cisco had the opportunity to unilaterally set both the problems and the solutions for large urban environments[553]. On their part, local authorities also benefitted from the growing marketisation of smart urban solutions. Advertised as means to achieve resource efficiency, technologies held the promise of helping post-recession, under-budgeted municipalities to make ends meet and relaunch cities' economic competitiveness[554]. On a normative level, the integration of corporative strategies into urban policies aimed to strengthen three important values that seemed to be often lacking in public administration: efficiency, quality and collaboration[555]. Allegedly, the private sector had more efficient management strategies and prompter problem-solving abilities, which could help local authorities to run public services in a more cost-effective fashion[556]. Additionally, it was assumed that PPPs could boost service quality through innovation and competition, and provide new solutions to long-standing urban issues[557]. Lastly, the involvement of private actors seemed to offer a more pluralistic and open decision-making process about how to manage the city[558].

Nonetheless, not all that glittered was gold. PPPs and broader privatisation processes were accused of jeopardising public values, leading to a worrying marketisation of essential services and life[559]. Transparency, protected at legislative and constitutional levels, was often cited as one of the most endangered principles. Values like universality, continuity and quality of service, and guiding principles in the public sector like probity, honesty or integrity were also mentioned[560]. In smart cities, the alleged erosion of public values extends to privacy, security, fairness, autonomy, control over technology, human dignity and the rule of law[561].

On the empirical level, however, studies have reported conflicting results on the dangers of PPPs. On the one hand, long-term and complex PPPs have been found to bear risks of increased financial costs, inappropriate risk allocation, misallocation of resources, over-engineered products, and most importantly, the under-provision of citizens' needs[562]. This is explained by the divergence between public goals (aiming at long-term sustainability, fairness and accessibility of public services) and market logics (prioritising short-term outcomes and financial benefits)[563]. On the other hand, other studies

549 Reynaers (2014), p. 42.
550 See §3.5.
551 See Introductory Chapter, §3.2.3; Voorwinden (2021), pp. 443-444.
552 Voorwinden (2021), p. 444.
553 Id., p. 446; Sadowski et al (2019). See also Meijer et al (2018).
554 Voorwinden (2021), pp. 444, 447. See also Cardullo et al (2019b), p. 816.
555 Voorwinden (2021), p. 448.
556 Id.
557 Id.
558 Id., p. 449.
559 Id.; Ranchordás et al (2020), pp. 10 ff.
560 This taxonomy is provided by Voorwinden (2021), pp. 449-450.
561 Voorwinden (2021), p. 454.
562 See the study of the European Court of Auditors (2018); Poon (2018) (referring to Songdo).
563 Voorwinden (2021), p. 451.

have also offered a more nuanced perspective on the impact of PPPs on public values, showing that certain factors can also improve transparency and quality of service in PPPs[564].

PPPs as a tool of (data) governance in smart cities. Importantly, PPPs in smart cities can also be considered as a particular output of governance[565], where public authorities leverage the experience of the market to tackle very specific tasks in public service delivery. PPPs are not mere contractual agreements, but also entail complex social interactions that develop between its public and private components. The effectiveness of the cooperation highly depends on whether and how parties are able to reach an "optimal bundling" between their different expertise, interests and normative expectations[566]. From the perspective of personal data processing, different arrangements between public and private entities can contribute to fairer or riskier management strategies of citizens' data. A delicate question regards *who* in control of the data is, specifically who the controller under data protection legislation is. To address this issue, the legal notions of controller, joint controllers and processor in EU data protection law will firstly be examined. Then, the focus will shift to how these roles are operationalised in smart city settings and how they should be used to achieve a fair governance of urban data.

3.2. On the notion of data controller

3.2.1. An autonomous concept in EU data protection law

Rationale for Data Controllership and issues. The categories of data controller and processor aim to achieve a clear and enforceable allocation of responsibilities among the actors participating in the processing[567]. Firstly, this ensures compliance with the principles of data processing set out in Art. 5(1) GDPR, including accountability. It is indeed the controller that, pursuant to Arts. 5(2) and 24 of the Regulation, must be able to demonstrate that such principles are being respected[568]. From the perspective of data subjects, the controller is also the entity responsible for implementing individual data protection rights to information, access, rectification etc. (Arts. 12-23 GDPR)[569].

Data processing was relatively simple and straightforward when the concept of data controller was firstly formulated[570]. Big data analytics had not yet taken over and large database processing was the main way in which organisations relied on personal data, often processed for clear and straightforward purposes. However, with the advent of ICTs and big data technologies, it has become more and more difficult to identify *who* is actually responsible for a given data processing operation. Micro-technology (e.g., RFIDs, but also IoT sensors) and distributed computing have also brought changes to old responsibility paradigms[571]. At the same time, private and public bodies have been undergoing a process of diversification, embracing new models of risk distribution, decentralisation and separation of policy departments[572]. In practice, all these factors together contribute to an ever-growing difficulty in allocating data protection responsibilities in the practice.

Against this backdrop, EU data protection authorities have proposed a *factual* and *functional* concept of the data controller[573]. This means that responsibilities shall be allocated according to contextual

564 Reynaers (2014), p. 44; Voorwinden (2021), p. 452.
565 See Introductory Chapter, §3.2.1.
566 Ross (2015), p. 449.
567 Article 29 WP (2010)", p. 4; EDPB (2020), p. 9.
568 EDPB (2020), p. 8.
569 Article 29 WP (2010), p. 4.
570 Id., p. 6.
571 Id.
572 Id.
573 Id., p. 8; EDPB (2020), p. 9.

circumstances of the case at hand, having regard to the actual role played by the processing entities. To foster a consistent application of data protection legislation, this notion of the data controller was identified as an *autonomous* concept of EU law[574].

3.2.2. Legal definition and interpretation

Overview. The Working Party and the EDPB have identified the notion of data controller as an autonomous concept of EU law. Art. 4(7) GDPR defines the data controller as follows:

> 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; 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.

Firstly, there is no limitation on the kind of body that can take up the role of controller: it can be an organisation, an individual or a group of individuals[575]. When an individual employee is processing the data on behalf of his or her employer (e.g., a company or public authority), the latter should be identified as the controller[576].

Secondly, a crucial element is the factual power of the controller to determine the purposes and means of the processing[577]. Control over the data can formally stem from legal provisions, but also from a factual influence[578]. Sometimes, the law or the relevant contract may not indicate who is responsible for the processing, or the formal appointment of responsibility does not simply reflect the actual situation[579]. Hence, the entity that actually exerts an influence on the purposes and means of the processing should be identified. Useful questions in this regard include *why* the processing is taking place and *who* initiated it[580].

Thirdly, the controller should exert influence both on the purpose and means of the processing, i.e., *why* and *how* the processing is taking place[581]. Nonetheless, in practice the controller can delegate the choice of the means of the processing to the processor, which is given a certain margin of appreciation on the matter[582]. The distinction between essential and non-essential means of processing is crucial to understand which kind of decisions the processor can make on its own. On the one hand, the "essential means" are strictly intertwined with the purpose and the scope of the processing and are usually determined by the controller[583]. These could include decisions on the type of personal data that are processed, the duration of the processing, who can access the data and the categories of data subjects impacted by the processing. On the other hand, "non-essential means" revolve around more practical angles of implementation, including the choice for a particular type of hardware or software or very technical security measures[584]. These can be left to the discretion of the processor.

Importantly, it should be remembered that the notion of controller applies to a narrow (or "atomistic") conception of processing. This means that an entity can take up the role of controller in relation to a set of operations, or even to a *single* processing operation (e.g., collection, storage, access,

574 Id.
575 EDPB (2020), p. 10.
576 Id.; EDPB (2020), p. 10.
577 EDPB (2020), p. 10.
578 EDPB (2020), p. 10; Article 29 WP (2010), p. 10.
579 Article 29 WP (2010), p. 8.
580 Article 29 WP (2010), p. 8.
581 EDPB (2020), p. 13; Article 29 WP (2010), p. 13.
582 Id.
583 EDPB (2020), p. 14; Article 29 WP (2010), p. 14.
584 Id.

transfer)[585]. Also, it is not necessary that the controller actually has access to the data that is being processed[586]. If an entity outsources the processing activity and continues to have a crucial influence on the purpose and (essential) means of the processing (e.g., by adjusting the conditions of a service impacting on which data should be processed), it should be regarded as the controller, even though it will never have actual access to the data[587].

A practical smart city example. The *Enschede* decision, mentioned above[588], offers a good picture of how taking up the role of controller can be problematic in the smart city context. Indeed, the Enschede Municipality rejected its role of controller under the GDPR[589]. It claimed that, although the contract with the technology provider designed it as the principal body responsible for the processing, such an appointment had to be kept distinct from the concept of data controller in the GDPR. Also, the Municipality held that the factual circumstances indicated that it was not, or was only jointly, responsible for the processing. For instance, the ways in which data were collected and processed were mainly determined by the processor (i.e., the Bureau RMC). Moreover, the Municipality indicated that it had no access to the data and no say on whether the Bureau RMC could transfer or sell data to third parties. Finally, it also stated that the CityTraffic Privacy Protocol (the privacy policy drafted by the Bureau RMC) identified the latter as the controller.

However, the AP did not accept the Municipality's arguments, based on a factual assessment of the situation. It found that, although the Bureau had a certain margin of discretion on *how* the processing was taking place, the Enschede Municipality was the one determining the *purposes* of the processing. It was the one that first decided to initiate the Wi-Fi tracking project and decided how many sensors had to be installed in the city centre, and where.

The Municipality could not invoke the fact that it had no direct access to rule out its responsibility as controller, as also clarified by the CJEU case law on the issue[590]. In fact, the Municipality had the power to impose conditions and means of the processing to the Bureau RMC. The Bureau had the right to sell the collected data only because it was entitled to an exit file (without personal data), i.e., a copy of the data that could be used by anyone having requested access. This operation would actually correspond to further processing – falling outside the scope of the Wi-Fi tracking experiment – for which the Bureau would take up the role of controller.

Lastly, even if the privacy policy named the Bureau as the controller for the processing of MAC addresses, this did not mean that it was a controller for every other processing operation. Various processing activities could indeed be distinguished. Although the Bureau assumed the role of controller specifically for the processing of MAC addresses, this did not mean that (i) the city was not a controller as well for that operation, and (ii) the Bureau was also a controller for other processing operations. Taking all of this into consideration, the AP found that the Municipality qualified as a controller for the whole Wi-Fi tracking initiative.

---

585 EDPB (2020), p. 15.
586 CJEU, *Wirtschaftsakademie,* judgment of 5 June 2018, Case C-201/16, §38; CJEU, *Jehovah's witnesses,* judgment of 10 July 2018, Case C-25/17, §69; CJEU, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, judgment of 29 July 2019, Case C-40/17, §69.
587 EDPB (2020), p. 16.
588 See Chapter I, §3.3.3.
589 Autoriteit Persongegevens (2021), §3.2.4.
590 Cf. CJEU, *Breyer*, §43.

Overall, this case shows how assuming the role of controller in smart city projects comes with high responsibilities, which both private and public actors may try to dodge. Legal mechanisms to ensure that accountability is ensured in such initiatives will be explored down below[591].

3.3. On the notion of joint controllership

3.3.1. Legal definition and interpretation

Overview. Joint controllership is regulated in Article 26 GDPR, which provides that "[w]here two or more controllers *jointly* determine the purposes and means of processing, they shall be joint controllers" [emphasis added]. Here, "jointly" shall be understood as "together with" or "not alone", even though such interactions may emerge in a variety of ways[592]. As for the identification of the controller, the existence of a joint controllership scenario shall be appreciated based on a factual, rather than formal, assessment[593]. For instance, the EDPB reiterated that "the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers", especially when the processing operations could be separated and carried out without the intervention of one or the other party. Also, the existence of a mere mutual commercial benefit should not be regarded as sufficient to identify a situation of joint controllership[594].

Forms of joint participation. Joint participation to the processing can take two forms, depending on the existence of (i) a common decision; or (ii) converging decisions of two or more parties regarding the purposes and the essential means of the processing. The first scenario coincides with the most common understanding of joint controllership, where the parties share a common intention in defining the essential elements of the processing.

On the contrary, joint participation through converging decisions results from the case law of the CJEU (see paragraphs below). Decisions are converging when "they complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing"[595]. However, even when purposes are jointly determined, the CJEU does not consider that all operators involved in the processing necessarily share the same amount of responsibility[596].

Processing purposes may be considered inextricably linked when controllers share a mutual benefit stemming from the processing itself[597]. In *Fashion ID*, for instance, the Court indicated that a website operator participates in the determination of the purposes and means of the processing when it inserts a social plug-in (e.g., a Facebook like button) on its own website to make its goods more visible on social networks[598]. The social plug made it possible to transfer personal data of website visitors to Facebook, although Fashion ID had no control over the processing of transmitted data.

The Court considered that by embedding a social plug-in in its website, Fashion ID was jointly participating with Facebook in the processing of visitors' data. Nonetheless, it was responsible only for the collection and disclosure phase, and not for further processing performed by Facebook. Fashion ID established the means of the processing by installing the plug-in, which allowed for the transfer of

591 See below §3.5.
592 EDPB (2020), p. 17; Article 29 WP (2010), p. 14.
593 Id. Cf. §3.3.1.
594 EDPB (2020), p. 20.
595 EDPB (2020), p. 18.
596 CJEU, *Wirtschaftsakademie,* §43; CJEU, *Jehovah's witnesses,* §66; CJEU, *Fashion ID,* §70.
597 EDPB (2020), p. 19.
598 CJEU, *Fashion ID.*

visitors' data regardless of them being Facebook users[599]. As for the purposes, the Court found that both Fashion ID and Facebook shared an economic interest in the processing. On the one hand, Fashion ID aimed at increasing publicity for its goods; while on the other, Facebook could use the data for its own commercial purposes (e.g., users' profiling)[600].

Previously, similar conclusions had been reached in the *Wirtschaftsakademie* and *Jehovah's Witnesses*. In the former case, the Court held that fan page administrators of a social network can be held liable with the social media provider when data protection rules are infringed. By creating a fan page, the administrator allows the social media network (Facebook) to install cookies on the device of the fan page visitor, regardless of whether said individual has a Facebook account[601]. The administrators had to choose specific parameters to produce statistics on its target audience, according to criteria established by Facebook.[602]. Therefore, the Court considered that the administrator of a Facebook fan page participated jointly with the social media provider to defining the purposes and means of the processing[603].

In *Jehovah's Witnesses* instead, the Court was asked whether the individual members of a Jehovah's Witness Community could be considered joint controllers with their broader religious community for the data they collected in door-to-door preaching activities. The Court found that the collection of the personal data of contacted persons and their subsequent processing pursued the goals of the wider Jehovah's Witnesses Community, namely spreading its faith. The Community also knew about the purposes of the processing and coordinated the preaching activities of its members[604]. Therefore, it was considered a joint controller with its members, even though it may not have access to the collected data or established written instructions for the processing[605].

3.3.2. General issues in smart environments

Issues in a broad notion of joint controllership. Ensuring a high level of protection for data subjects may in principle favour a broad conception of joint controllership. This extensive interpretation seems to give more importance to the *interests* rather than to the *purposes* of the processing, something which may be more coherent with the big data paradigm[606]. Nonetheless, this more elusive and holistic approach could also be counterproductive for data subjects. A lack of clear allocation of responsibilities may indeed be leveraged by controllers to elude their data protection obligations.

Specifically, this issue becomes critical in smart environments[607], and this is only likely to intensify in light of the extensive interpretation of the notion of data controller made by CJEU[608]. While the Court aims to ensure a high level of protection of fundamental rights[609], its approach may also translate in a very low threshold for parties to be labelled as (joint) controllers[610]. In turn, these may end up being overburdened by compliance obligations, including those stemming from the activities of their partners.

---

599 Id., §78.
600 Id., §80.
601 CJEU, *Wirtschaftsakademie,* §35.
602 Id., §36.
603 Id., §39.
604 CJEU, *Jehovah's witnesses,* §71.
605 Id., §73.
606 See Moerel et al (2016). Cf. Chapter I, §3.3.1.
607 Article 29 WP (2010), p. 18.
608 Chen et al (2020), p. 284; Ducuing et al (2020), §3.; Zalnieriute et al (2020), p. 867.
609 CJEU, *Google Spain,* §34; CJEU, *Wirtschaftsakademie,* §28; CJEU, *Jehovah's witnesses,* §66; CJEU, *Fashion ID,* §66.
610 Zalnieriuteet al (2020), p. 871.

To avoid these risks, the Court tries to limit the qualifications of joint controllerships *only to specific operations* (i.e., fragmented approach)[611]. Controllers' responsibilities are thus excluded for prior or subsequent activities that actually fall within the exclusive competence of joint controllers. In this sense, the Court tries to mitigate such a broad notion of data controller with a "fragmented" approach to joint controllership.

Issues in a fragmented interpretation of joint controllership. This meticulous allocation of responsibilities avoids that entities are held liable for processing operations for which they actually have no real information and control[612]. It also averts the risks of negative conflicts of competence among data controllers, avoiding that "making everyone responsible means that no-one will in fact be responsible"[613]. However, the scholarship has criticised this approach for being too casuistic and not supported by a correct reading of the GDPR[614]. Specifically, the step-by-step approach to joint controllership has been regarded as not being sufficiently protective of individual data protection rights, especially in smart environments[615]. It was contended indeed that such "'fragmentation' ultimately jeopardises the ability to recognise the societal risks posed by complex, networked, personal data processing systems", as in the case of powerful service providers (e.g., Facebook)[616]. It may allow controllers to take advantage of the services of influential companies, while turning a blind eye to their reckless data processing strategies.

Furthermore, the interpretation of the CJEU is problematic with regard to essential notions of data processing, i.e., its purpose. Critically, the CJEU is not clear on the notion of purpose and how this relates to the qualification of a controller[617]. In *Fashion ID*, it held that Facebook and the website owner could be defined joint controllers not because they had determined the *purpose* of the processing together, but because they shared an economic *interest* in the operation. Arguably, the Court seems to conflate the wider concept of "interest", and the more technical one of "purpose" of the processing[618]. In fact, while the purpose represents the specific objective that is pursued with a given processing activity, the interest is the "broader stake" that a controller may have in carrying out the processing[619]. Arguably, such a vague characterisation of purpose as simple "economic interests" may not actually meet the standards of precisions required by Art. 5(1)(b) GDPR in this regard[620].

In smart houses. Issue of controllership in the IoT domain have already been explored in the more confined context of smart houses. Here, some scholars have promoted a more holistic and "layered" approach to responsibility allocation in data protection. They argued that duties of care cannot be distributed in an all-or-nothing fashion[621]. Rather, smart environments rely on a "collaborative involvement" of manifold actors with different roles and levels of control over data and the overall functioning of the IoT system.

---

611 Id.
612 Ducuing et al (2020), §5.
613 Opinion of Advocate General Bobek *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, §92.
614 Ducuing et al (2020), §3.
615 Zalnieriute et al (2020), pp. 874 ff.
616 Id., pp. 873, 875.
617 Ducuing, Schroers (2020), §5.
618 Cf. EDPB (2020), p. 20 (stating that mere mutual commercial benefit is not sufficient to identify a situation of joint controllership).
619 Cf. Chapter I, §3.3.1.
620 Ducuing et al (2020), §5.
621 Chen et al (2020), p. 290.

This diversified approach to responsibility is also supported by the Working Party. In smart environments, it is prone to assign to different stakeholders a controllership role in relation to specific aspects of the processing. Firstly, device manufacturers who design the "thing" and install the operating software, determine the amount and frequency of data to be collected, as well as when and to whom these are transmitted. Hence, they should be qualified as controllers for the processing of data generated by the device[622]. Social platforms towards which data are transferred are instead responsible for further profiling operations carried out with IoT data[623]. Third parties also develop applications to access sensor data through APIs. If data subjects install these applications in their devices and the transferred data is not properly anonymised, such app developers should be the designated controllers for the processing consisting of access to collected data[624]. Similarly, developers of platforms built to centralise data gathered by different IoT devices (especially smartphones and tablets) should also be deemed controllers when they process data for their own purposes[625].

In this perspective, it can be argued that software developers have *schematic control* of the system, as they defined the structure of the data and the protocols used to transmit data between nodes[626]. Device manufacturers have an *input control* because they determine which data are collected and transferred[627]. Developers of apps installed in IoT devices have an *interpretative control* over the data, as they establish the criteria according to which data patterns are uncovered and operationalised in decision-making[628]. Lastly, users of IoT applications (individuals, but also entities in the wider smart city context) have *operational control* as they choose which components or functionalities should be used[629].

Responsibility allocation in smart cities. These considerations are useful for understanding how complex it is to distribute responsibilities over data in IoT systems that are as big as entire cities. Importantly, the GDPR tends indeed to trace clear-cut lines between who should be liable for the processing and who should not, but also foresees mechanisms to manage different layers of responsibility between controllers. Art. 26(1) of the Regulation provides that joint controllers may rely on bespoke arrangements to determine their respective responsibility vis-à-vis the data subjects, although the latter remain free to exercise their right to each of the controllers. Regrettably, the drafting of such legally binding documents does not seem to be mandatory for the emergence of a joint controllership[630]. This means that two or more entities can exercise joint controllership on the processing without signing any binding (contractual) document beforehand.

In smart cities, the solution foreseen by Art. 26 GDPR shall be leveraged as much as possible to clarify the allocation of respective responsibilities. This would allow public authorities to exclude their direct involvement in further marketing processing conducted by technology providers, activities that do no not fall within their general interest missions. At the same time, however, these instruments should not enable public authorities to altogether ignore the societal risks associated with the processing in smart environments. For instance, city authorities should not think of entering into partnership with service providers that – once in possession of city data – rely on reckless data

622 Article 29 WP (2014a), p. 11; Chen et al (2020), p. 290; Recital 78 GDPR simply *encouraging* but not *obliging* manufacturers to take into account data protection obligations in their work).
623 Article 29 WP (2014a), p. 12.
624 Id.
625 Id., p. 13.
626 Chen et al (2020), p. 290.
627 Id.
628 Id.
629 Id.
630 Id., p. 291.

monetisation practices for their own commercial purposes. Similarly, they should not choose providers that do not take into account data protection obligations in developing their sensor technology[631]. Legal instruments facilitating this challenging task will be explored down below[632].

3.4. On the notion of data processor

In the GDPR. A processor is defined in Article 4(8) as a natural or legal person, public authority, agency or another body that processes personal data on behalf of the controller[633]. Two basic conditions are necessary to qualify as processor: (i) being a separate entity in relation to the controller; (ii) processing personal data on the controller's behalf[634]. Firstly, the controller shall decide to *delegate* the processing of personal data to an external organisation (departments and employees within the same company not being apt to qualify as such)[635]. Secondly, processing needs to be done on behalf of the controller but not under its direct authority or control: the processor is simply tasked with implementing the instructions of the controller about the purpose and essential means of the processing. It retains nonetheless a certain degree of discretion in deciding how to achieve the set goals[636]. Lastly, the processor cannot perform processing outside the scope of the instructions given by the controller, or for its own purposes. Art. 28(10) indicates that the processor may be sanctioned for such behaviour and shall be considered as a controller for the operations carried out on its own initiative. The lawfulness of such further processing shall be assessed separately pursuant to Arts. 5-9 GDPR[637].

Legal framework of controller-processor relationships. Art. 28(3) GDPR states that the activities of a processor are governed by a contract or other Union or national law. These legal bases are binding on the processor and should lay down the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

In this regard, the Working Party addressed the situation of standard services and contracts offered by service providers acting as processors. Sometimes, big service providers will set up such standardised documents, *de facto* imposing the conditions of the processing on small data controllers[638]. In the platform economy, the imbalance of contractual power between these actors may be significant. However, the Working party has clarified that such a situation cannot be invoked by controllers to accept clauses and terms of contract that are not compliant with data protection law[639]. This is an important warning for smart cities that are increasingly privatised and delegate the provision of their urban services to big technology corporations that tend to unilaterally impose terms and conditions of the processing[640].

Also, the EDPB indicated that not every service provider that processes personal data while delivering a service can be labelled as a "processor" under the GDPR[641]. A factual analysis should

631 Cf. Recital 78 GDPR.
632 See below §3.5.
633 EDPB (2020), p. 24; Article 29 WP (2010), p. 25.
634 EDPB (2020), p. 24.
635 Id.
636 Id.
637 Cf. Article 29 WP (2010), p. 25.
638 Article 29 WP (2010), p. 26.
639 Id.
640 See, e.g., the case of Google's system Flow in Taylor (2019).
641 EDPB (2020), p. 25.

always be performed. When the processing operation does not constitute a key element of the proposed service, the provider may independently define the purposes and means of the processing, and could be qualified as a separate controller[642]. In the smart city context, again, this is important to highlight how private technology providers should be held responsible for additional profiling and marketing processing carried out with the data collected while operating public services in the city.

3.5. Preferred solutions for smart city public-private partnerships

3.5.1. Problematic situations and trends

Data control in smart cities. Empirical research has shown that PPPs pose difficult scenarios in terms of responsibility allocation in smart cities. When public authorities, often lacking the necessary expertise, choose to process data out-of-house, they need to rely on private companies that will likely try to maximise the economic value of data[643]. In this sense, three situations are identified as particularly problematic: (i) a joint data controller taking the role of data processor; (ii) joint data controllers; (iii) data controller outsourcing to a data processor[644].

In a situation of factual joint controllership, it can happen that one of the actual controllers downsizes its role in the processing to present itself as a processor[645]. In the smart city context, this appears to be a standard practice of technology providers, which attempt to avoid controllers' responsibilities when stipulating agreements with local authorities[646].

In other cases, the involved parties may decide to formalise the joint controllership, often with joint control agreements (JCAs)[647]. Sometimes, mapping different risks and respective responsibilities may not be straightforward, and conflicts may arise in the process. Also, joint control may not always be the right solution for smart city services. When the controllers do not have the same processing goals (*mutatis mutandis,* the same purposes or interests), each party will have to assume the role of controller separately and perform its own DPIA[648].

In controller-processor scenarios, conversely, one of the key issues is the provision by the processor of the necessary information for the controller to comply with its data protection obligations[649]. For processors, giving such information will often entail the risk of disclosing proprietary processing information[650]. To solve the issue, some local authorities have drafted standardised data processing agreements, but private parties have been resistant to signing such documents[651]. Public authorities are trying to improve these negotiating processes, and, on their part, private companies are learning to draw up such agreements themselves[652]. It should also be considered that large smart city projects may entail complex operations, with long processing chains (potentially also involving sub-processors). The longer the chain, the more difficult it will be for the public controller to acquire meaningful information to comply with GDPR obligations, thus diminishing the overall transparency of the processing[653].

---

642 Id.
643 Vandercruysse (2019), p. 558.
644 Id.
645 Id.
646 Id. See also Vandercruysse et al (2020), p. 10.
647 Vandercruysse (2019), pp. 558; Van Zeeland et al (2019), p. 5.
648 Vandercruysse (2019), pp. 558.
649 Id., p. 559.
650 Id.
651 Id. From a public law perspective, this may also be a problem for the overall transparency of the project, see Voorwinden (2021), p. 452.
652 Vandercruysse (2019), pp. 559.
653 Voorwinden (2021), p. 457.

Against this backdrop, some cross-cutting issues were identified: avoiding responsibility over the data; lack of information in the processing chain; lack of awareness of smart city actors regarding legal responsibilities and respective margin of manoeuvre[654]. To address these problems, some recommendations have also been put forward: (i) including processing agreements in the tenders; (ii) including information disclosing agreements for (sub)processors in the public procurement process as well; (iii) higher partners in the processing chain should leverage their contractual power; (iv) for joint controllers, define respective responsibilities in JCAs in a decisive manner; (v) raise awareness in public procurement divisions about data protection problems[655]. For this, an obligation to submit the project to a participatory DPIA should be encouraged, as explained below[656]. Overall, such recommendations follow a more fragmented conceptualisation of the responsibilities in the smart city context. Nonetheless, legal mechanisms should determine allocation of responsibility, and should also be used to grasp and tackle the broader, societal consequences of ubiquitous urban processing.

3.5.2. Controllership and commercial repurposing

Conflicting interests in PPPs. When personal data is collected in the context of public service delivery, or to satisfy the general interest of improving the urban environment, citizens may have an expectation that their data continues to be used for the public good[657]. Of course, PPPs do jeopardise this assumption. Nowadays, private technology and service providers have strong interests in maximising the commercial value of the data that they have processed while providing for public services. From the perspective of public authorities – that are bound to pursue the general interest – such phenomenon should be resisted. Data commercialisation may indeed lead to discriminatory practices towards disadvantaged citizens and communities, for instance in the domain of insurance and credit scoring.

Which controllership scenario can avoid commercial data repurposing? Arguably, data rewards should be linked to data responsibilities[658]. It does not seem fair for a party to avoid responsibilities as a controller and then still get access to data to commercialise it. In smart cities, this poses many difficulties as private technology providers are usually the ones having direct access to the data, because they are the ones who usually perform processing activities. To avoid commercial repurposing of data, different legal solutions should then be experimented, regardless of the private party being a controller or a processor.

When the private technology provider is a joint controller, the JCA shall forbid the commercial reuse of the data. In this way, the private party should be bound to the initial purpose of the processing (i.e., public service delivery) and should not be allowed to process the data for an incompatible purpose (Art. 5(1)(b) GDPR). If the company decides nonetheless to sell the data, it will be the only controller for this further processing and the lawfulness of the latter shall be assessed separately. The private entity could attempt to repurpose the data, but this operation would unlikely pass the multi-criteria assessment set out in Art. 6(4) GDPR. Therefore, it could be held liable for violation of GDPR principles.

Similarly, when the technology provider is a processor, the contract with the public authority should hamper further data exploitation. Also, the agreement may avoid giving the private party entitlement to have an exit file of the data collected, as happened in the *Enschede* case. Considering the weakness of the anonymisation techniques used in that processing system, even those "anonymised" datasets could

654 Vandercruysse (2019), p. 560.
655 Id. p. 559.
656 See §4.5.
657 See the arguments in Chapter VI.
658 Vandercruysse (2019), pp. 559.

bring negative consequence for data subjects if further commercially exploited. In this scenario, the processor having access to the data could certainly use it for its own commercial purposes. However, it would incur a two-fold risk. On the one hand, the processor could likely be held liable for violation of the purpose limitation principle, that would not easily allow commercial reuse of data collected in the context of public service delivery (Arts. 5(1)(b) and 6(4) GDPR). On the other, it could also be sanctioned for violation of the instructions given by the controller (Art. 28(10) GDPR[659].

4. Data protection impact assessments in smart cities

Introduction and outline. In these two chapters several data protection issues in smart cities have so far been examined, ranging from the very applicability of data protection law to grounds of data collection, the purpose limitation principle and data controllership. Approaching the end of this investigation, it is time to focus on which tools are instead available to address the risks that arise with intensive data processing in smart cities. In this sense, central may be the role of data protection impact assessments (DPIAs). The potential impact of this instrument may indeed cover not only legal aspects of smart city processing, but also ethical and societal ones.

The analysis will be articulated as follows: preliminarily, a glimpse of the risk-based approach which informs the structure of the GDPR and inspires the rationale of DPIAs will be sketched[660]. Subsequently, an overview of major provisions relating to DPIAs as regulated in the GDPR will be provided, focusing on aspects that may be of major interest for the smart city setting[661]. To further understand the logics behind these provisions, insights will be drawn from the field of environmental law, where similar governance mechanisms have already been explored[662]. The investigation will go beyond the strict legal domain to examine how the instrument of the DPIA could be leveraged to deal with a number of societal and ethical questions that underline large smart city processing. To this end, various impact assessment models (i.e., surveillance impact assessments, HRESIAs impact assessments and algorithmic impact assessments) will be scrutinised[663].

Lastly, it will be investigated how the tool of DPIAs may be concretely leveraged in smart cities to achieve a more democratic management of big data processing in the city. For this reason, firstly I will analyse the rationale of Art. 35(9) GDPR, which foresees a non-mandatory mechanism to involve data subjects in decisions about the envisaged processing[664]. Secondly, the ECtHR's case law on environmental law will be scrutinised and used to argue for a more extensive application of participatory DPIAs in smart cities[665].

4.1. Background: The risk-based approach in the GDPR

An enforcement model based on risk management. In the GDPR, the risk-based approach is the main enforcement model, which mainly builds on data controllers' self-rule[666]. Many are indeed the provisions in the Regulation where the risk-based approach is inscribed[667].

Gonçalves observes that the integration of a risk-based model in data protection is "part of a societal process whereby the impacts of technological development are increasingly perceived through

[659] It appears so by the initial clause of the provision: "Without prejudice to Articles 82, 83 and 84, (…)".
[660] See §4.1.
[661] See §4.2.
[662] See §4.3.
[663] See §4.4.
[664] See §4.5.1.
[665] See §4.5.2.
[666] Gonçalves (2020), p. 140.
[667] See Arts. 25, 30, 32, 33, 35, 36 GDPR and the accountability principle in Arts. 5(2), 24 GDPR.

the *angle of risk*, and regulated accordingly"[668]. Generally speaking, risk management strategies inform decisions involving the distribution of resources, in such a way that a greater portion of the assets can be devoted to the situations likely to be more heavily impacted by the occurrence of the risk event[669]. From the regulatory perspective, the integration of risk management practices in data protection mainly translated into the adoption of a procedural approach, devoted to the regulation of the different stages of the processing and the definition of the powers and tasks attributed to different subjects involved in the processing[670].

Reception in the legal scholarship. The incorporation of a risk-based stance in the GDPR was hit by mixed reactions in the legal domain. Various concerns were raised on the fact that a risk-based approach would discard a right-based one in the field of privacy and data protection. Indeed, the two methodologies had traditionally been seen as antagonistic[671], being these two forms of value-based judgements relying on different logics.

On the one hand, the risk-based approach seems to be informed by a classic risk-benefit (or utilitarian) analysis, where all different interests involved in the balancing are placed at the same level[672]. Procedural obligations for data controllers should be adjusted based on the increasing magnitude of the risks associated to the processing activities undertaken.

On the other hand, the rights-based approach does not accept the idea that the balanced interests can have the same weight and instead assumes that fundamental rights will always prevail on interests of a lower order[673]. The right to data protection affected by the processing deserves a uniform set of safeguards, regardless of the risks posed by the operations in specific situations.

In this perspective, some scholars have been afraid that welcoming a risk-based approach in the GDPR would result in uneven levels of protection, with the danger of some core principles of data protection not being applied in low-risk instances of processing[674]. Although a risk-based approach is by definition modular and scalable, the Working Party refused to consider it as an alternative to the right-based one[675].

Some situations of high risk to fundamental rights certainly call for stricter procedural obligations on the part of the controllers and demand for more technical and organisational resources (Arts. 35 and 36 GDPR). However, core principles of data protection still offer a minimum standard of protection which applies to any data processing activity.

As a matter of fact, a different solution would not be compliant with Art. 52(1) CFREU, which provides that any interference upon the fundamental rights protected should not jeopardise their essence. The structure of fundamental rights typically comprises a "core" (or essence in the wording of the Charter) and a "periphery" or "penumbra"[676]. If the concept of risk (including that of interference) can exclusively impact on the penumbra of the right[677], it follows that the risk-based approach can logically produce its effects only outside the purview of the essence of the right to privacy and data protection.

668 Gonçalves (2020), p. 145. [emphasis added]
669 Id., p. 143.
670 Mantelero (2019), p. 7.
671 Gellert (2016), p. 481.
672 Mantelero (2019), p. 8.
673 Id.
674 Gellert (2016), p. 483; Gonçalves (2020), p. 143.
675 Article 29 WP (2014c), p. 2.
676 Demetzou (2020), p. 9.
677 Id., p. 10.

Risk management and legal methodologies coming together: The idea of risk mitigation. One idea that brings together the risk-based approach and the rights-based one is that of *risk mitigation* (or safeguards). Risks to fundamental rights stemming from data processing need to be circumscribed by the provision of additional safeguards, which become an integral component of balancing mechanisms in data protection. Because legal and technical safeguards can limit the scope and invasiveness of the interferences, these need to be carefully assessed in the context of proportionality[678]. The provision of specific safeguards is a factor to be considered in the act of balancing[679], as they allow to achieve a fair equilibrium between the needs of safety and security, and those relating to the protection of fundamental rights: instead of having zero-sum games (i.e., trade-offs), we need to ensure that "more security measures that impact civil rights on one side of the scale, require more effective legal safeguards on the other side"[680].

Risk mitigation obligations in the GDPR. From the procedural standpoint, different risk mitigation obligations are imposed to data controllers by the GDPR according to the magnitude of the risk (appreciated through the lens of likelihood and severity[681]). In this scalable model of protection, Mantelero discerns three assorted layers of risk management provisions[682]. Firstly, there are general obligations regarding data security (Art. 32 GDPR), applicable to any data processing operation. Secondly, when high risks to fundamental rights emerge in this first assessment, data controllers are asked to perform a further mandatory and documented procedure, the DPIA (Art. 35 GDPR). Finally, if some risks are likely to persist even after the DPIA, a third obligation is represented by the prior consultation with the Supervisory authority (Art. 36 GDPR). In the following sections, obligations relating to DPIAs will be examined.

4.2. Data protection impact assessments in the GDPR

DPIAs in the GDPR. DPIAs play a central role in identifying significant risks for privacy, data protection and other fundamental freedoms in the life cycle of data, and constitute "process for building and demonstrating accountability"[683]. When controllers deem that their processing activities – especially those involving new technologies – are likely to result in high risks to the rights and freedoms of individuals, they shall conduct a DPIA prior to the intended processing. In specific instances, the Regulation establishes a presumption of the necessity of a DPIA, namely in cases of:

> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
>
> (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
>
> (c) a systematic monitoring of a publicly accessible area on a large scale[684].

678 CJEU, *Digital Rights Ireland*, §66.
679 See Hildebrandt (2013), p. 372 (distinguishing trade-offs and balancing). *Compare* EDPS (2017a), p. 5.
680 Hildebrandt (2013), p. 372.
681 Recitals 75-76 GDPR.
682 Mantelero (2019), p. 9.
683 Article 29 WP (2017a).
684 Art. 35(3) GDPR. In smart cities, see Bu-Pasha (2020); Vandercruysse (2019).

Concerning the contents of the DPIA, the GDPR foresees some minimum requirements for the assessment. Indeed, Art. 35(7) of the Regulation provides that the assessment shall contain at least:

> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
>
> (b) an assessment of the *necessity* and *proportionality* of the processing operations in relation to the purposes;
>
> (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
>
> (d) the measures envisaged to address the risks, *including safeguards*, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned [emphasis added].

DPIAs as a tool to balance risks and rights in data protection. From the wording of Art. 35, we understand that the DPIA represents one of the privileged contexts to balance risks and rights in the EU data protection system. While only Art. 35(7)(b) GDPR explicitly recalls the concepts of necessity and proportionality, all the listed required contents of the assessment presuppose some kind of balancing. On the one hand, letters (a) and (c) embody what Gellert calls "*data legitimacy*", which refers to the balancing of risks and rights entailed in the choice of the legal basis for the processing[685]. On the other, the tasks listed in letters (b) and (d) are closely intertwined and shift their focus on the *means* of the processing. Referring to "*data quality* principle" indeed, the processing may comply with the principles of necessity and proportionality only insofar as technical and legal safeguards are provided to circumscribe the scope and impact on data subjects' rights[686]. With due consideration of the hierarchy of the sources of EU law, it is necessary to recall that this proportionality assessment should be carried out in light of the procedural steps set out in Art. 52 of the Charter.

Weaknesses of the DPIA model. As outlined in the Regulation, one of the shortcomings of the DPIA process is that little or no space is devoted to the assessment of wider *social* and *ethical* impacts of the processing[687]. This is of course coherent with the individualistic focus that still informs EU data protection law and appears increasingly obsolete with regard to the challenges of big data environments[688]. However, the inclusion of the public in the impact assessment may fill this gap and give a more collective dimension to balancing processes in data protection[689]. This would allow to consider not only technical security measures, but also community-based insights, which may also affect the outcome of the balancing process[690]. As will be covered below, the issues of participatory and social-oriented impact assessments have traditionally been dealt with in the field of environmental law, which presents several links with privacy and data protection.

4.3 From environmental impact assessments to privacy and data protection

From EIAs, to PIAs and DPIAs. While DPIAs constitute one of the main novelties of the system of the Regulation, similar instruments have already been experimented both in the fields of privacy and environmental governance. Indeed, DPIAs find their direct predecessors in privacy impact assessments (PIAs) and environmental impact assessments (EIAs)[691]. Arguably, environmental law was one of the first policy areas to implement preventive procedures designed to assess the risks and societal implications of large-scale projects. This instrument later inspired the adoption of PIAs in common

685 Gellert (2016), p. 485.
686 Id.
687 See Mantelero (2018); MacMahon et al (2020).
688 Mantelero (2016).
689 Mantelero (2018), pp. 756, 758.
690 Mantelero et al (2021), p. 21; Council of Europe (2017).
691 Van Dijk et al (2016), p. 287; Gonçalves (2020), p. 144; Binns (2017), pp. 22-25. On the connection between privacy and environmental law literature, see Galetta et al (2014); Froomkin M (2015).

law countries, from the 1990s onwards[692]. Clearly, there is a methodological continuity bringing together EIAs, PIAs, and now DPIAs. This also shows how the governance of risk in the environmental and big data share common issues[693].

Data Protection Impact Assessments: combining risk-based and human rights approaches. Despite the conceptual and historical links, DPIAs may not always be the best instrument to assess the societal implications of large-scale projects, which once was the focus of EIAs. The attempt of combining risk-based approaches with the human rights perspective in DPIAs is indeed visible in the proliferation of templates for the industry, where human rights like privacy and data protection are almost exclusively quantified through the technical notions of "impact" (or severity), "likelihood", "risk level"[694]. These parameters, however, seem to be ill-suited to deal with values and principles, which are by nature incommensurable and thus inapt to be quantitatively measured. In fact, the methodologies embedded in these templates often fail to justify the choice of certain (mathematical) measurement scales to assess the risks to fundamental rights[695].

A legal approach: Turning to the ECtHR's case-law in environmental law. Little room is devoted to pure legal and ethical discourses involving value-risk balancing. As far as the right to private life is concerned, van Dijk proposes to draw inspiration from the ECtHR's case-law in environmental law, where legal methods to deal with risks to human rights have been devised. In these cases, the environmental impacts caused by (technological) projects on individuals' health and homes are framed by the Court as interferences on the right to private life[696]. In performing the proportionality assessment, the Court considers that the mediation between opposing rights and values can be first achieved by some *procedural* obligations, including that of performing an impact assessment[697]. In the environmental domain, this results in the provision of *positive* obligations for public authorities.

Therefore, risks to fundamental rights are addressed by producing knowledge about events that may impact on individuals' rights[698]. These procedural obligations are meant to lay down the basis for a more substantial assessment of the issues at stake. Such knowledge can indeed become contestable in the adversarial context of a court of law and loose its veil of objectivity when underlying normative issues are examined[699]. In the case-law of the ECtHR, these procedural obligations are instrumentalised to give the public an effective chance to contest authorities' decisions in a court of law. Nonetheless, as we will see further below, this jurisprudence seems to have recently developed to also include a wider right to participation in the decision-making process[700].

---

692 Wright et al (2012) define PIAs as follows: "a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts" (p. 5).

693 Van Dijk et al (2016), p. 288 (stressing that environmental regulation has been one of the first domains of convergence of law and science).

694 Van Dijk et al (2016), p. 293.

695 Id.

696 See, e.g., ECtHR, *Hatton v. the United Kingdom*, judgment of 8 July 2003, App. no. 36022/978; ECtHR, *Taşkin v. Turkey*, judgment of 30 March 2005, App. no. 46117/99; ECtHR, *Giacomelli v. Italy*, judgment of 2 November 2006, App. no. 59909/00; ECtHR, *Saadi v. Italy*, judgment of 20 February 2008, App. no. 37201/06; ECtHR, *S. and Marper v the United Kingdom*; ECtHR, *Tătar v. Romania*, judgment of 27 January 2009, App. no. 67021/01. Van Dijk is skeptical about applying the solutions developed in this case-law to pervasive technologies like the IoT. See van Dijk (2016), p. 299, note 66.

697 ECtHR, *Giacomelli v. Italy*, §94; ECtHR, *Tătar v. Romania*, §112.

698 van Dijk (2016), pp. 294, 299.

699 Id.

700 See §4.5.2.

4.4. Broadening the scope of impact assessments

DPIAs: A strict perspective? With the "ethics turn" in research and regulation on digital technologies, privacy and data protection scholars acknowledged the highly individualistic focus of existing impact assessments[701]. Risk monitoring in data protection is mainly turned to the evaluation of potential negative consequences for *individual* data subjects, with barely any reference to broader ethical values (e.g., autonomy, human dignity, beneficence, social justice, equality, solidarity, digital citizenship)[702]. Against this backdrop, broadening the scope of DPIAs under Art. 35 GDPR may be useful to incorporate ethical values and collective interests[703], as argued by the Working Party[704]. In its Opinion on DPIAs indeed, it clarified that the reference to the "rights and freedoms" of data subjects mainly involves the rights to data protection and privacy but may also concern other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion[705]. A more "fluid" reading of Art. 35 GDPR is thus apt to open up the way to more well-rounded technology impact assessments. Scholars have already explored this path, developing a wide range of social and ethical-oriented impact assessments models which may be useful in smart cities. These will be explored in the following subsections.

4.4.1. Surveillance impact assessments

Surveillance Impact Assessments. Surveillance Impact Assessments (SurvIA) aim to address specific risks associated with monitoring technologies, like financial or economic consequences for individuals, or categorical discrimination in society, social exclusion, hindering of social and political interaction (i.e., chilling effect)[706]. Governing surveillance requires going beyond individual privacy values[707], and in this perspective SurvIAs attempt to involve diverse stakeholders to assess the necessity and proportionality of proposed surveillance systems, how they could be designed and tested, whether the risks for the wider public are acceptable[708]. SurvIA developers argue that these assessments could open up surveillance to public scrutiny and discussion, if these were mandatory to authorise the certification and deployment of the technology[709]. Nonetheless, important criticism seems to stand in the way of wider adoption of this model. Among most-cited drawbacks, we find: curb of technology innovation, difficult implementation in the security and law enforcement domains, intellectual property rights impeding a public discussion of the technologies at stake[710].

4.4.2. HRESIA impact assessments

Human Rights, Ethical and Social Impact Assessment-HRESIA Impact Assessments. HRESIA impact assessments are built upon the comparison between previous impact assessment models (e.g., PIAs; social impact assessments, SIAs; ethical impact assessments, EtIAs; human rights assessments, HRIAs)[711]. The main goal here is to create a more streamlined procedure to evaluate the individual and

[701] Raab (2020), pp. 2, 9; Mantelero (2018), p. 758. Specifically, the "ethics turn" in research and regulation entailed a growing interest in wider ethical, societal, political impacts of the implementation of digital technologies, exploring issues going beyond the strict domain of the law. See EDPB (2015).
[702] Raab (2020), p. 2.
[703] Mantelero (2016).
[704] Raab (2020), p. 9.
[705] Article 29 WP (2017), p. 6.
[706] Raab (2020), p. 9.
[707] Id.
[708] Id., p. 10.
[709] Id.
[710] Id.
[711] Raab (2020), p. 12.

social impact of new technologies[712]. HRESIAs are made of two elements: a self-assessment questionnaire and an *ad hoc* expert committee[713]. The former is used to determine the value framework that the system should abide by, while the latter is tasked with the contextualisation of such framework in a given application. The intervention of the *ad hoc* committee of experts is only optional. It may be required to step in only in cases featuring a high level of complexity[714]. This should ensure a tailored application of general ethical principles in all kinds of concrete technology applications.

HRESIAs aim to overcome the limitations of both legal and ethical-oriented impact assessments. Changing the focus from traditional data quality and security issues to the impact on fundamental rights and freedoms may help controllers to tackle the collective dimension of data processing[715]. On the one hand, however, legal and human rights assessments may not give due consideration to other ethical and societal concerns, especially in terms of unforeseen bias and public acceptability[716]. On the other, ethical impact assessments rely too much on broad ethical categories which may lead to excessively heterogeneous solutions in different cases[717]. Therefore, a balance between these two approaches should be found in an extensive interpretation of data protection principles. These general principles (e.g., fairness, proportionality) and clauses (e.g., necessity and legitimacy) may indeed introduce non-legal, social values into the framework[718].

4.4.3. Algorithmic impact assessments

Algorithmic Impact Assessments. Algorithmic Impact Assessments (AIAs) or Algorithmic Impact Statements (AISs) focus on automated decision-making initiatives[719]. They make controllers address the potential negative consequences of automated decision making on data subjects. Some AIAs have been conceived as sector specific. Notoriously, Selbst proposed an AIS that would apply only to police departments implementing predictive policing projects. This would require them to comply with some procedural obligations, such as: sifting through all possible alternatives, including by turning to third-party vendors; explaining design choices; measuring the efficacy of best auditing methods; comparing the impacts of different options[720]. A proposal from the civil society organisation AI Now called for making AISs a pre-procurement requirement for any public agency wishing to adopt an automated decision-making system[721].

In the GDPR, DPIAs may integrate the model of AIAs[722], bringing a twofold benefit. On the one hand DPIAs-AIAs may push companies to give due consideration to risks of unfairness, error, bias and discrimination stemming from the use of algorithms in decision-making[723]. On the other, they could provide source material to comply with individuals' rights about automated decision making (Arts. 13-15 GDPR), not to mention data subjects' rights to obtain meaningful information about the logic involved and the envisaged consequences of automated decision-making[724].

Operationalising DPIAs as AIAs can certainly broaden the scope and impact of such instruments, beyond sector-specific applications. Nonetheless, the biggest shortcoming of this approach is that the

712 Id.
713 Mantelero (2018), p. 758.
714 Id.
715 Id., p. 762.
716 Id., p. 765.
717 Id., p. 771.
718 Id., p. 765.
719 Raab (2020), p. 13.
720 Kaminski et al (2021), p. 11.
721 Id., p. 12.
722 Id., p. 13.
723 Id., p. 16.
724 Id., p. 17.

GDPR does not include a mechanism for mandatory disclosure to the public[725]. Without any public oversight over these impact assessments – either in the form of market or regulatory feedback from individuals – it appears difficult to trigger necessary third-party oversight (e.g., civil society actors or civic-minded experts acting as external auditors), especially in light of the constant lack of resources of national data protection authorities[726].

4.5. Leveraging data protection impact assessments in smart cities

4.5.1. Seeking the views of data subjects

Meaning and legislative history of Art. 35(9) GDPR. Article 35(9) of the Regulation is an interesting tool to open up balancing processes in smart cities also to data subjects. It provides that "[w]here appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations". A participatory DPIA may allow data controllers not only to demonstrate both their compliance with GDPR requirements to a broader audience, but also to involve the direct users (or targets) of the technologies in a more democratic assessment of the distribution of risks across different segments of the population. Despite its potential, however, both the opening and closing clauses of Art. 35(9) leave a wide margin of appreciation to data controllers in deciding whether data subjects should be involved in the process[727].

It should be recalled that the initial version of the text provided for an unequivocal obligation for data controllers to perform a DPIA *anytime* commercial or public interests, or the security of the processing could be jeopardised[728]. Since this "stronger" wording was considered to be too burdensome for data controllers, a Parliament decision initially deleted the provision. Finally, a Council position led to the final version, whereby data subjects' views are sought only "where appropriate"[729].

A legal obligation to consult data subjects? Faced with such weakly formulated provision, European and national data protection authorities have not so far tackled the question whether seeking the views of data subjects may be understood as a legal obligation in the first place. Decisions on the "appropriatedness" of such initiatives seem *prima facie* left to the discretion of data controllers[730]. Nonetheless, the Belgian DPA has indicated that involving data subjects may not be entirely optional: the nature, context, scope and purpose of the processing may make the consultation necessary, although no further information on which circumstance may trigger such obligation were provided[731].

Regardless of the mandatory or non-mandatory nature of the consultation, Art. 35(9) GDPR is not even clear on the modalities and consequences of the consultation[732]. For instance, *how* the participatory process should be conducted, and *who* should be involved is not explained. The Working Party did not further clarify these aspects, but merely remarked that such choices should be based on the circumstances of the case at hand[733]. Nonetheless, what seems to be clear from the guidelines of both the Working Party and other national authorities is that controllers are not bound to the opinions expressed by data subjects or their representatives; the process should always involve active

[725] Id., p. 19.
[726] Id.
[727] Cf. §4.5.1.
[728] Christofi et al (2022), p. 504.
[729] Id.
[730] Id.
[731] Commission de la Protection de la Vie Privée (CPVP) (2018), §82.
[732] Christofi et al. (2022), pp. 505-506.
[733] Article 29 WP (2017), p. 15 ; Christofi, Breuer et al. (2022), p. 510 (outlining possible ways to consult data subjects).

participation of data subjects, being the passive provision of information about the processing insufficient. Controllers are not in principle obliged to initiate the consultation, but if they do and receive negative feedback, they should explain why they intend to depart from the views expressed by data subjects[734].

Why seeking views from data subjects? Some DPAs have tried to explain the rationale of Art. 35(9) GDPR. For instance, the Irish and Spanish DPAs described consultation as a tool for controllers to achieve transparency *vis-à-vis* (future) data subjects and comprehend individuals' potential concerns over the envisaged processing[735]. The Belgian DPA instead focused the value of DPIAs in a thorough identification of risks[736]. Importantly, scholars have observed how these explanations oversee the role that legitimacy, social learning and pluralism may have in justifying participatory processes in DPIAs: the main focus is on the supposed benefits for data controllers, rather than for data subjects[737].

Transcending the domain of the Regulation, impact assessments have often been attributed a two-fold justification: a multi-perspective understanding of risks, as well as democratisation of the risks associated with introducing new technologies. Under the first aspect, scholars have highlighted the dangers of focalism, that is the tendency to overly focus only on one or few variables of a problem, thus missing possible alternative solutions[738]. In this sense, impact assessments allow to explore the same issue from manifold angles, gathering different opinions and prospective solutions. A richer debate increases the chances of successful technology development and implementation, as allows decision-makers to fill information gaps and obtain public feedback over their initiatives[739]. Under the second dimension, public participation is said to vest technology projects with greater democratic legitimacy. Citizens that are ultimately exposed to the risks of new initiatives are given a voice on the consequences they are willing to accept as members of the society[740]. Risks are not imposed with a top-down approach only, but have they received a democratic endorsement from the community, are more likely to be welcomed as justified in society.

The need for external scrutiny in the GDPR. Another factor has been put forward by the experts to argue for the need to foster public consultation in the context of the Regulation. In a world of pervasive processing – especially at the urban scale – it may arguably become impossible for under-budgeted data protection authorities to examine *all* performed DPIAs[741]. Indeed, Art. 36 GDPR takes a lighter approach on the matter, requiring external scrutiny by DPAs only where controllers consider that their DPIAs have uncovered high residual risks which cannot be mitigated with appropriate measures. Against such backdrop, tasks of external scrutiny over DPIAs and related projects may partially migrate from national data protection authorities to members of wider public, including civil society organisations, academia, individual citizens[742]. In order to do so, publication of DPIA results should be encouraged as much as possible[743].

Reasons for performing a participatory DPIAs in smart cities. All the abovementioned arguments can be invoked in support of a more participatory process in DPIAs for smart city services. If cities are rightly

734 Id., p. 15. Commission de la Protection de la Vie privée (CPVP) (2018), §86.
735 Irish Data Protection Commission (2019), p. 13; Agencia española de protección datos (AEPD) (2019), p. 149.
736 Commission de la Protection de la Vie privée (CPVP) (2018), §83.
737 Christofi et al. (2022), p. 507.
738 Id., p. 6.
739 Id, pp. 6-7.
740 Id., p. 10. For a critical perspective, see Ferretti (2010).
741 Christofi et al (2022), p. 516.
742 Id.
743 Id.

seen as social, cultural and political constructs, rather than simple networks of systems[744], reaching out to urban dwellers can arguably be a crucial step to achieve a more appropriate implementation of technology application in the city context. Participatory processes can indeed serve as venues for citizens to convey their political and cultural perspectives on smart city projects. In this perspective, DPIAs can really fulfil their function of ensuring a well-rounded identification of risks, highlighting also value-laden, non-technical variables in the process.

Participatory DPIAs can also provide greater transparency and thus legitimacy to smart city projects, as the Toronto Sidewalk case recently showed. From 2017 to 2020 indeed, Google's affiliate Sidewalk Labs partnered with Toronto authorities to transform the Quayside neighbourhood into a fully data-driven environment. Despite its advertised benefits in terms of efficiency, the initiative was hit by public backlash. Local communities were concerned for their rights to privacy and data protection, and were not informed of key points of the project, since agreements between Sidewalk Lab and the city were kept secret. Eventually, a number of public-facing events were organised to rebuild trust in the initiative, but were not successful. In the aftermath of the pandemic, the project was discontinued: Sidewalk's CEO attributed this decision to the economic crisis prompted by the health emergency, but the failure may be actually rooted in more complex issues, namely the lack of citizens' confidence and involvement in the project[745].

All in all, the need for participatory DPIAs in smart cities is supported by multiple reasons. Technologies do not function in a vacuum and must be implemented according to the specific environment in which they are embedded. In this perspective, cities are a topical example of how cultural, political, ethical values can shape a space and the communities living in it[746], which makes citizens' involvement all the more important in these processes. From a surveillance perspective, moreover, participatory processes can increase democratic oversight of monitoring initiatives in the city, rebalancing power asymmetries between powerful private companies and public authorities on the one side, and citizens on the other. Considering the non-consensual nature of many processing operations in smart cities, citizens' prior involvement in DPIAs may be a valuable way for them to have a say on how surveillance is operationalised in the urban area.

4.5.2. Leveraging environmental law for participatory DPIAs

Transparency obligations in EIAs. In the field of environmental law, procedural obligations of transparency and access to information are already well established in EIA practices[747]. In general terms, the public should be made aware when decision-making procedures are launched, and should have access to data and studies on the negative and positive impacts of the envisaged activities. These prerogatives lay down the basis for initiating participatory processes, where the public is given a chance to have a say in various initiatives (e.g., citizens' juries, citizens' panels, consensus conferences, focus groups, and public hearings)[748], or before competent authorities. These inclusive deliberation processes do not only build trust from early stages of the project, but also involve interested parties in the decisions on the distribution of risks across the population.

---

744 De Waal (2017), p. 18.
745 Green (2019), p. 155; Keymolen et al (2019), p. 247.
746 Bell et al (2012).
747 Cf. Article 6 of the Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the Assessment of the Effects of Certain Public and Private Projects on The Environment, OJ L 26, 28.1.2012, p. 1–21.
748 Gonçalves (2020), pp. 147-148. See also Principle 10 of the Rio Declaration.

Art. 8 ECHR: A common ground for environmental, privacy and data protection law. A "participatory turn" in the data protection and privacy landscape has only recently begun to be discussed. In this perspective, a *trait d'union* between environmental and privacy-data protection regimes is the case-law of the ECtHR under Article 8 of the Convention. Since the Convention lacks a specific provision on a right to the environment, the ECtHR has developed its case-law on the matter under the broad umbrella of Article 8[749]. The Court thus established a set of positive obligations of a procedural nature, including those of transparency, information and participation.

An extensive interpretation of the concept of "home" enshrined in Article 8 could expand the application of these obligations. According to the Court, the right to the respect for the home does not simply cover the physical boundaries of one's dwelling, but also the "quiet enjoyment of the area"[750]. The catalogue of the interferences that one should be shielded against is also quite broad, going beyond forms of physical or concrete intrusion[751].

In this context, the Court recognised that the Contracting Parties have an obligation of conducting investigations on the possible effects of the prospective measures, and making this information available to the general public[752]. In the *Tatar* judgment, moreover, the Court seems to have made a step forward towards the inclusion of a right to the *participation* of the public among the range of procedural obligations under Article 8 of the Convention[753].

Applying ECtHR's environmental case-law on data-driven urban initiatives. What implications could this case-law have when data-driven infrastructure and services are installed in proximity of citizens' homes? With a speculative argument, the procedural obligations of investigation, information and public participation could be claimed to be applicable in these instances as well.

The argument would proceed as follows: IoT-embedded infrastructure and services rely on extensive personal data collection practices to function. Data collection can give rise to invasive forms of surveillance, including profiling, which can impair citizens' autonomy and enjoyment of other fundamental rights (e.g., freedom of expression, association), not only within their homes but also in the surrounding public areas.

Drawing on the Court's extensive interpretation of the concept of home and related interferences, it could be argued that these forms of non-physical limitations may equally affect individuals' enjoyment of the area. The potential impacts of environmental-related projects (e.g., waste management or industrial implants, airports) would be equated with those building on extensive data harvesting operations. Hence, procedural safeguards already elaborated in the environmental case-law should be applied in this case too. This is all the more so as the link between the two fields is provided by Article 8 of the Convention.

Repercussions on Art. 35(9) GDPR. Extending environmental law requirements to the sphere of privacy and data protection may also affect the interpretation of these rights in EU legislation. Pursuant

---

749 To be precise, the Court has reiterated that the Convention does not include a right to the protection of the environment as such. Applications on environmental issues can result in a violation of Article 8 only insofar as the degradation of the environment has an impact on the private and family lives of the individuals. Cf. ECtHR, *Cordella and others v. Italy*, judgment of 24 January 2019, App. nos 54414/13 and 54264/15, §§100-101; ECtHR, *Guerra and others v. Italy*, judgment of 19 February 1998, App. no. 14967/89, §60.

750 ECtHR, *Giacomelli v. Italy*, §76.

751 Id.

752 ECtHR, *Guerra and others v. Italy*, §60; ECtHR, *Hatton v. the United Kingdom*, §128; ECtHR, *Taşkin v. Turkey*, §118; ECtHR, *Giacomelli v. Italy*, §§83-84.

753 ECtHR, *Tătar v. Romania*, §§113-119.

to the correspondence clause enshrined in Article 52(3) CFREU, indeed, the meaning and scope of the rights guaranteed in the Charter itself should be the same as their correspondents protected in the Convention.

In the case of investigative obligations, this reasoning would not add much to the existing EU secondary sources on privacy and data protection, as Article 35 of the GDPR already mandates the performance of an impact assessment for processing operations entailing a high risk for the fundamental rights the freedoms of data subjects.

Nonetheless, the same may not hold true for the accessibility of the information and public participation. Indeed, no provision in the GDPR requires the publication of the results of the DPIA, nor the inclusion of data subjects' views in the impact assessment as such[754]. This may change if those provisions were read in light of the ECtHR's interpretation of the right to the respect for private life.

Firstly, the right to public access to the information gathered in the context of impact assessments is clearly established in the interpretation of the ECtHR. Likewise, the public should be informed of the consequences of large-scale smart city projects, in order to assess the risks associated to such measures. This could result in a legal obligation to publish the results of a DPIA relating to the implementation of urban IoT critical infrastructure and services[755].

Secondly, if the right to public participation were fully established in the Court's case-law this would provide a strong justification for a systematic integration of inclusive deliberation processes in DPIAs, as those foreseen in Art. 35(9) of the GDPR. Stronger procedural safeguards may be applied to projects with uncertain implications and that need a wide support by the community.

Limitations: Individualistic perspective in the ECtHR's case law. Although speculative, this argument allows us to argue for democratising risk distribution decisions about smart city initiatives, not only on an ethical, but also on a legal level. This is not to ignore the practical complexities of implementing these approaches[756]. To mention one, a correct understanding of *who* should be included in the processes so as to a have a good representation of all impacted communities is difficult to attain. The ECHR's interpretation of the right to participation may not be helpful in this regard, as it seems to keep an individualistic perspective, focusing on whether the applicants in the proceedings have had the chance to express their views in the deliberation process.

The feasibility of potentially give all stakeholders a chance to have a say on these matters is questionable. What is certain is that public-facing initiatives can take many forms, some of which allow to intercept a wide portion of the public. In any case, as far as the principle of the proportionality is concerned, participatory processes may work as a good procedural safeguard limiting the margin of discretion exercised by private and public entities when balancing between safety and security needs and other fundamental rights.

5. Interim conclusions

Following the first part of the analysis on data protection in smart cities, this second chapter tackles this question: *What are the issues that arise from personal data flows in smart cities and how should these be addressed?* Through the lens of EU data protection law, three main issues were explored: purpose limitation, data controllership, and DPIAs.

754 Article 29 WP (2014d), pp. 17-18.
755 As clarified by the WP29, publishing a DPIA does not necessarily entail releasing the full document; the publication of portions of it or of a summary is in itself sufficient.
756 On inclusive deliberation processes, see Ferretti (2010), pp. 508-511.

At the outset, systemic data reuse is crucial to keep the city going as efficiently and smoothly as possible. Nonetheless, this trend in smart cities stands in contrast with one of the pivots of data protection law: purpose limitation. Thus, the analysis focused on how this principle applies in different smart city scenarios. As for other data processing operations, repurposing requires some kind of balancing, when the processing is not based on individuals' consent.

Following the CJEU case law, there is a granular methodology to perform this exercise, which should be conceived both as *multi-factor* and *multi-layered*. The first step should frame the strictness of the proportionality assessment. The second step can take two forms according to whether the reuse is based on a new national or EU law, or on a compatibility assessment pursuant to Art. 6(4) GDPR.

These criteria were all translated into the smart city context. Importantly, a systematic reading of the opinion of EU data protection authorities reveals that a lighter approach in terms of proportionality should be embraced when the data is to be reused for general interest goals. So far, however, EU policy has rather supported data transfers in the opposite sense.

Within the public sector instead, the option that affords the best degree of foreseeability is the explicit provision of data-sharing schemes. Regrettably, however, the adoption of this kind of legislation is still minor in EU Member States. Lastly, the application of purpose limitation does not seem to pose serious issues in structural PPPs in the law enforcement context, although further reuse of data within the security context should be surrounded by greater caution.

Furthermore, the participation of multiple actors in city management manifests itself through PPPs. Within such arrangements a major concern regards who is in control of the data. In data protection, this issue is addressed through the concepts of data controller, joint controllers and data processor. As PPPs may generate various horizontal and vertical relationships between public and private entities, situations of controllership and joint controllership cannot be addressed *a priori* but are always the result of factual assessments. In this light, various problematic smart city scenarios were analysed, and solutions to avoid commercial reuse of data collected through public service delivery were proposed. Allocating responsibilities over data in smart environments is a difficult task, but legal instruments to ensure that data subjects' rights are respected can already be found in the GDPR. However, a meticulous separation of responsibilities within PPPs does not mean that public authorities should be exempted from taking a broader view on the behaviour of the entities they involve in urban processing, e.g., disregarding reckless data practices by their commercial partners.

Lastly, the role of DPIAs in smart cities was examined. This tool should be operationalised as much as possible to provide *ex ante* solutions to many data protection issues in this context. Indeed, DPIAs could be a privileged instrument to perform balancing exercises and let citizens have a say on how (surveillance) technologies are implemented in the city. To this end, alternative models of impact assessments were explored to incorporate broader ethical views in DPIAs.

Secondly, the ECtHR's case law in environmental law was scrutinised and applied to the smart city context. It was argued that transparency, information and participatory obligations established for environmental projects under Art. 8 ECHR could be extended to initiatives involving data processing on a large scale. Pursuant to the correspondence clause in Art. 52(3) CFREU, Article 8 of the Charter could be interpreted extensively to incorporate these requirements and align it with Article 8 of the Convention. Ultimately, this would allow a case to be made for mandatory participation of the public in DPIAs under Art. 35(9) GDPR, thus allowing the "democratisation" of balancing exercises in smart cities.

Having examined smart city issues under the strict perspective of data protection law, the analysis will now shift to the right to privacy, which is also heavily affected by the inclusion of IoT technologies in the urban sphere.

III. Privacy Expectations in Smart City Public IoT Environments

1. Introduction

What is up with privacy? If one thing can be agreed upon, it is that *everything* has been said in literature about privacy. Privacy is an essentially contested concept[757], and maybe, this is unavoidable. As put it by Bloustein, "[t]he words we use to identify and describe basic human values are necessarily vague and ill-defined"[758]. Undoubtedly, legal vocabulary is limited in describing the nuances between states like distress, humiliation, anxiety, indignity, or mental suffering, which often emerge when one's private sphere is impinged[759].

The disagreement about privacy, however, goes to great lengths. There are those who consider it as "the dearest of our possessions"[760] or "the most fashionable of rights"[761], and those that see it as a concept in disarray, practically useless[762]. Some attempt to highlight its conceptual uniqueness, others think there is nothing special about privacy, and that any private interest can be equally protected by other fundamental rights. Admittedly, most quarrels about privacy seem to be rooted in its irreducible *vagueness*. Escaping definitional stability, privacy appears indeed too unsubstantial and evanescent as a concept, something too rich and complex to be grasped in clear-cut definitions[763].

Different privacies. Nonetheless, some scholars have decided to embrace privacy's "fruitful indeterminacy" and take advantage of its "open texture" as much as possible[764]. Indeed, there are several functions that privacy is said to serve at the individual and collective level in society. Privacy is deeply interrelated with intimacy and provides the necessary context for developing relations of trust, friendship and love[765]. It protects human dignity and the integrity of the person (both physically and psychologically) from external interferences[766]. It also creates a safe space for individuals to develop their own personality and try new experiences away from the judgemental gaze of others[767]. At the broader societal level, privacy is a quintessential feature of constitutional democracy, as it makes people free to develop and express their own opinions, without fear of being judged or watched by state powers[768].

Supposedly, reaching an agreement about what privacy means seems to be difficult, also because the term not only refers to a legal right, but also to a concept (or concepts) and to a socio-behavioural phenomenon or practice[769]. That is why, from a multi-disciplinary perspective, it is important to

757 Mulligan et al (2016).
758 Bloustein (1984, original work of 1964), p. 186.
759 Id., p. 187.
760 Floridi (2014), p. 101.
761 Halper (1996), p. 122.
762 Solove (2015), p. 156.
763 Hildebrandt (2006), pp. 2, 10.
764 Id., p. 2. Cf. also Mulligan et al (2016), p. 3; Cohen (2019), p. 2.
765 Fried (1984, original work of 1968), pp. 209 ff.; Moore (2003), p. 223.
766 Bloustein (1984, original work of 1964).
767 Gutwirth et al (2006), pp. 5, 11 ff.
768 Id.; Rouvroy et al (2009), p. 55; Hildebrandt (2006), p. 11; DeCew (2018), § 3.6.
769 Hildebrandt (2006), p. 3; Galič (2019), p. 114.

combine a legal analysis of privacy with a philosophical and sociological background on the matter[770]. Importantly, distinguishing privacy as a concept and as a legal right is crucial in order to understand the relative nature of privacy. Indeed, if people may experience factual loss of privacy, this does not necessarily mean that their privacy has been violated[771].

How to deal with privacy? In this regard, two ways of dealing with privacy are possible. We can keep digging to find a common underlying value capturing all existing *privacies*; or we can just accept it as a multi-faceted concept and offer a pluralistic account of what should fall within the scope of (the right to) privacy. Both approaches have their pros and cons. If unitary concepts of privacy have a common normative connotation[772] and can help us to address new legal and ethical problems, pluralistic accounts of privacy may lean towards more descriptive perspectives and offer a wider glimpse of what is protected under the label of privacy.

Outline. Against this backdrop, this chapter will combine philosophical and legal approaches to privacy. Because this work focuses on smart cities, the analysis will mainly take public venues as the reference setting. Specifically, the sub-research question for this chapter is: "*Which reasonable expectations of privacy can individuals have in complex IoT environments, such as public places in smart cities?*".

Following a brief account of privacy's philosophical roots, its different normative rationales will be mapped, explaining *why* this value should be upheld both in private and public places. Afterwards, the analysis will move forward and explore the notions of "space" and "place", which are central in privacy conceptualisation[773]. Specifically, a typology of places from a privacy perspective will be outlined, with a specific focus on public venues. This inquiry will further clarify the importance of privacy rights in these settings, in particular in the urban context. Lastly, the American and European case law on reasonable expectations of privacy will be examined. This review will serve to provide more practical indications about how the intensity of privacy interferences should be assessed in public places.

2. Privacy in public

Introduction: The emergence of the right to privacy. History shows how privacy has always been interrelated with life in the urban sphere. In ancient Greece, there was stark separation between the public sphere of political activity, the *polis* (also "city" in ancient Greek), and the private or domestic sphere of the family, the *oikos*[774]. Humans could only flourish when engaging in political activities in the public realm[775], while retreating from the public sphere meant escaping social responsibilities in the city[776].

A crucial moment of transition in the way privacy was conceived first occurred in the 16th century[777]. The word "private" started to be used in contrast to *public*, as in "private house" or "private property". From describing a state of deprivation (and possibly depravation), privacy went to define a state of *privilege*, where limited access or exposure was seen in a positive light[778]. In this period, the philosophical foundations were laid down in the work of major liberal thinkers, like Locke, Kant and Mill[779].

---

770 See Introductory Chapter, §3.1.
771 Schoeman (1984), p. 3; Tavani (2008), p. 162; Solove (2008), p. 102.
772 Koops et al (2017a), p. 487.
773 Hildebrandt (2006), p. 4.
774 DeCew (2018), §1.
775 Schoeman (1984), p. 10.
776 Solove (2008), p. 163; De Hert et al (2006), p. 14.
777 Galič (2019), p. 121.
778 Id.
779 On Locke, see Galič (2019), p. 123; Solove (2008), p. 26. On Kant, see Galič (2019), p. 124; DeCew (2018), §3.3.

With the advent of industrialisation in the 18th century, European cities faced exponential immigration, and new social networks started to develop. The "City of Strangers" was born: large public parks with promenades were built, and looking at and being seen by strangers while walking became a major social activity[780]. People also started to experience anonymity in public venues.

Throughout the 17th and 18th centuries, therefore, the term "private" began to be understood as "independence" and "intimacy"[781]. However, the expression "right to privacy" only emerged in the 19th century with the influential 1890 article published by American scholars Warren and Brandeis in the *Harvard Law Review* [782]. Their analysis heavily contributed to the acknowledgement of a right to privacy in common law, until its discussion gained a primary space in legal scholarship from the 1960s onwards.

Normative justifications for privacy. One of the common threads in the history of privacy builds on the rigid separation between the public and private sphere. Despite diffused assumptions on the matter, however, normative justifications of privacy do not exclude the public from its scope. This is evident in the philosophical and theoretical discourse on this fundamental right, whose interpretation cannot be separated from its underlying ethical values[783]. The following sections will thus provide an overview of different normative justifications for the protection of private life. These arguments are meant to answer the fundamental question of *why* privacy should be safeguarded, including in public spaces.

2.1. Why privacy should be protected

2.1.1. Human dignity and autonomy

Privacy and human dignity. One of the most recurrent normative justifications for privacy is the protection of human dignity and personal autonomy[784]. Notably, Bloustein argued that the common denominator of disparate privacy claims was the principle of "inviolate personality"[785]. Similarly, Fried submitted that the intrinsic value of privacy lies in basic human dignity[786]. Not without reason, privacy violations are often experienced by individuals as extremely distressing, even though they do not entail any monetary or material damages[787].

Privacy and autonomy. Another underlying concept of privacy is personal autonomy, which is understood as the capacity to govern oneself, to be led by considerations and desires that are not externally imposed, but are part of one's own authentic self[788]. In other words, a person should be able to determine their course of action[789], as well as control their own relation with others[790].

The growth of the autonomous self thus depends on the establishment of "social boundaries"[791]. Privacy allows not only the development of this kind of "self-knowledge", but also self-criticism and

780 Id. Brill (1992), p. 15.
781 Id.
782 Warren, Brandeis (1984, original work of 1890).
783 De Hert et al (2009a), p. 14 ; Koops et al (2017a), p. 493.
784 Cf. Cohen (2019), p. 3; Tzanou (2017), p. 8; Clifford, Auloos (2018), p. 153; Mulligan (2016), p. 12; Linskey (2015), pp. 94 ff.; González Fuster (2014), p. 23; Rouvroy et al (2009), pp. 59 ff.; Rodotà (2009), pp. 80, 82; Hildebrandt (2006), p. 2; Poullet (2014), pp. 9, 18, 28; van der Sloot (2016a), p. 426; Taylor (2002).
785 Bloustein (1984), p. 163; Warren, Brandeis (1984), p. 82.
786 Fried (1984, original work of 1968), p. 213.
787 Id., p. 214; Halper (1996), pp. 121, 123.
788 This normative justification is also extensively accepted in the legal domain, see ECtHR, *Pretty v. United Kingdom*, judgment of 29 April 2002, App. no. 2346/02, §61.
789 Id.
790 Id.
791 Id.

self-evaluation capabilities[792]. The argument is that the people who have grown and changed through introspective reflection enjoy more autonomy than those that do not[793].

Moreover, the idea of autonomy as a justification for privacy relies on the assumption that individuals are autonomous only when free of any external constraints of a social or political nature[794]. This explains why privacy was originally conceived as a negative liberty in liberal thinking[795].

Nonetheless, developments in social sciences have highlighted the fundamentally social nature of the human self[796]. For instance, communitarian theories describe how individuals are necessarily embedded in social contexts and have their identity shaped by multiple factors such as ethnicity, culture, religion, national identity or citizenship[797].

Also from the policy perspective, the link between privacy and autonomy seems to have undermined the weight of the right against other collective values (e.g., security)[798]. Consequently, scholars have tried to embrace more dynamic views of the self[799], and to enhance collective justifications for privacy, as will be shown next[800].

2.2.2. Identity-building

Privacy allows individuals to build their own identities. Theories seeing privacy as co-essential to self-awareness and self-development rest their premises on a liberal (and static) conception of the self[801]. In recent years, however, these traditional views on selfhood have been criticised for disincentivising growth in individual personality.

For instance, Cohen's work on privacy stems from the theoretical (and empirical) unsoundness of the liberal conception of the self. As shown in cognitive science, the self does not really have a "precultural core" but is situated within peculiar social and cultural contexts[802]. Selfhood and social shaping can thus coexist. Individual identity has a relational nature and develops between the experience of autonomous selfhood and the reality of social shaping[803].

Similarly, Hildebrandt believes that the core of privacy lies in the notion of identity[804]. Importantly, this approach allows for the merging of the positive and negative aspects of privacy into one single definition, seeing it as both a freedom *from* undue constraints, and a freedom *to* develop one's own identity[805].

Arguably, also Floridi's ontological account of privacy builds on its identity-building value. The focus of his analysis is informational privacy[806]. Floridi reinterprets privacy in light of the informational nature of human beings and their interactions: each person is considered "as constituted by his or her information", and each breach of one's informational privacy is understood as a form of aggression towards one's personal identity[807]. This approach thus equates privacy protection to the preservation of

---

792 Id., p. 83.
793 Id., p. 84.
794 Mokrosinska (2018), p. 121.
795 Id., p. 120; Cohen (2013), pp. 1906 ff; Hildebrandt, Koops (2010), p. 446.
796 Mokrosinska (2018), p. 121. Cf. Moore (2003), p. 220.
797 Mokrosinska (2018), p. 121; Solove (2008), p. 90.
798 Cohen (2013), p. 1904; Mokrosinska (2018), pp. 118-119; Solove (2008), p. 89; Solove (2015), p. 78.
799 See Cohen (2013) and (2019). See below §2.2.2.
800 See below §2.2.3.
801 Cohen (2013), pp. 1906-1907.
802 Cohen (2013), p. 1908.
803 Id., p. 1909.
804 Hildebrandt (2006), p. 7; Cohen (2013), p. 1906.
805 Id.; Hildebrandt, Koops (2010), p. 447.
806 Floridi (2014), p. 103; Floridi (2005).
807 Id., p. 119. See Durante (2017), pp. 117 ff.

identity, which is regarded as a fundamental right[808]. Interestingly, informational privacy is not sensitive to the dichotomy between private and public spaces: the information that constitute us does not change according to context, and privacy breaches can be conceptualised as kidnapping rather than trespassing[809].

Overall, these considerations suggest how digitisation has impacted on the notion of privacy. Due to the increasing collection and manipulation of personal information, the focus of privacy protection seems to have shifted farther towards the preservation of our (digital) identity. Through predictive technologies, individuals may be wrongfully represented in their habits and tendencies. While the impact of external (e.g., social, cultural) forces on the self is not new, profiling technologies now exert their "modulating power" in more subtle and unintelligible ways. The knowledge built upon one's digital trails can have a huge impact on personal choices, which significantly undermines people's autonomy in developing their own identities.

2.2.3. Collective value

The social and political value of privacy. Between the 1960s and the 1980s, many liberal thinkers focused on privacy as an individual right[810]. At the same time, however, some scholars tried to highlight its collective value. Privacy is seen here as an essential requirement for the functioning of healthy societies[811], and allows the development of various kinds of social and interpersonal relationships[812].

Beyond the individual sphere, privacy firstly enables the development of intimate and other social relationships[813]. In fact, information about us is the primary "commodity", the "moral capital" through which we can build bonds with others. Getting intimate, building friendships and romantic relationships is thus nothing more than a process through which we give away our privacy to get closer to others. Furthermore, privacy enables individuals to develop and keep different kind of relationships with different people, sharing varying amounts of information (e.g., work relations vs. intimate friendships)[814]. Thus, privacy is what allows us to "put forth different versions of ourselves in different contexts", an aspect that also reverberates in the process of identity-building[815].

If privacy has often been seen as constitutive of personal autonomy, the same has been said for democratic societies[816]. Privacy provides for that safe space for the free formation of opinions, the exercise of freedom of speech and association that are necessary to pluralistic and dynamic political debates in society. In practice, it also ensures that individuals are free to contribute to collective decision-making processes, e.g., through the institution of anonymous speech and secret ballots[817].

Hence, it has been argued that the value of privacy should not be measured according to the benefits brought to the individual, but to those brought to society as a whole[818]. Privacy protects individuals not simply for their own sake, but also for the sake of society[819]. On the one hand, privacy bears the social

---

808 Floridi (2014), p. 120.
809 Id.
810 Regan (2015), p. 53.
811 Solove (2008), p. 92; Cohen (2013), p. 1927; Regan (2015), p. 53.
812 Schoeman (1984), pp. 22 ff.
813 Fried (1984, original work of 1968), p. 205; Schoeman (1984), pp. 22 ff.; DeCew (2017), §3.6.
814 Cf. Nissenbaum (2009), p. 85; Galič (2019), p. 140.
815 Galič (2019), p. 132.
816 Regan (2015), p. 54; Solove (2008), p. 92; Hildebrandt, Koops (2010), p. 446; Floridi (2014), p. 116. In law, see Gavinson (1980), p. 444; Rouvroy et al (2009), p. 46; Hildebrandt (2006), p. 11; Gutwirth, de Hert (2006), pp. 3 ff; Mokrosinska (2017), p. 126.
817 Nissenbaum (2009), p. 86.
818 Solove (2008), p. 91; Solove (2015), p. 80.
819 Solove (2008), p. 92.

purpose of reinforcing "the norm of civility"[820], i.e., respectful relationships with our fellow beings. On the other, privacy circumscribes the reach of social norms into individuals' lives[821]. To function, societies always need some level of social control to address the natural risks of communal life and ensure order[822].

2.2.4. The value of privacy in private and public venues

The importance of protecting privacy in public urban environments. The previous sections have shed light on privacy's multiple rationales. Importantly, its normative justifications are often insensitive to whether individuals find themselves in private and public spaces. People need to have their dignity and autonomony protected in public venues as well, where they should also find a space to develop their own identity. Lastly, the political and social function of privacy may even find their privileged setting in public venues (e.g., political demonstrations, bonding with new friends).

Therefore, privacy is apt to cover a large number of activities in citizens' daily lives, which makes privacy expectations in urban environments very wide in scope. This also explains why privacy should be a core value in smart city development. Privacy is at once constitutive and instrumental to the maintenance of democratic institutions and citizenship, especially if one conceives the city as a political construct, rather than a simple system of sensors and computers. Privacy in public also favours identity-building and the construction of social relationships, as one can develop interpersonal relationships in parks and other public venues, decide to enjoy solitude while commuting to work, or convey one's sense of self through a precise way of dressing.

Certainly, the digitisation of space is reducing spaces for anonymity in smart cities, which may frustrate the fulfilment of privacy's societal functions. Digital technologies can divide urban communities in different segments according to life patterns, and possibly refrain citizens from adopting non-ordinary behaviours in public spaces. That is why it is crucial to preserve privacy not only in private, but also in the public domain. The following sections will provide an analysis of concept of "place" to further substantiate this argument.

2.2. Privacy places

The most contentious of dichotomies. One of the most discussed conceptual distinctions in the privacy debate is the private/public dichotomy[823]. At least since classical times, people have perceived the existence of a dividing line between public and private[824], and this separation was established as one of the "grand dichotomies" of Western thought[825]. Unsurprisingly, also the normative claims about privacy and its mechanisms of legal protection have been built around this division[826].

Generally speaking, the two terms of reference have gained multiple meanings over time. "Private" has been associated with the sphere of familial, personal, intimate relations, the realm of private citizens and corporations[827], spaces that are secluded or hidden (like the home)[828]. On the contrary, "public" has designed the world of civic action, government and public institutions, as well as physical spaces

[820] Halper (1996), p. 124.
[821] Solove (2008), p. 97.
[822] Id., p. 94.
[823] Koops et al (2017a), p. 545; Nissenbaum (2009), p. 90.
[824] Westin (2018, original work of 1967).
[825] Galič (2019), p. 187.
[826] Nissenbaum (2009), p. 90; Koops et al (2017b), p. 20.
[827] Nissenbaum (2009), p. 90 ff.
[828] Koops (2018), p. 614.

available for shared use[829]. In deeper analyses, intermediate states of "privateness" and "publicness" have been identified between these two extremes, showing that privacy should be perceived in a continuum, and that the lines between private and public can also be blurred.

The importance of space. The private/public spectrum brings to light one persistent thread: the importance of *places* in conceptualising privacy[830]. Places should not necessarily be understood in a naturalistic sense[831], but they can also be looked at in terms of the interpersonal relationships in which people engage[832]. Arguably, this has something to do with the fact that the concept of privacy is clearly *relational*. In other words, the degrees and the quality of our privacy are always defined in relation to the others and the space surrounding us.

Against this backdrop, some terminological clarifications on the concepts of "space" and "place" will first be provided[833]. A typology of places from a privacy perspective will then be outlined, focusing on public venues[834]. In this respect, issues of privatiszation and securitisation of public places will also be highlighted[835]. The impact of digital technologies on space will lastly be explored[836]. Following this overview, conclusions on privacy protection in public places in smart cities will be drawn[837].

2.2.1. "Space" vs. "place"

Key concepts: space and place. "Space" and "place" have been extensively discussed in (human) geography and other scholarly disciplines[838]. Although the two terms have been used interchangeably so far, more technical definitions will be employed in this overview. On the one hand, a basic and rather naturalistic understanding of "space" is considered. In this perspective, space is defined as the "backdrop against which human behaviour is played"[839]. This physical-empirical understanding is labelled as *absolute* in human geography, and is opposed to the general meaning of "place", which is instead defined as any "*meaningful* location"[840].

The duality between space and place somehow reflects the evolution that geography has undergone as a discipline[841]. Emerging in the 18th century, the field is usually divided into *physical* geography (focusing on natural environments), and *human* geography (studying cultural and constructed environments)[842]. While the former branch was dominant in the 19th and 20th centuries, the latter gained traction in the second part of the last century. Specifically, two major schools were opposed. Initially, the "positivist" stream developed in the 1960s and relied on a more naturalistic conception of space, mainly applying statistical and quantitative approaches to geography[843]. From the 1970s instead, a "critical" school of human geography was established, which focused on a culturally embedded notion

829 Id.
830 Koops (2018), pp. 618 ff.
831 Hildebrandt (2006), p. 4.
832 Koops et al (2017a), p. 564.
833 See §2.2.1.
834 See §2.2.2.
835 See §2.2.3.
836 See §2.2.4.
837 See §2.3.
838 Koops et al (2017b), p. 20.
839 Hubbard et al (2011), p. 4.
840 Cresswell (2004), p. 7 [emphasis added]. See also Koops et al (2017b), pp. 23-25; Altman et al (1992), p. 2; Kitchin et al (2014), pp. 66-67; Lefebvre (1991, original work of 1974), p. 141.
841 Hubbard et al, pp. 5-6.
842 Koops et al (2017b), p. 21.
843 Id.

of space[844]. The insights stemming from critical human geography are today considered fundamental in privacy scholarship.

For critical human geographers nowadays, a place is "a distinctive (and more-or-less bounded) type of space which is defined by (and constructed in terms of) the lived experiences of people"[845]. More precisely, place should be considered as a composite notion, made of (i) location; (ii) locale; (iii) sense of place[846]. Firstly, each place has a location, meaning that it can be pinpointed by fixed coordinates on Earth. Secondly, a locale is the material shape of a place where human (inter)actions occur. Lastly, sense of place describes the emotional and subjective attachment that people have towards places. Simply put, spaces become places only when people attach some meaning to it.

Privacy "places" and the contribution of human geography. In recent years, privacy scholars have deepened the study of (critical) human geography to acquire a more comprehensive understanding of what a place is[847]. Theoretical and empirical insights from this discipline should be integrated in the legal doctrine to overcome the long-standing, abstract dichotomy between private and public places. Indeed, the distinction between public and private does not follow a naturalistic pattern (i.e., open vs. closed off spaces), with private places being automatically attached a higher expectation of privacy, and public places a lower (if non-existent) one. Public and private do not exclude each other, but are interdependent and often overlapping[848], as will be shown next.

Against this background, one of the most comprehensive and recent overviews of private and public places is offered by Koops, who integrated inputs from human geography in his research extensively. He developed the concept of "*privacy space*", which identifies "a space in which you can be yourself–that is in which you can play, in your own way, the relevant role you have in social life"[849].

Here, the expression "*privacy place*" will be preferred to refer not only to physical settings, but also to the meaning attached to them in terms of privacy expectations. If spaces are settings to enact identity building and social life, they should be classified not only according to their naturalistic features (e.g., open vs. secluded spaces), but also according to the level of privacy that we can usually enjoy (or think we can enjoy) in them. This does not mean that the classification below is legal or normative in nature. Rather, it features a more descriptive (even though not neutral) character[850]. It is not interested in how public and private places *should* be perceived but looks at how people usually perceive these environments[851].

Specifically, Koops identifies four privacy zones: the personal and intimate zone, pertaining to the private domain; a semi-private zone; and a public zone. These will be explored in the following subsections.

2.2.2. A typology of "privacy places"

The personal and intimate zone. The private domain includes both the "personal zone" and the "intimate zone", where individuals can exercise (full) control with no external interference (e.g., other

[844] Id.
[845] Hubbard et al (2011), p. 6.
[846] Cresswell (2004), p. 7.
[847] See generally Koops et al (2017b); Koops (2018); Galič (2019).
[848] Koops et al (2017b), p. 20.
[849] Koops (2018), p. 613.
[850] Koops et al (2017b), p. 26.
[851] Id.

citizens, the government)[852]. The personal zone is equated with solitude, and identifies situations where individuals are on their own and interact with no other, experiencing the highest level of privacy[853]. For instance, the mind is arguably the most intimate of privacy places and one of the safest areas to be ourselves in a world of ubiquitous surveillance[854]. The integrity of our thought is safeguarded under the heading of mental and decisional privacy, and its protection arguably relates to the core essence of the right to privacy (as will be shown next in relation to emotion recognition technologies)[855]. Moreover, personal writings, belongings, the home and private communications constitute primary examples of personal and intimate places[856].

Blurred lines in the semi-private zone. Outside the remit of the home, there are zones standing at the crossroads between private and public. For instance, privacy scholars have argued that the advent of digital technologies (especially the IoT) has severely impacted on the traditional separation between private and public spaces, making their boundaries more blurred[857]. Even before that, however, different were the instances of spaces that did not easily fall either within the "private place" or "public place" box. Hence, the proposal to abandon the rigid public/private dichotomy is not new[858]. On the contrary, it is argued that the concepts of public and private should be regarded as "multi-dimensional (…), continuous and relative, fluid and situational or contextual"[859].

Regardless of their public or private nature, spaces function as settings for enacting social life. Social interactions (even of a rather intimate nature) may also occur in non-strictly secluded spaces like the home (e.g., bars, restaurants, workspaces, shopping malls). The "semi-private zone" is precisely what we find at the intersection between private and public places[860].

Importantly, this category includes cafés, restaurants, concert halls, public transport. Rather than being "privacy places" per se, however, these venues are probably best conceptualised as larger spaces in which different privacy places can co-exist and overlap[861]. For instance, people walk in public spaces and expect others to respect their personal space. When we travel on public transportation we often withdraw in mental bubbles listening to music or podcasts. When we have private conversations with friends in the train or in cafés, we try to lower our voice if the matters discussed are sensitive and we expect others not to make too much effort to eavesdrop.

Nonetheless, some publicly accessibly venues may present some peculiar characteristics, which could make them privacy places in their own right. This is the case of public transportation, which favours mental bubbling and sharing of intimacies with co-travelling friends[862]. The same goes for coffee houses and bars which are typically used for social gatherings and conversations[863]. These serve as "third places", that is places that are neither the home nor the work office, where people still hang out, enjoy themselves without too much fear of being judged. Here, private conversations are more fluid, may often involve new acquaintances, and gazing at others is much more accepted[864]. Unsurprisingly, coffee

[852] Id., p. 28.
[853] Koops (2018), p. 624.
[854] Koops (2018), pp. 623 ff.
[855] Chapter V, §2.3.2.
[856] See Koops (2018), pp. 643 ff.
[857] See Koops (2014b); Koops (2018), p. 661.
[858] Marx (2001), p. 160; Kumar et al (2008), pp. 324 ff.
[859] Marx (2001), p. 160; Galič (2019), p. 199.
[860] Koops (2018), pp. 642 ff.
[861] Id., pp. 648, 653; Kumar et al (2008), p. 327.
[862] Koops (2018), p. 648.
[863] Id.
[864] Id.

houses are considered to have played an important role in the establishment of the bourgeois public sphere[865].

Fully public places. Public places are defined as spaces that are generally accessible to everyone, regardless of their nationality, ethnicity, gender, physical handicaps and other characteristics[866]. In this definition, many scholars prefer to focus on the concepts of *access* and *use*, rather than *ownership*[867]. Indeed, privately owned spaces can also be open to the public (e.g., shopping malls), and some publicly owned areas cannot (e.g., military or government buildings)[868]. Also, public places may be distinguished into open or multiple-use public spaces (e.g., parks, public streets, sidewalks), and specified-purpose public spaces (e.g., railway stations or airports), which can in turn be subject to specific regulatory regimes[869].

From a privacy perspective, it is evident that actions performed in open spaces are visible to a potentially unlimited number of people[870]. This may lead us to think that there is no privacy in public places[871], and yet we often experience solitude, intimacy or anonymity even among the crowds, especially in metropolitan contexts.

Certainly, we cannot expect to exercise the same level of "boundary-control" when engaging in private actions in non-secluded spaces. Nonetheless, we can count on other people's *discretion* to have our privacy respected (at least partially)[872]. A mechanism of "civil inattention" is here at play: what matters for privacy in public places is remaining inconspicuous in the crowd, thus being able to be ourselves even when our appearance and behaviour is displayed in public view[873].

Different arguments support the case of privacy in public. Paradoxically, when alternative secluded spaces are not available, people can even proactively seek for privacy in outdoor spaces (as is often the case for teenagers). That is how public spaces can sometimes host quite intimate activities[874]. At the same time, continuously following someone in public will often be equated to a privacy infringement and criminally sanctioned as stalking[875].

When moving around in public, we expect to be seen by others but noticed by none[876]. We accept that our actions will be observed, but we think that each observer will only get disparate bits of information about us[877]. This mechanism of *de facto* anonymity is what enables us to feel like we can be ourselves even in public places[878]. This state of affairs, however, is significantly jeopardised today by IoT and AI technologies. In fact, these allow surveillants to aggregate discrete datapoints, collected in different times and spaces, to automatically reconstruct unitary profiles of individuals.

Political privacy places. Moreover, scholars agree that public places are crucial to foster political expression in liberal democracies, as well as social integration and identity-building (either at the group

---

865 Habermas (1989, original work of 1967, pp. 31 ff; Koops (2018), p. 648; van der Sloot (2021b), pp. 321, 322.
866 Altman et al (1992), p. 1; Habermas (1989, original work of 1967), p. 1; Galič (2019), p. 190; Madanipour (2003), pp. 98, 204.
867 Altman et al (1989), p. 1; Ruppert (2006), pp. 273, 277.
868 Altman et al (1992), pp. 1-2; Marx (2001), pp. 161-162; Ruppert (2006), p. 278.
869 Galič (2019), p. 335. Cf. Walzer (1986), pp. 470-471.
870 Koops (2018), p. 649.
871 As remarked by Koops et al (2017a), p. 553; Nissenbaum (1998), pp. 567 ff.
872 Koops et al (2017a), pp. 552-553; Brill (1992), p. 10.
873 Koops (2018), p. 650; Koops et al (2017a), p. 552; Sharon et al (2021).
874 Koops (2018), p. 650; Kumar et al (2008), p. 325.
875 Id, pp. 650-651.
876 Nissenbaum (1998), pp. 575-576; Nissenbaum (2009), p. 117; Koops (2018), p. 651.
877 Id.
878 Koops (2018), p. 650.

or individual level). Indeed, if these ideas are empirically observed in the field of human geography[879], they also find confirmation in more theoretical insights in political philosophy[880] and privacy scholarship[881].

Actually, all privacy places allow for self-development processes and social interactions that are fundamental to build citizens' opinions in well-functioning, pluralistic democracies[882]. To be more specific, however, "political privacy place"' identify settings that should be covered by specific privacy protection, allowing the free and autonomous exercise of political rights (e.g., parliaments, venues for public demonstrations)[883]. In these venues, citizens should be safeguarded as political agents, which entails certain conditions of anonymity being provided.

Public places vs. public sphere. The idea of political privacy places is closely connected to that of public sphere, which allows citizens to engage in political activities through collective discussions and joint actions[884]. One of its main theorists, Jürgen Habermas[885], did not focus on concrete physical spaces, but on the public sphere as a normative ideal[886]. This is seen as an abstract space where individuals can enact (essentially face-to-face) debates and undertake a critical use of reason over issues of a political nature[887]. From a historical standpoint, in the 18th century emerging institutions like coffee houses, together with the printed press, allowed in-presence debates and public critical reflection to be intensified[888]. Nowadays, however, the advent of capitalism and the commercialisation of communication media have arguably led to an erosion of the public sphere, which is increasingly contaminated by private interests.

Insights about the public sphere suggest how actual public places are important for people to engage in political participation. These are the stage for individual rights that are politically and spatially grounded at the same time, like rights of representation, assembly, freedom of action[889]. They are "space[s] of co-presence and simultaneity, where different actors can be present in the same place at the same time, where individuals can develop freely within a plurality of possibilities that are negotiated collectively"[890].

That is why "messiness" acquires a positive connotation in cities[891]. If understood as political constructs[892], public urban places can be the stage for continuous contention and instability between different communities and actors, venues to go beyond our personal sphere and engage with others. Also, public places can function as arenas for mutual contestation, where citizens can obtain visibility and acknowledgement of their demands[893].

---

879 Ruppert (2006), p. 272; Madanipour (2003), pp. 191-192.
880 Habermas (1989, original work of 1967).
881 See above §2.2.3.
882 Koops (2018), p. 651.
883 Id.
884 Koops et al (2017b), p. 30; van der Sloot et al (2021a), p. 322. Madanipour (2003, p. 207) defines the public sphere as "a collection of material and institutional common and inclusive spaces, in which the members of society meet, to share experiences, to present and exchange symbols and create meaning, and to deal with collective self-rule through seeking consensus as well as exploring difference".
885 Madanipour (2003), p. 192; Ruppert (2006), p. 274; Galič (2019), p. 191.
886 Madanipour (2003), p. 149; Ruppert (2006), p. 275.
887 Habermas (1989, original work of 1967), p. 27.
888 Id., pp. 27 ff.
889 Galič (2019), p. 193.
890 Madanipour (2003), p. 159.
891 De Lange (2019), p. 75.
892 De Waal (2017), pp. 17 ff.
893 Ruppert (2006), pp. 275-276.

This does not mean, however, that individuals should be identifiable to be "seen" – quite the opposite. Anonymity in public places is important to exercise political rights in open settings, especially when one expresses dissent[894]. As efficaciously put by Galič, "anonymity can be said to have both identity-negating as well as identity-forming features"[895]. On the one hand, the identity-negating aspect of anonymity shields the individual from the gaze of powerful (public and private) entities, and of their peers. On the other, anonymity also allows us to conceal our civil identity and freely express (political) contents in the public sphere[896].

Importantly, Habermas' ideas have been operationalised in the smart city context as well. For instance, some scholars have claimed that ideal features of deliberative democracy are now jeopardised by technocratic management strategies in smart cities and living labs[897]. Public places and their dwellers are increasingly made more and more visible. This compromises their freedom and autonomy in the public arena (i.e., chilling effect), as well as their ability to engage critically with others in political discourse[898]. In addition, the systematic involvement of commercial entities in managing public services and spaces further contributes to the growing privatisation of the public sphere. Indeed, these actors often put forward their own normative ideas on "quality of life" standards in urban environments. These are presented in an acritical way, but are certainly beneficial to the financial interests of the actors involved. Without any democratic debate on the legitimacy of these perspectives therefore, public places in smart cities are handled according to unilateral visions of how the city should be administered, undermining the rule of law and the neutrality of public places[899].

Social privacy places. Public places have also been conceptualised as the realm of sociability, although this approach often remains a minor one among the scholars as opposed to the political perspective[900]. These allow us to enact our social life with closer friends or less close acquaintances, often away from the prying eyes of family members. They also constitute the stage for face-to-face conversation with strangers, possibly creating a certain level of tolerance among communities[901]. Public places thus serve key social functions because they steer mingling between people of different cultures, ages, religions, ideologies (especially in large urban centres), and encourage mutual respect and trust[902].

Arguably, the social integration function of public places seems to be best served by what Walzer calls "open-minded places". Indeed, he distinguished between "single-minded places", designed by city planners and entrepreneurs with one specific purpose in mind (e.g., airports, libraries), and "open-minded spaces", which are designed for a variety of (unforeseen) uses[903]. Squares are open-minded places *par excellence*, the epitome of open-mindedness and urbanity[904]. There is no other place that attracts more disparate confluxes of citizens[905].

On the contrary, single-minded places are "designed to serve and facilitate privacy", allowing people to go unnoticed[906]. It is important to note that also single-minded places, especially when privately

894 Galič (2019), p. 195.
895 Id.
896 Galič (2019), p. 195.
897 See van der Sloot et al (2021a).
898 Id., p. 339.
899 Id., p. 341. See below §2.2.3.
900 Id.; Brill (1992), p. 8; Ruppert (2006), p. 272.
901 Madanipour (2003), p. 191; Ruppert (2006), p. 272; Walzer (1986), p. 470; Patton (2000), pp. 182-183.
902 Walzer (1986); Galič (2019), pp. 196-197; Madanipour (2003), p. 145.
903 Walzer (1986), pp. 470-471.
904 Id., p. 471.
905 Id.
906 Id.

owned (e.g., cafés, restaurants), can ensure a higher level of personal and interpersonal privacy, as we often get to choose with whom to interact within these venues. On the contrary, the same is not always true in open-minded public places, which represent the privileged arena for social-cohesion and community-building.

2.2.3. Privatisation and securitisation of public places

Places are power constructed. Because places are socially construed, power relations are crucial ingredients for defininge how these are designed and used by the public[907]. Foucault, for instance, saw space as "fundamental in any exercise of power"[908]. Likewise, scholars have also spoken of "architectures of power", referring to space design strategies aimed at conveying, symbolising, justifying the exercise of authority[909].

Privatisation of public places. Since the 1990s, changes in power relations in cities have led geographers to talk about privatisation of the urban environment[910]. The public sphere is commodified as private, and neo-liberal interests dominate the provision, regulation and maintenance of public space[911]. Historically, these strategies gained traction at the conjuncture between the process of de-industrialisation and the advent of the service sector[912]. The private sector started to meddle in city planning, and newly built out-of-town shopping malls and business districts became increasingly important in comparison to ("dead") central urban areas[913]. In this respect, scholars have also talked of "disneyfication" of public places: private and public developers actively sought to create environments mirroring a desire for security rather than interaction, for *entertainment* rather than for divisive political and social issues[914].

Privately owned/publicly accessible places are often shaped in light of needs for order, surveillance, and control over the behaviour of the public[915]. For example, taking pictures without a permit, giving speeches, rough sleeping, drinking a beer on the grass or having a picnic with wine in the park are all activities that may be forbidden in privately owned grounds[916]. Their design may suggest that marginalised communities (e.g., the homeless) could be denied access. The same goes for those wishing to spend a lot of time there, those not well dressed, or those behaving out of the ordinary.

Securitisation of public places. This phenomenon refers to the decline of openness and accessibility of public places by action of state and private entities, who are increasing their control and policing of public venues[917]. It is a response to the feelings of insecurity and fear of crime that have intensified withdrawal from public settings[918].

Privatisation and securitisation often go hand in hand. Firstly, public authorities are gradually absorbing risk management practices that naturally belonged to corporate environments[919]. Secondly, in privately owned places, visitors' behaviour is managed by employing CCTV and private security

907 Hubbard, Kitchin (2011), p. 7; Foucault (1982); Koops, Galič (2017), p. 20; Harvey (2008, original work of 1973).
908 Foucault (1982).
909 Schuilenburg et al (2018), p. 1.
910 Galič (2019), p. 204; Koops et al (2017b), p. 33.
911 Galič (2019), p. 204; Kumar et al (2008), p. 326.
912 Id.
913 Id.; Madanipour (2003), p. 189; Mitchell (2003), pp. 138 ff.
914 Mitchell (2003), p. 138.
915 Mitchell (2003), p. 138; Ruppert (2006), p. 277.
916 Galič (2019), p. 205.
917 Galič (2019), p. 206.
918 Ruppert (2006), p. 277; Madanipour (2003), p. 189.
919 Ruppert (2006), p. 285.

personnel, who frequently relies on trespass laws without any accountability[920]. Thirdly, digital technologies contribute to strengthening the ties between the police and security companies, which are the main providers of these tools and the relevant expertise.

In addition, trends of securitisation of public places are part of a broader paradigm shift from crime repression and crime prevention[921]. Indeed, a wide range of activities that are not strictly criminal can still be labelled as "rowdy", "unruly", "anti-social" or "escalated"[922], and is addressed in urban policing strategies.

From a privacy standpoint, these regulatory practices are dangerous because they discourage spirited or non-ordinary activities, and push towards stereotyped behaviour, dressing styles and general "social neutrality"[923]. The importance of public places as venues for chaotic fluxes, unmediated encounters and dialogues is thus declining, which has led scholars to even talk about the "end of public space"[924]. Assumed needs of security and public order can easily translate into patterns of discrimination, exclusion, or domination[925], especially for marginalised communities and political protesters[926].

Unsurprisingly, privatisation and securitisation trends have gained renowned attention as digital technologies are being integrated in the city. As of today, indeed, new architectures of power express themselves through intensified surveillance practices that severely impact individuals' rights connected to public places, as the Sidewalk Toronto project and *De-escalate* in Eindhoven show.

2.2.3. Digital environments

Everyware. The proliferation of digital technologies has certainly had a huge impact on our conception of space and social interactions[927]. Thanks to the IoT, computational power can now be infused in any place. The term "everyware" describes the process through which "computational power will soon be distributed and available at any point on the planet – calculative capacity […] literally available everywhere, with multiple computers operating for every person"[928]. The underlying idea of this concept is that we should not organise our daily lives around computation; instead, computation should surround us and be available as needed[929].

Nowadays, spaces can increasingly communicate with one another in unprecedented ways[930]. Digital and physical spaces, including people, devices, and software are all connected in the same ecosystems, made of biological, spatial and urban components brought together by information flows[931]. Importantly, in smart cities the development of this common information layer (or ecosystem) allows managers to have a comprehensive view of different and potentially distant physical spaces.

Urban geographers have further referred to the expression "code/space" to represent this mutual interdependence between space and embedded software[932]. In smart environments, space is created and

[920] Id.; Kumar et al (2008), p. 335.
[921] See Ashworth et al (2014); van Brakel (2017); Mitsilegas (2015); van Brakel et al (2011).
[922] Wilding (2017); Galič et al (2021); Galič (2019), p. 208.
[923] Id.
[924] See Mitchell (2003), pp. 118 ff.
[925] Ruppert (2006), p. 191.
[926] Amnesty International (2018) (on the Gang Matrix software); Kruope A (2020) (on the Russian facial recognition software challenged before the ECtHR).
[927] Koops (2018), p. 612.
[928] Kitchin et al (2014), p. 216.
[929] Id., pp. 215, 217.
[930] Lacerda et al (2019), p. 728. Resmini et al (2016), p. 19.
[931] Id.
[932] Kitchin et al (2014), p. 16.

evolves according to software commands, and the software exists mainly to produce a particular kind of spatiality[933].

How the digital changes urban public places. Urban geographers have argued that the hyperconnectivity of space is contributing to the decline of public places[934]. As face-to-face interactions diminish, its social and political function has been undermined.

Generally speaking, the law has the complex task of regulating a multiform and changing world, and the only way in which this can reasonably be done is through general categories. The law needs to classify in order to understand the world, and this is often done through legal boundaries (e.g., married/non married person, child/adult, etc.)[935]. When it comes to privacy, the public/private divide has long been the primary "boundary marker" to modulate the intensity of privacy protection. Of course, the digital revolution has put an ulterior strain on these classifications. The result is that today the original dichotomy is no longer a useful proxy to determine the boundaries of privacy protection[936]. This does not mean, however, that space (although not necessarily in its naturalistic dimension) no longer matters in defining what privacy is and how it works[937].

Evaporating privacy places. Arguably, the digital technology impacts on legal boundaries as follows: (1) existing privacy places are opening up to new information leaks, becoming transparent to the outside world; (2) new boundary-markers are being established, extending the scope of privacy places in unexpected venues[938].

Concerning the first problem, digital technologies are making it difficult for individuals to exercise any kind of boundary control over their own personal space. The topical example here is that of the home, which is "*evaporating* as the classic place where private life happens"[939]. Thermal image detectors can spot heat sources (not only marijuana cultivation nurseries, but also humans), directional microphones can bypass walls, and networked devices such as home computers, nannycams, and IoT appliances like smart fridges or thermostats can be hacked or eavesdropped upon[940]. Smart metering data can also give granular information about the habits of home dwellers (sleeping patterns, food and drink consumption, working hours). Consequently, rules sanctioning the *physical* trespassing of the home are becoming obsolete[941].

Similar considerations can be made for public venues. If once we could enjoy anonymity in public, now private and public entities can have access to hundreds of discrete data points to reconstruct people's movements across the city and potentially other private life aspects, including work, interests, friendships, love life. Information that once was dispersed in different times and places can now be easily brought together.

At the interpersonal level, it should be mentioned how "civil inattention" mechanisms have allowed us to be inconspicuous amongst crowds. When squashed in public transportation, or sitting in a packed coffee bar, we acknowledge the presence of others, but we turn our heads away or stare at our feet not

933 Id.
934 Madanipour (2003), p. 159; Kumar et al (2008), p. 326.
935 Koops (2014b), p. 248.
936 Koops (2014b), pp. 255-256; Winter (2014), p. 29; Kumar et al (2008), p. 326.
937 Koops (2014b), p. 253.
938 Cf. Koops (2018), p. 661.
939 Koops (2014b), p. 256.
940 Id., p. 257.
941 Id.

to display too much interest in others[942]. This subtle and common-sense form of respect is one of the most widespread and powerful norms enabling privacy in public places, especially in direct personal interactions[943].

Nonetheless, the growing use of tools like smart glasses or consumer facial recognition may have disruptive effects on this consolidated social practice, e.g., by allowing strangers to take snaps of us to feed them to a facial recognition app[944]. Specifically, facial recognition tools have now become available to the wider public and could be used in these publicly accessible spaces[945].

In these venues, the use of consumer facial recognition may first of all increase *visibility* (as smartphone cameras can steal people's glances in snapshots); secondly, it also magnifies *knowability* and *recognisability* (as face recognition apps can match the snap with social media images, identifying the portrayed subject)[946]. Both behavioural and informational privacy of individuals could be jeopardised[947].

But there are other ways in which more invasive expressions of facial recognition can affect privacy in public. As of today, developers of EFR claim that their technology is able to detect emotions like joy or distress by processing facial and other biometric features. At the time being, these technologies are now being tested mainly to spot improved targeted advertising or individuals' suspicious behaviour in public venues. These technologies may also affect people's behavioural privacy, because of their chilling effect and potential inaccurate inferences.

Extending privacy places. Another trend that is mixing up existing assumptions about privacy is the proliferation of technical artefacts that deserve protection, but are not easily classifiable into some of the traditional boundary markers, like the body or the home. For instance, it is become increasingly difficult to distinguish between "things" and "bodies" when we consider advancements in human microchipping and other IoT devices whose function is closely interconnected with monitoring the human body[948]. Opening up doors and paying for things just by hand swiping is not a thing of the future anymore, and one can imagine how this kind of embedded artefact could be leveraged in many smart city initiatives, e.g., to improve fluxes at public transportation flows, or to access other kinds of public services or facilities (e.g., post offices or police stations).

The same questions arise with less edgy examples like smart glasses or Fitbits, biometric templates stored in mobile devices, and to some extent the IoT device *par excellence*, the smartphone. Although not an integrated part of the body, some already consider smartphones as natural extensions of our organic bodies[949]. It is common knowledge indeed that these devices now store very sensitive information (e.g., banking or period monitoring apps, Covid-19 tests results, internet search history, intimate pictures and videos), that once stayed in the home and is now carried around in public places, being more exposed to intrusions[950]. Unsurprisingly, the case law is increasingly recognising the peculiarity of smartphones in terms of the quantity and quality of the data they carry[951]. Their approach to these questions will be outlined in the following sections.

---

942 Goffman (1963), pp. 83 ff.; Sharon et al (2020), pp. 1-5.
943 Sharon et al (2020), p. 2.
944 Walker (2016).
945 Sharon et al (2020), p. 6.
946 Id.
947 Id.
948 Koops (2014b), p. 251.
949 *Riley v. California*, 573 U.S. __ (2014), p. 9.
950 Lasagni (2018), p. 387.
951 *Riley v. California*, 573 U.S. __ (2014), p. 3.

2.3. Which privacy or *privacies* for public spaces in smart cities?

Not only one privacy? Following the previous discussion, it is safe to argue that privacy is pretty much everywhere. It is one of the primary mechanisms through which we regulate any kind of social interaction and relations with the outside. Precisely because privacy is suitable for regulating multiform aspects of our daily life, its nature is necessarily multifaceted and cannot easily be grasped with very tight definitions. In this perspective, the discussion on the normative foundations *and* "places" of privacy has shown how this is a fundamentally pluralistic right[952].

Beware of conflating informational and non-informational privacy. One of the choices in this dissertation was to analyse privacy and data protection issues separately. This is not to say that the two rights never overlap or should not be considered in conjunction, as the use of digital surveillance technologies frequently pushes us to do.

When speaking of monitoring devices and digital data, indeed, there is a strong temptation to conflate all possible privacy issues under the umbrella of "informational privacy", in the technical form of the right to data protection. This possibly explains the growing interest of academia on informational privacy, to the detriment of other (still relevant) privacy dimensions (e.g., behavioural, mental or bodily privacy)[953]. Indeed, rights like informational privacy and data protection do not necessarily bear the same "spatial dimension" as other aspects of privacy. As traditional space and time boundaries collapse under the influence of digital technologies, these concepts thus appear more appropriate for dealing with the issues of contemporary surveillance.

Nonetheless, it should be considered that this phenomenon of boundary blurring is not specific to digitisation only, although new technologies certainly contribute to amplifying this process. Indeed, surveillance has *always* aimed to bring down spatial and temporal barriers in order to store information about individuals, spaces or items in one single venue[954], reconstructing behaviours and phenomena occurring in different moments and locations. If this process relies on the collection and aggregation of information, however, the effects of surveillance can go far beyond this, exerting an impact on people's lives even when no information flow is at stake[955].

For example, this is evident in Foucault's panopticon[956]. Its controlling effects do not strictly depend on the transmission of information: the panopticon could impose discipline even if the tower was empty[957]. It is enough that people inside the building believe that someone is possibly monitoring them. The same happens today in many urban contexts, either for more traditional means of surveillance like CCTVs or for more invisible ones, like sensors. Here as well, the fear of being watched is independent of the fact that there is actually someone behind the camera. Today, pervasive IoT surveillance seems to push this lack of reciprocity between surveillers and the surveillees in smart cities even further. Indeed, not only are people not aware of whether someone is actually watching them behind a camera, but they cannot even determine the location of potential points of data collection.

Privacy for public places. One further caveat consists in recognising the functional and interdependent relationship between (traditional) private and public places. Although this analysis mainly focuses on privacy issues in the public context, more personal and intimate expressions of private life could not be

[952] Cf. Solove (2008).
[953] On privacy dimensions, see Koops et al (2017).
[954] Galič (2019), p. 331; Patton (2000), p. 184.
[955] Sharon et al (2020), p. 7.
[956] On the panopticon, see Chapter IV, §2.1.
[957] Id.; Patton (2000), p. 182.

excluded from its scope, as they can develop not only within the boundaries of the home, but also in the urban public sphere.

The value of privacy in public is not limited to the fact that we enact our private life in public places, in a continuum between the private and public domains. The need to protect privacy in public – and even more so in datafied environments[958] – also stems from privacy being a constitutive element of truly pluralistic and dynamic democracies. In this vein, Galič explains that rather than talking about privacy *in* public spaces, we should discuss privacy *for* public places[959]. The expression "privacy in public space" has a strong spatial/physical focus, and ignores the interdependent relationship between privacy and public space, whereby privacy protects some of the constitutive elements of the latter, e.g., political participation and sociability[960].

Some characteristics of public places are also crucial to the protection of privacy in terms of self-development and identity-building. To foster people's development, public places should be (1) open to access; (2) free of exclusivity of control; (3) subject to multiple use; (4) tolerant to a level of disorder; (5) anonymous; and (6) allowing for dissent[961]. For instance, individuals can feel free do act freely and develop their personality in places that are open to access and whose use is not pre-determined too tightly (as in privately owned publicly accessible places)[962].

The same level of "messiness" should be ensured to strengthen the social function of public places. Indeed, experiencing places that are too "strictly scripted" – even through the modulating effects of embedded sensor technologies – may give us a sense of safety and order, as we are spared the sight of marginalised people like migrants, homeless people and addicts[963]. The danger however lies in the long run, as filter bubbles may not exist only online, but also in the offline world. Specifically, if people do not "meet" with those that are different from them, even those that they do not feel at ease around, they could become separated from other parts of social life, isolating in their own cultural and ideological bubbles[964].

Concluding remarks. Overall, this analysis showed that there is a wide range of activities worthy of being protected in public places in smart cities. As indicated above, there are multiple rationales to provide these safeguards, ranging from individual anonymity to societal interests. These emerge especially if one embraces a critical notion of space that goes beyond its physical characteristics (open vs. secluded). For the meaning they acquire in collective conscience, public places may also raise expectations in terms of privacy protection. Therefore, the following sections will shift the focus to the legal analysis, in order to identify when – and to which extent – privacy is interfered upon in public IoT environments in smart cities.

3. Privacy expectations in public smart city environments

Another piece to the conundrum. Just like privacy, "reasonable expectations" have been defined as an "essentially contested concept" in the legal domain[965]. While the concept of reasonable expectation is pivotal to many legal doctrines[966], the "reasonable expectation of privacy" test was first designed in the

[958] Cf. van der Sloot et al (2021a).
[959] Galič (2019), p. 330.
[960] Id., p. 331; Patton (2000).
[961] Galič (2019), p. 338.
[962] Id., p. 339.
[963] Id.
[964] Id.
[965] Kuklin (1997), p. 21.
[966] Id., p. 19.

landmark case *Katz v. United Stated* (1967), which radically changed the regime of protection of the Fourth Amendment in the United States. In its decision, the USSC revised its interpretation of the constitutional safeguard by shifting from a definition of privacy as physical trespass to one in terms of expectations[967].

Years later, the idea of reasonable expectations of privacy gradually made inroads in the case law of the ECtHR. Specifically, the notorious case *von Hannover v. Germany* (2004) again put the question of privacy in public at the centre of attention[968]. Although in different terms, both the USSC and the ECtHR seem to have exploited the idea of reasonable expectations of privacy as a tool to address changing needs in privacy protection, which was to be extended outside the traditional sacred space of the home. The idea of reasonable expectation of privacy is not completely deprived of a spatial component, but it is certainly more flexible: it tackles not only *where* the intrusion has taken place, but also *how* the information is going to be used, and for which *purposes*. Because of this flexibility, it is worth exploring how courts have developed and used this parameter in order to understand how to approach the problem of multi-purposed, pervasive cyber-surveillance in smart cities.

What are "reasonable expectations" in the law? The Oxford English Dictionary provides many possible definitions of the term "expectation". One in particular resembles how the term is usually understood in the legal domain: "[t]he action or fact of expecting something as rightfully due, appropriate, or as fulfilling an obligation"[969]. This meaning has to be kept separate from a more general understanding of expectations, which refers to people's desires, hopes, fears or ideas about the future[970].

Legal and non-legal expectations are indeed very different in nature[971]. If non-legal (or conative) expectations are purely subjective, *reasonable* expectations in the law also have an objective character[972]. Also, the specifier "reasonable" adds an objective and normative layer to the concept. Not only should the individual subjectively anticipate a future occurrence, but his or her expectation must be objectively and normatively acceptable[973]. This means that not all kinds of expectations can be protected by the law. Only those that overcome a certain threshold of likelihood and meet some socially recognisable normative standards can be acknowledged in the legal order[974].

Nonetheless, even within the boundaries of the law, expectations can be treated differently. On the one hand indeed, private law relates to consensual matters and gives more importance to personal preferences, covering purely subjective and non-necessarily reasonable expectations as well. On the other, for what mostly concerns the topic of this dissertation, public law generally emphasises more (although not completely) the *reasonableness* of expectations, and how these are objectively shared in society at large[975].

---

967 Reidenberg (2014), p. 144.
968 Moreham (2006), p. 607. See ECtHR, *von Hannover v. Germany,* judgment of 24 June 2004, App. No. 59320/00.
969 Oxford English Dictionary (2022); Kuklin (1997), p. 23.
970 Oxford English Dictionary (2022).
971 Kuklin (1997), pp. 23-24, 27.
972 Id., p. 24. For instance, the term expectation conveys an idea of subjectivity and likelihood: a person has a sufficient amount of information about a situation to foresee the probability of a future event (e.g., the fact that one's legal claim will be satisfied by the system, or that the rain is about to come when the sky is cloudy).
973 Id.
974 Id, p. 21.
975 Id., p. 24.

The conservatism of reasonable expectations. One of the main criticisms against the notion of reasonable expectations is their supposed circularity, as it is argued that the law protects only those expectations arising from existing legislation[976].

Unsurprisingly, similar remarks have been addressed to the notorious framework of privacy as contextual integrity, developed by Helen Nissenbaum. This theory identifies intrusions of privacy in violations of accepted social norms regulating the flow of information in specific contexts[977]. Nissenbaum actually draws considerably from the idea of reasonable expectations[978]: if "contextual integrity" flags any deviation from existing social practices as potentially problematic, reasonable expectations also tend to emphasise norms entrenched in a given socio-legal system. As a result, both concepts are confronted with dangers of conservatism, or as Nissenbaum calls it, of the "tyranny of the normal"[979].

Possible solutions. These issues have been addressed in different ways. From the narrower perspective of the law, the tautological circle of reasonable expectations could be broken by taking into consideration not only positive legislation, but also the broader social and legal culture in which interested actors are involved[980]. The law and reasonable expectations should be tied by a mutual feedback mechanism: reasonable expectations affect the state of the law, and the state of the law affects reasonable expectations[981].

In this perspective, reasonable expectations may also be a factor of change. When the "law in the books" is under significant stress and is not able to address people's discontent, the expectations stemming from society could actually steer reform and ground new norms to address recent developments[982].

In a slightly different way, Nissenbaum addresses issues of conservatism by devising a methodology to overcome informational practices that no longer meet society's expectations. Certainly, a presumption in favour of existing practices/expectations should be established, but this does not mean that such presumption cannot be overcome under certain circumstances[983]. When there is a violation of a socially established informational practice, a *prima facie* violation of contextual integrity could be spotted[984]. Nonetheless, if the moral (or legal) superiority of the new practice can be demonstrated, this can be accepted as legitimate[985].

These lines of reasoning seem to find confirmation in legal practice. For instance, the doctrine of reasonable expectations of privacy has not prevented the USSC from changing its interpretation of the Fourth Amendment when technological developments called for it[986]. This shows that, if one applies the parameter critically, the tendency to "freeze the law at the status quo" can be avoided[987].

---

976 Id., pp. 21, 25.
977 See, e.g.,Nissenbaum (1997), pp. 581-582; Nissenbaum (2009).
978 Nissenbaum (2009), p. 162.
979 Nissenbaum (2009), pp. 161 ff. More generally, it is interesting to note that certain ethical theories have been also blamed for their conservatism e.g., communitarianism. See Beauchamp (1991), pp. 278-279.
980 Kuklin (1997), pp 25-26.
981 Id., p. 33.
982 Id., p. 34.
983 Nissenbaum (2009), p. 164.
984 Id.
985 Id.
986 See, e.g., *Kyllo v. United States*, 533 U.S. 27 (2001), or USSC, *Carpenter v. United States*.
987 Kuklin (1997), p. 43.

Outline. Reasonable expectations of privacy can be a useful tool to address the mutated needs for protection of privacy in public triggered by smart surveillance. However, different gaps should be filled for this purpose. Firstly, these protect places and situations that, for legal consensus, can be considered private and shielded from undue intrusion.

Secondly, reasonable expectations of privacy have primarily been used as an instrument of *individual* protection, i.e., in situations where specific people had been targeted by surveillance measures in a criminal proceeding, or their privacy had been violated as a result of the actions of another private subject (e.g., press company or work employers). Sensor surveillance in smart cities, instead, do not always have such circumscribed focus, and fit within broader models of mass or unfettered surveillance.

To understand how the criterion of reasonable expectations of privacy could be useful in such contexts, the foundations of the relevant doctrine in the USSC case law will be explored[988]. Secondly, the focus will turn to the ECtHR case law[989]. Lastly, recurring patterns and relevant factors will be discerned to understand how reasonable expectations of privacy may work in smart public environments[990].

3.1. Privacy expectations in the case law of the United States Supreme Court

Meaning and scope of the Fourth Amendment. The Fourth Amendment to the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". In criminal proceedings, this safeguard translates into the obligation for government agencies to obtain a judicial warrant prior to any investigative activity (i.e., searches and seizures) entailing an interference with protected areas.

A literal reading of this provision suggests that "searches" and "seizures" are the limit to the scope of the Fourth Amendment. Not every law enforcement activity necessarily calls for its application, and over the years judges and scholars have put considerable efforts in understanding what these terms actually mean. On the one hand, the meaning of "seizures" has not posed the greatest difficulties, being generally identified with the "act of physically taking and removing tangible property[991]. Later on, however, it emerged that seizures could entail broader privacy implications, going beyond property rights[992]. Seizures within the meaning of the Fourth Amendment can indeed occur even if no previous search was carried out, and no property was physically trespassed[993].

On the other hand, the meaning of "searches" has sparked a much more intense debate, and to this day it is not subject to a comprehensive definition. Generally, a search implies "prying into hidden places", but importantly "it is generally held that the mere looking at that which is open to view does not amount to a 'search'"[994].

In *Olmstead v. United States* (1928), for example, the USSC initially considered that placing a tap on telephone wires and thus eavesdropping upon the defendant's conversations did not constitute a search under the Fourth Amendment, because "wires are not part of his house or office, any more than are the highways along which they are stretched"[995]. Therefore, for a long time, acts of seeking could be "elevated" to a Fourth Amendment search only if those concretely intruded in constitutionally protected areas, i.e., those enumerated in the provision at stake: "persons", "houses", "papers", and

[988] See §3.1.
[989] See §3.2.
[990] See §3.3.
[991] LaFave (1996), pp. 375-376.
[992] Id., pp. 377-378.
[993] *Soldal v. Cook County*, 506 U.S. 56 (1992).
[994] Id., p. 380.
[995] See *Olmstead v. United States*, 277 U.S. 438 (1928).

"effects". Things definitely changed with the seminal *Katz* case, which first introduced the reasonable expectation of privacy test.

3.1.1. The *Katz* case

The Fourth Amendment protects people and not places. Mr. Katz had been convicted in federal court based on evidence obtained through the electronic surveillance of conversations he had on an exterior telephone booth, from where he often placed long-distance calls. Following *Olmstead*, it had been excluded that those monitoring operations could amount to a Fourth Amendment search because the microphone placed by the police had not pierced the wall of the telephone booth. Before the USSC, two constitutional questions had to be examined. There was a need to determine, on the one hand, whether a public telephone booth was a constitutionally protected area; on the other, whether a physical penetration of that area was necessary to trigger the application of the Fourth Amendment.

The government tried to stress the circumstance that the booth was partly made of glass and that Mr. Katz remained *visible* while in there. Also, it claimed that the surveillance technique employed entailed no physical penetration of the booth, and that the Fourth Amendment only shielded *tangible* property from searches and seizures.

According to the USSC, however, the government had a very physical and property-oriented conception of the Fourth Amendment, which in the 1960s was already put into question by the use of new surveillance techniques (although not as sophisticated as contemporary ones). Justice Steward notoriously commented in this regard that: "the Fourth Amendment protects *people*, not *places*" [emphasis added].

Therefore, the effort of discerning the concrete "areas" covered by the Fourth Amendment was a sterile exercise: everything that people sought to keep private, even in public, could be constitutionally protected. All these things considered, the USSC deemed that the wiretapping of Mr. Katz's calls constituted a search under the Fourth Amendment, and thus was illegal because police agents had not previously obtained a judicial warrant.

Harlan's twofold requirement. In extending Fourth Amendment safeguards also to public and semi-public places, a "reasonable expectation of privacy" test was introduced for the first time in the USSC case law. Specifically, Justice Harlan stated that a person could claim Fourth Amendment protection where he or she had "exhibited an actual [subjective] expectation of privacy and, second, that the expectation that society is prepared to recognise as 'reasonable'"[996].

In this case, "reasonable expectations of privacy" comprise both a subjective and objective component. The first subjective element is certainly the most problematic. There are many situations in which people cannot expect to have any privacy, either for the time and place, or the (criminal) nature of the activity being carried out[997]. Looking at personal expectations can often lead to the correct outcome in the assessment, but this is not always the case. For instance, subjective expectations could be easily lowered if the government announced the deployment of extensive means of electronic surveillance[998]. Given the fuzzy contours of this criterion, its importance was later downplayed in the USSC case law – including by Justice Harlan[999]. That is why the essential focus of the test is universally placed on the second objective parameter of *reasonableness*.

---

[996] *Katz v. United States*, 389 U.S. 347, 351 (1967), p. 347.
[997] LaFave (1996), p. 386.
[998] LaFave (1996), p. 387.
[999] Id., pp. 387-389; *United States v. White*, 401 U.S. 745 (1971), Harlan dissenting.

In fact, this second requirement is aimed to give a response to the question of *which* expectations of privacy are constitutionally "justifiable". People should be free of *any* risk of being overheard or discovered to claim that their privacy expectations are reasonable[1000]. For instance, in his dissenting opinion in *White*, Justice Harlan observed that a privacy intrusion is unreasonable when the individual's sense of security outweighs the utility of the investigatory activity[1001].

At its core, therefore, the reasonable expectations of privacy test entail a balancing exercise between fundamental rights and collective needs of law enforcement. The background for this exercise is not simply given by the law, but by "the customs and values of the past and present"[1002]. The answer is to be found in social patterns of interaction, norms and values collectively upheld[1003]. This approach has been then confirmed by the Supreme Court too, that in *Oliver v. United States* made reference to "our societal understanding" of what is worthy of "protection from government invasion" as something important in defining which expectations of privacy are reasonable[1004].

In addition, the appeal to a "sense of security" should be understood as implying a prognostic test on the acceptability of certain police surveillance practices. What should be inquired, is whether allowing the police to systematically resort to that type of practice, with only self-restrain to limit them, sacrifices too much of the privacy that should be protected by the Fourth Amendment[1005].

This reasoning is important from a twofold perspective. On the one hand, it partly breaks the problem of the circularity of reasonable expectations, calling for a value judgement on the *future* consequences for society of a given surveillance practice. On the other, the merely individual perspective is put aside to embrace a more *societal* one. In this sense, the Fourth Amendment is not only specifically meant to protect the individual against a given search, which may not even lead to uncover things of great value[1006], but also the features of openness and freedom from governmental intrusion of democratic societies[1007].

The legacy of Katz. Beyond wiretapping, *Katz* was crucial to redefine the basis of Fourth Amendment protection[1008]. Its reasonable expectations of privacy test have indeed been applied in varied contexts, such as aerial surveillance, electronic surveillance of public movements, acquisition of GPS and smartphone location data. These will be examined in the following Sections as relevant for our analysis.

3.1.2. Aerial surveillance

Ciraolo, Dow Chemicals and Riley. After *Katz,* the USSC had the chance to refine the reasonable expectation of privacy test and apply it to aerial surveillance in three different cases[1009]: *California v. Ciraolo*[1010], *Dow Chemical v. United States*[1011], *Florida v. Riley*[1012]. *Ciraolo* was the first of this triad and concerned naked-eye observation of a suspect's backyard from a low-flying plane[1013]. In this decision,

---

1000 LaFave (1996), p. 390.
1001 *United States v. White*, 401 U.S. 745 (1971), Harlan dissenting [emphasis added].
1002 USSC, *United States v. White*, Harlan dissenting.
1003 LaFave (1996), p. 391.
1004 *Oliver v. United States*, 466 U.S. 170 (1984).
1005 LaFave (1996), p. 392.
1006 *Arizona v. Hicks*, 480 U.S. 321 (1987).
1007 LaFave (1996), p. 395.
1008 LaFave (1996), pp. 384-385.
1009 Koerner (2015), p. 1144.
1010 *California v. Ciraolo*, 476 U.S. 207 (1986).
1011 *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986).
1012 *Florida v. Riley*, 488 U.S. 445 (1989).
1013 Wilkins (1987), p. 1101. Santa Clara police department had received an anonymous tip about the existence of a marijuana plantation in Ciraolo's backyard, which at the ground level was protected from sight by two high fences. Police

the Supreme Court excluded that such kind of aerial surveillance could constitute a search under the Fourth Amendment and thus required a prior judicial warrant.

The Court here relied on the "plain view doctrine", an exception to Fourth Amendment protection. It stated that, even though the curtilage was shielded from public street by the fences, it was still to be considered in "plain view" because it could be observed from an aircraft flying in public air space[1014]. Secondly, the Court took into account the kind of technologies that were used to carry out the surveillance[1015]. It considered that "mere" flyovers of airplanes were sufficiently widespread to exclude that the defendant could have high privacy expectations with regard to the activities he was performing in his garage.

Importantly, this reasoning came back later in *Kyllo v. United States*, where the Court compared the aerial surveillance in the *Ciraolo* case with the use of heat sensors to detect the presence of a marijuana nursery in a garage. In this case, however, heat detecting technologies were not considered of "general public use", and thus could not diminish the expectation of privacy that Mr. Kyllo had over the activities that he was performing in his garage.

In *Dow,* the namesake chemicals company refused to grant the Environmental Protection Agency (EPA) access to their two power plants located in its manufacturing facility. Instead of obtaining an administrative warrant for the inspection, the EPA flew aircraft over the property and had photographs taken from altitudes of 12000, 3000, and 1200 feet. In this decision as well, the USSC excluded that this investigatory activity could be equated to a search and thus be subject to the Fourth Amendment.

In *Florida v. Riley*, lastly, the Supreme Court examined whether Fourth Amendment protection could apply to naked-eye aerial observation of a partly enclosed greenhouse. Following up on an anonymous tip, police officers had flown a helicopter four-hundred feet over Riley's greenhouse. Because the greenhouse roof was missing some sections, the officers were able to see inside and spot marijuana plants through naked-eye observation.

Although the Court acknowledged that the greenhouse was within the perimeter of the defendant's house, it stated again that this kind of aerial observation did not fall within the scope of the Fourth Amendment. The absence of sections in the greenhouse roof was decisive: by not fully protecting the contents of the greenhouse, Mr. Riley could not claim a reasonable expectation of privacy with respect to observation from public airspace. As in *Ciraolo*, the also Court considered that helicopter flights were not sufficiently rare in the United States to support a reasonable expectation of privacy from this kind of surveillance.

Balancing factors in aerial surveillance. In the above-mentioned decisions, which were adopted at rather close together in time, the Supreme Court set out some analytical criteria to assess the legitimacy of aerial surveillance measures under the Fourth Amendment: (1) the place where the surveillance occurred, (2) the degree of intrusiveness of the surveillance, and (3) the object of the surveillance itself[1016].

First of all, the Court acknowledged that expectations of privacy were much more heightened in a home backyard rather than in an industrial plant open to public view. Among scholars, this attention to

officers thus flew an airplane over his property, photographing the plantation from an altitude of 1,000 feet (i.e., around 300 metres). Based on these images, the police obtained a search warrant and seized the illicit goods. In the subsequent proceedings, Ciraolo asked to suppress the marijuana evidence as the fruit of an unreasonable search, and his request was initially satisfied by the appeals court. Specifically, the judges held that the defendant had manifested a reasonable expectation of privacy by installing fences of a considerable height.

[1014] USSC, *California v. Ciraolo*.

[1015] Reidenberg (2014), p. 144; Koerner (2015), p. 1146.

[1016] Wilckins (1987), pp. 1101 ff.

the venue impacted by surveillance has been interpreted in the sense that any Fourth Amendment discussion will *always* imply a reference to "place" at the outset, although this should not be considered a decisive criterion in the analysis[1017].

Moreover, in assessing the nature of the venues subject to governmental monitoring, the Court refrained from "abstract geographical considerations", but made multiple reference to the *intimacy* of the activities that are usually carried out within a given place[1018]. Rather than focusing on the naturalistic features of the location at issue, therefore, the Court seems to emphasise the kind of "human contact" that individuals can experience therein[1019], thus giving meaning to the notorious statement that the Fourth Amendment protects people and not places[1020].

Secondly, the degree and the object of the intrusion are the factors that often determine the ultimate result of the balancing exercise[1021]. As for the degree of the intrusion, in *Ciraolo* the Court relied on the absence of physical intrusion of aerial surveillance to exclude the applicability of the Fourth Amendment, a position that directly contradicted the reasoning in *Katz*.

Thirdly, with regard to the object of the surveillance, the Court stated that the protection of physical objects (such as marijuana plantations in a curtilage, or the layout of a manufacturing facility) did not raise the same constitutional concerns as the secrecy of "non-tangible" items like private communications in *Katz*. Regrettably, this approach also stood out as incoherent with respect to the appreciation of the value of the place of surveillance (1), for which an exclusively physical perspective was rejected.

3.1.3. Electronic surveillance of public movements and relationships

Outside the scope of the Fourth Amendment? Traditionally, the Fourth Amendment does not protect "[w]hat a person knowingly exposes to the public". Different kinds of public surveillance, from "fixed surveillance" (e.g., exploiting the use of CCTVs), to "moving surveillance" (e.g., police shadowing) and attendance at certain kinds of public gatherings would thus be excluded from its scope[1022].

The USSC case law and legal scholarship has long struggled to pin down which Fourth Amendment interests are touched by mere visual surveillance[1023]. In *Cardwell v. Lewis*, for instance, the Supreme Court stated that an individual moving around in public in his or her car has no reasonable expectation of privacy[1024]. In *United States v. Knotts*, the Court also examined the question of visual surveillance combined with the monitoring of an electronic device installed in a container, which the suspect was transporting. The Court excluded that the beeper signals emitted by the tracking device constituted a search under the Fourth Amendment, because they only revealed facts and movements that could have been ascertained through visual observation[1025].

In other words, the electronic device was seen as merely instrumental to augment the sensory (i.e., visual) capacities of law enforcement, and their use was not considered to imply a search. They only tracked movements in plain sight, where individuals could not claim to have a reasonable expectation of privacy.

1017 Id, p. 1103.
1018 Id.
1019 Id.
1020 USSC, *Katz v. United States*.
1021 Wilckins (1987), p. 1107.
1022 LaFave (1996), pp. 658 ff.
1023 Id.
1024 *Cardwell v. Lewis*, 417 U.S. 583 (1974), p. 417.
1025 *United States v. Knotts*, 460 U.S. 276 (1983), p. 460; cf. *United States v. Karo*, 468 U.S. 705 (1984).

As these instruments became increasingly available and powerful, however, the Court was drawn to review its traditional position, with the aim of preserving the degree of privacy against government surveillance that existed when the Fourth Amendment was first adopted[1026]. Two notorious decisions in this sense are *Jones* and *Carpenter*. These will be the subject of the next subsections.

3.1.3.1. United States v. Jones

The Fourth Amendment and digital location information. After *Knotts* and *Karo*, the Supreme Court again addressed the problem of surveillance in public places, in light of the new potential of digital technologies to generate new types and amounts of information that would have never been conceived in the 19th and 20th centuries[1027]. This required an interpretative effort by the Court, which had to adapt old constitutional safeguards to unforeseen factual situations (e.g., so-called translation problem[1028]).

This issue was first tackled in *United States v. Jones*[1029], although in partially disappointing terms. The case concerned an FBI investigation into suspected drug smuggling. The FBI had obtained a warrant to bug Jones's vehicle with a GPS tracking device but failed to execute it before the expiration date. Nonetheless, law enforcement still proceeded with tracking the vehicle over a one-month period and acquired over 2,000 pages of data from the device. Jones was later arrested on drug trafficking and sentenced to life imprisonment. During the trial, Jones's motion to exclude the GPS data from evidence was rejected based on the *Knotts* doctrine, according to which people circulating on public roads enjoy no reasonable expectation of privacy in their movements.

In its ruling, the Supreme Court held that placing a GPS tracking device in a suspect's vehicle constitutes a search under the Fourth Amendment because it entailed a physical intrusion in the person's effects. To do so, however, it simply relied on a trespass-based interpretation of the Fourth Amendment, thus evading the issues of data aggregation that emerged after the digital revolution[1030]. While the resolution of the case was clear under the "physical trespass" interpretation of the Fourth Amendment, the nine justices disagreed on how to appropriately translate the constitutional protection in the digital age.

Justice Scalia's majority opinion and Justice Sotomayor's concurrence. Writing for the majority of five Justices, Justice Scalia contended that the issue had to be resolved merely on technical terms, looking at how the Fourth Amendment was understood at the time of its conception. In his view, the presence of an act of physical intrusion upon the suspect's property was enough to evade the application of the *Katz* test, and simply rely on the original meaning of the constitutional provision.

On the contrary, Justice Sotomayor seemed more willing to go beyond this "old-fashioned" interpretation of the Fourth Amendment, and raised concerns over the correct application of the Constitution in a renewed context of pervasive digital surveillance[1031]. In her opinion, the Court had failed to address this aspect and the impact of surveillance technologies that may not even entail a physical trespass[1032].

Justice Sotomayor saw a major danger in the threat to fundamental liberties in a democratic society:

1026 USSC, *Kyllo v. United States*, p. 534.
1027 Washington et al (2019), p. 373.
1028 Cf. Introductory Chapter, §3.1.
1029 *United States v. Jones*, 565 U.S. 400 (2012).
1030 Reindenberg (2014), p. 150; Koops (2014b), p. 260.
1031 Washington et al (2019), p. 375.
1032 USSC, *United States v. Jones*, pp. 1 ff.

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about his or her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility"[1033].

This shows that if one wants to uphold the protection of the constitutional text alive, one needs to make an imaginative effort[1034]. Gathering an amount of information such as that in *Jones* by analogical means would have required hundreds of paid policing officers and informants. In the physical world, policing is legal but its excesses are limited by financial and democratic constraints. Where the large presence of patrols on the streets would encounter strong opposition from the general public, the use of inexpensive and obtrusive technology like GPS trackers can reduce both costs and hostility constraints[1035]. The increasing availability of discrete datapoints to law enforcement may "alter the relationship between citizens and government in a way that is inimical to democratic society"[1036].

Justice Alito's concurrence. Likewise, Justice Alito focused on the issue of the increasing availability of surveillance technologies: "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but *practical*. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken"[1037].

Nonetheless, he warned about the unsuitability of the "reasonable expectation of privacy test" to address the challenges brought by digital surveillance technologies. In his view, *Katz* relies upon the hypothetical assumption that people have a well-defined and set standard of privacy expectations in society. What it does not take into account is that technologies in themselves can change those expectations: new technologies can bring increased convenience, which may be accepted by society to the detriment of security and privacy[1038]. And even if such developments are not welcomed, their integration in society may be an inevitable outcome.

Critically, Alito's concurring opinion highlights the negative impact that technologies can have on social practices regulating the flow of information, and how the tool of reasonable expectations may not be sharp enough to uphold the constitutional protection of privacy. In this sense, the commercial availability of specific surveillance technologies (as in *Ciraolo* and *Kyllo*) may not an appropriate factor to establish the right level of privacy expectations[1039], especially in contexts where their gradual use is an unavoidable trend.

On a different note, Alito joined Sotomayor in criticising the trespass/property-based conception of the Fourth Amendment that was adopted by the majority. He contended indeed that "the attachment of the GPS device was not itself a search; if the device had not functioned or if the officers had not used it, no information would have been obtained. And the Court does not contend that the use of the device constituted a search either"[1040]. Importantly, Alito found the actual legal issue in the *prolonged* threat of location surveillance[1041]. *Time* is thus taken as a criterion to assess the intrusiveness of the

[1033] USSC, *United States v. Jones*, p. 3, Sotomayor concurring.
[1034] Washington et al (2019), p. 376.
[1035] USSC, *United States v. Jones*, pp. 3-4, Sotomayor concurring.
[1036] Id., p. 4.
[1037] Id., p. 12, Alito concurring.
[1038] Id., p. 10, Alito concurring.
[1039] Reidenberg (2014), pp. 145-146.
[1040] USSC, *United States v. Jones*, p. 2, Alito concurring.
[1041] Id., pp. 12 ff.

monitoring operation. As we will see later on, this suggests how the *Katz* test needs to encompass further parameters to address surveillance phenomena that are increasingly dynamic and multi-purposeful.

3.1.3.2. Carpenter v. United States

Katz and Miller confronted with modern cell phone surveillance. Carpenter v. United States[1042] first examined whether the acquisition of cell-site location information (CSLI) is a search under the Fourth Amendment, requiring a prior judicial warrant for probable cause.

Notoriously, cell phones function by continuously connecting to radio antennas called "cell sites". When a phone connects to a cell site, it generates time-stamped cell-site location information (CSLI) that is stored by wireless carriers for business purposes (e.g., billing). Nonetheless, this information has also increasingly become invaluable to law enforcement, as these data can provide for important information to locate a subject in time and space and infer other sensitive details of his or her private life.

In *Carpenter,* the Federal Bureau of Investigation (FBI) had obtained CSLI for Mr. Carpenter's phone and chronicled the suspect's movements over 127 days, demonstrating that the device was near four robbery locations. Based on this evidence, Carpenter was convicted for the robberies.

In this case, the Supreme Court dealt with the challenge of applying Fourth Amendment safeguards to a new phenomenon: the possibility to reconstruct an individual's past movements through the record of his or her cell phone location metadata. According to the Court, the acquisition of this kind of digital data (i.e., CLSI information stored by a third party) did not fit into existing precedents.

On the one hand, there was the question of a person's expectation of privacy with regard to his or her physical movements, which had been recently addressed in *Jones* with respect to GPS data. On the other, the Court needed to (re)examine which kind of privacy expectations a person could claim with regard to information voluntarily turned over to third parties. The so-called "third party-doctrine" had indeed been a long-standing exception to Fourth Amendment protection and allowed government agents to subpoena transaction records from private service providers (e.g., banks, communication companies) without breaching customers' reasonable expectations of privacy. In *Miller v. United States,* this reasoning was first applied to the information that individuals voluntarily share with their banks[1043].

In addressing the first question, the Court importantly stated that "a person does not surrender all Fourth Amendment protection by venturing into the public sphere"[1044]. Quite the contrary, referring to *Katz*, the Court indicated that "what [one] seeks to preserve as private, *even in an area accessible to the public*, may be constitutionally protected"[1045].

Even if CLSI records are made for commercial purposes, their storage does not exclude that individuals may retain an expectation of privacy as for their physical location. Like GPS, indeed, CLSI data is time-stamped and thus allows a detailed picture of one's intimate life to be built, comprising not only a person's movements, but also his or her "familial, political, professional, religious, and sexual associations"[1046]. In addition, CLSI seem to pose even greater privacy concerns than GPS data attached to a vehicle. Differently from the bugged container in *Knotts* or the car in *Jones*, a cell phone is now "almost a feature of human anatomy"[1047], which makes cell phone tracking a surveillance practice of

---

[1042] USSC, *Carpenter v. United States.*
[1043] *United States v. Miller*, 425 U.S. 435_(1976); *Smith v. Maryland*, 442 U.S. 735_(1979) (on data shared with telephone companies).
[1044] USSC, *Carpenter v. United States*, p. 12.
[1045] USSC, *Katz v. United States*, pp. 351-352 [emphasis added].
[1046] USSC, *Carpenter v. United States,* p. 12.
[1047] Id., p. 13.

even wider outreach. Also, CLSI information is continuously logged in for over 400 million people in the United States, and law enforcement does not even need to know if they want to monitor a particular subject or not to get the most of information[1048]. The accuracy of CSLI is rapidly reaching the level of GPS, as the number of cell sites has proliferated, especially in *urban areas*[1049]. In the Court's view, all these factors clearly pointed to the particular invasiveness of the acquisition of cell phone metadata, which deserved to be included in the area of constitutional protection.

As for the application of the third-party doctrine to CLSI information, the Court considered that "cell phone location is not truly "shared" as one normally understands the term"[1050]. It further acknowledged that there is great difference between the limited categories of personal information that were the object of *Smith* and *Miller*, and the detailed chronicle of one's movements that nowadays can be inferred from data collected by wireless carriers[1051]. Moreover, carrying a cell phone around is inescapable to participate in modern society[1052]. At the same time, virtually any activity on a cell phone generates metadata, from incoming calls, texts, emails[1053]. Based on these considerations, the Court refused to extend the scope of the third party doctrine to CLSI information, whose acquisition was thus qualified as a search under the Fourth Amendment.

3.1.4. Convergences and gaps in the reasonable expectation of privacy test

From places to tools of surveillance. Undoubtedly, the reasonable expectation of privacy test has helped the Supreme Court to overcome a strictly physical understanding of the Fourth Amendment and privacy protection (as in *Olmstead*). Truth be told, the *Katz* doctrine has not completely supplanted the traditional conception of the constitution safeguard, which still survives today as shown by majority opinion in *Jones*. The idea of reasonable expectation of privacy is only an alternative test, useful to tackle intrusions that do not involve any physical trespassing element, and which can thus be more apt to address the dangers of digital surveillance.

Probably because of its flexibility, however, the reasonable expectation of privacy test has not really brought clarity to USSC jurisprudence. Harlan's opinion on *White* – as well as later positions taken by Justices Sotomayor and Alito highlighted the dangers of a purely subjective understanding of reasonable expectations. Relying exclusively on what people perceive as "normal" practice in society can expose the test to unjust results, especially as severely intrusive technologies become commercially available and of common use among the population.

As said, this danger echoes what Helen Nissenbaum calls "the tyranny of the normal" in her framework of contextual integrity. Indeed, changes brought by technologies may go unnoticed for a long period of time, causing a huge fracture in social practice. When these ruptures finally surface before the public or the courts, "the new normal" may already have made inroads in the fabric of society[1054].

Systemising the components of the test of reasonable expectations. Against this background, the test should gravitate towards a more *objective* understanding of reasonable expectations, which supersedes mere individual subjective expectations about social practice. Specifically, the test should involve both (1) an

[1048] Id., pp. 13-14.
[1049] Id., p. 14 [emphasis added].
[1050] Id., p. 17.
[1051] Id., pp. 15-17.
[1052] Id., p. 17.
[1053] Id.
[1054] Nissenbaum (2009), p. 161.

assessment of overarching principles regulating the flow of information in that particular context; (2) a prognosis about the potential future consequences of widely adopting a specific surveillance technology.

This second part of the test could be one of the most important contributions of the USSC version of the assessment of reasonable expectations. The questions to be asked should be the following: (how) will technology change the capabilities of public and private actors to interfere upon individuals' private lives? Will it do so beyond what is acceptable in a democratic society? Importantly, a negative assessment of these profiles would not always lead to a simple ban of given surveillance practices, but rather to the extension of specific constitutional protections (e.g., a judicial warrant in this case) to previously unregulated monitoring activities. With reference to the Fourth Amendment, Justices Sotomayor and Alito contended that a relevant factor in addressing these questions is whether technologies significantly modify law enforcement sensory capabilities, providing them with resources that would likely be opposed by the public if physically apparent to them.

Moreover, a fundamental shift in what should be the focus of constitutional privacy protection seems at play: rather than caring for the concrete *spaces* of surveillance, one should be concerned with the *tools* of monitoring.

Certainly, the analysis of privacy interferences should not exclude any spatial consideration altogether; the meaning attached to particular venues (included public ones) should indeed be leveraged to argue for the application of constitutional protections beyond the boundaries of the home. In this sense, the analysis made by the USSC in *Ciraolo* and *Dow* remind us of the spatial dimension of privacy and the meaning of *places*[1055].

Other questions, like the features of the employed technology, should acquire more weight in the overall assessment. As suggested by Alito in *Jones*, the extension of the surveillance timeframe allowed by new tools should also be taken into consideration. The same goes for how data could be further used (e.g., capabilities for data aggregation). We will see below how such parameters can be systematised and applied to the smart city context[1056].

3.2. Privacy expectations in the case law of the ECtHR

From the home to the right to lead a private life in public contexts. In general, the evolution of Art. 8 in the ECtHR's case law suggests that the right to private life goes well beyond the protection of specific spaces designed as "private"[1057]. Values like human dignity and individual autonomy, which are pivotal for individual self-development, also lie outside the remit of the home and have been explicitly identified as normative justifications of the right enshrined in Art. 8 of the Convention[1058]. In light of this, the Court has progressively extended its protection to people's interactions with others, even if these occur in public venues[1059]. Against this backdrop, the following subsections will provide an account of the ECtHR's case law in relation to privacy in public in general[1060], and then to reasonable expectations of privacy specifically[1061].

[1055] See §2.2.
[1056] See §3.3.
[1057] Galič (2019), p. 269; Schabas (2017).
[1058] Cf. §2.1.1. See ECtHR, *Pretty v. United Kingdom*, and ECtHR, *von Hannover v. Germany,* §50.
[1059] ECtHR, *Peck v. the United Kingdom,* judgment of 28 January 2003, App. no. 44647/98; ECtHR, *von Hannover v. Germany*; ECtHR, *Bărbulescu v. Romania*, judgment of 5 September 2017, App. no. 61496/08; ECtHR, *Gillan and Quinton v. United Kingdom,* judgment of 12 January 2010, App. no. 4158/05, §6; ECtHR, *Pretty v. United Kingdom*, §61; ECtHR, *Vukota-Bojić v. Switzerland,* judgment of 18 October 2016, App. no. 61838/10, §62.
[1060] See §3.2.1.
[1061] See §3.2.2.

3.2.1. Privacy in public in the ECtHR's case law: A brief overview

The Commission's earlier cases: No protection for "public behaviour" in public. The evolution of the Court's (and Commission's) jurisprudence has been significant in this sense. In earlier cases, the Court excluded the applicability of Art. 8 ECHR where (private) activities were carried out in public contexts[1062].

In *X v. UK*, the Commission considered manifestly ill-founded the applicant's claim that his right to private life had been violated because some pictures portraying him had been taken during a public demonstration, an essentially public activity in which he had voluntarily taken part[1063].

Likewise, in *Friedl v. Austria*, the applicant was photographed while participating in a sit-in demonstration organised by homeless people in an underground pedestrian passage in Vienna. Upon their arrival, the police asked the participants to clear the place as they were obstructing pedestrian traffic. As the protesters initially refused to obey, police officers noted down their identities and took their photographs to initiate an investigation against them for breaching the Austrian Road Traffic Regulations. Their personal data was then stored in a file by the Vienna Federal Police Department. The Commission excluded that there had been an intrusion into the "inner circle" of the applicant's private life (as if the authorities had entered his home). The photographs referred to a *public incident*, a manifestation held *in a public place*, to which the applicant was *voluntarily taking part*. Importantly, these photos had been taken only to record the features of the manifestation (e.g., the sanitary conditions) and to initiate an investigation against the participants for offences against the Road Traffic Regulations"[1064].

In *Herbecq and Association "Ligue des droits de l'homme" v. Belgium,* these factors were once again applied by the Commission[1065]. It noted that the mere visual observation of public or semi-public spaces through technology for security purposes only amounts to monitoring "public behaviour" and does not call into question one's right to private life if data is not stored for subsequent use[1066]. Importantly, this first approach echoes the one undertaken by the USSC in *Knotts* and *Karo,* where the installation of signalling devices was excluded from the scope of the Fourth Amendment because it only provided police officers with an increased perception of activities occurring in the public space. A strictly spatial approach to private life protection was upheld in these decisions. A distinction between private and public behaviour in public contexts was drawn, to the detriment of those social and political activities that should be protected by privacy.

Later on, the Court diverted this reasoning to a more sophisticated distinction between the public and private *sphere*[1067]. In drawing this line, voluntary participation in public events was again a relevant factor in excluding the applicability of Art. 8 of the Convention[1068]. For instance, relying on the idea of reasonable expectations of privacy, in *Friend and Others v. United Kingdom,* the Court ruled out that fox hunting could fall within the scope of the right to private life. The Court considered this activity as having an "essentially public nature", based on diverse criteria: (1) the fact that it was carried out in the open air; (2) the number of participants and spectators; (3) its far connection to the development of *personal autonomy* and *social interactions*[1069].

1062 Cf. Galič (2019), pp. 289 ff.
1063 Galič (2019), p. 290.
1064 ECommHR, *Friedl v. Austria*, decision of 19 May 1994, App. no. 15225/89, §49 [emphasis added].
1065 Galič (2019), p. 290.
1066 ECommHR, *Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium*, decision of 14 January 1998, App. nos. 32200/96 and 32201/96, p. 97.
1067 Galič (2019), p. 291.
1068 ECtHR, *Friend and Others v. United Kingdom*, judgment of 24 November 2009, App. nos. 16072/06 and 27809/08, §42; ECommHR, *Friedl v. Austria*, §§49-52; ECtHR, *Peck v. the United Kingdom,* §§61-62.
1069 ECtHR, *Friend and Others v. United Kingdom*, §43. In the Court's view, fox hunting was rather connected to a sense of enjoyment and personal fulfilment.

With regard to political protest activities, however, scholars have criticised the exclusion of the applicability of Art. 8. This suggests that the Court may downplay the value of the right to privacy in (essentially) public activities, both those relating to informal civic activities (e.g., sociability in public space) and formal civic activities (e.g., peaceful assembly and protesting)[1070].

The right to lead a private social life. References to the social dimension of private life gradually gained traction in the Court's case law, as part of a generally extensive approach to Article 8[1071]. In *P.G. and J.H. v. the United Kingdom*, the Court explicitly recognised that there is "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'"[1072]. Because of its broad scope, the right enshrined in Art. 8 ECHR can encompass a wide range of aspects, such as the right to (gender) identity and personal autonomy, sex life and orientation, and importantly "the right to establish and develop relationships with other human beings and the outside world"[1073].

Notably, this right has been considered to also extend to activities of professional or business character[1074]. This process culminated in *Bărbulescu v. Romania*, where a new interpretative profile of Art. 8, the "right to lead a private social life", was explicitly introduced[1075]. In a subsequent judgment, *FNASS and Others v. France*, the Court further contended that the right to lead a private social life "may include professional activities or activities taking place *in a public context*"[1076].

3.2.2. The concept of reasonable expectations of privacy in the ECtHR's case law

A limited and confusing application. The extension of the scope of the right to privacy outside the physical boundaries of the home entails the use of instruments assessing level of privacy in public contexts. If, despite its limitations, this interpretative effort has been clear and systematised in the USSC's jurisprudence with the reasonable expectations of privacy test, the same cannot be said about the Strasbourg Court. Indeed, the concept of reasonable expectations of privacy is far more recent in the ECtHR's jurisprudence compared to the USSC's and has been confusingly and incoherently applied so far[1077]. Since the very first decision, *Halford v. United Kingdom* (1997), the concept of reasonable expectation of privacy has seemingly been referred to in Strasbourg case law only 26 times[1078]. Sometimes, the Court has also used the term "legitimate", rather than "reasonable" to identify privacy expectations, adding further confusion to this already fuzzy concept[1079].

Origins of the concept in the Court's case law. The origins of the test in the ECtHR's case law are unclear. Analysing the arguments put forward in *Halford*, the concept of reasonable expectations was allegedly

---

1070 Galič (2019), p. 293.
1071 Harris et al (2014), p. 525.
1072 ECtHR, *P.G. and J. H. v. United Kingdom,* judgment of 25 September 2001, App. no. 44787/98, §56; ECtHR, *Peck v. the United Kingdom,* §57.
1073 ECtHR, *Burghartz v. Switzerland*, judgment of 22 February 1994, App. no. 16213/90, §24; ECommHR, *Friedl v. Austria*, §44; ECtHR, *P.G. and J. H. v. United Kingdom,* §56; ECtHR, *Amann v. Switzerland*, judgment of 16 February 2000, App. no. 27798/95, §65.
1074ECtHR, *Niemietz v. Germany*, judgment of 16 December 1992, App. no. 13710/88, §29; ECtHR, *Amann v. Switzerland*, §65.
1075 ECtHR, *Bărbulescu v. Romania*, §70. Galič (2019, p. 270) notes that "the right to lead a private social life can already be found in the second section judgment in ECtHR, *Boulois v. Luxembourg*, judgment of 3 April 2012, App no. 37575/04, §63. However, the Grand Chamber, which decided finally on the case in 2012 did not refer to the right".
1076 ECtHR, *National Federation of Sportspersons' Associations and Unions (Fnass) and Others v. France*, judgment of 18 January 2018, App. nos. 48151/11 and 77769/13, §151 [emphasis added].
1077 Galič (2019), p. 280.
1078 See search methodology down below.
1079 See, e.g., ECtHR, *von Hannover v. Germany,* §51.

introduced before the Court by the British government, which first asked for its application[1080]. It has been noted indeed that this benchmark has been mentioned mostly in cases against the United Kingdom, which obviously shares strong ties with American common law jurisdictions, where the test first originated[1081]. The Court did not wait too long to absorb the concept, and in the subsequent case *P.G. and J.H. v. the United Kingdom* referred to the standard on its own initiative[1082]. In the ensuing years, references to the standard have increased, although the Court refrained from extensively laying down its relevant criteria – even with the disappointment of some Court judges[1083].

Selection of decisions and contexts of application. To identify relevant decisions, a search was conducted in the official HUDOC database[1084] in March 2022. The specific phrase "reasonable expectation of privacy" was queried and Art. 8 ECHR was used as the filter criterion. The output of the query was 26 decisions.

Those where the concept of reasonable expectations of privacy was only invoked by the parties, but not picked up by the Court in its own reasoning, were excluded from the pool[1085]. Cases where the context of application related to non-public venues different from the home (e.g., a private sex club), which do not really match the scope of this dissertation, were also omitted[1086].

Subsequently, four thematic clusters of decisions were identified, according to the context in which the test was applied: (1) surveillance in the workplace; (2) surveillance in public places; (3) online environments (i.e., protection of dynamic IP addresses); (4) dissemination of information by journalists. The latter will not be specifically analysed, as it does not fit within the particular context of this inquiry[1087]. Nonetheless, references to the principles adopted in those decisions will be integrated in the analysis where relevant (especially with reference to the criterion of further dissemination of personal information). The following subsections will thus focus on surveillance in the workplace[1088], in public places[1089] and in online environments[1090]. Before delving into this, some general clarifications on the nature and scope of the test will be dealt with.

An overarching criterion or one among many? One of the main contentious issues with the "European version" of the reasonable expectation of privacy test is whether this should be considered as an overarching benchmark, comprising diverse sub-factors, or as one assessment criterion among others. While the first option has been explicitly chosen by the USSC, the opposite solution seems to have been embraced by the ECtHR, which has often declared that

---

1080 ECtHR, *Halford v. United Kingdom,* judgment of 25 June 1997, App. no. 20605/92, §43.
1081 Galič (2019), p. 280.
1082 ECtHR, *P.G. and J. H. v. United Kingdom,* §57.
1083 See, e.g., the separate opinions of Judge Zupančič (e.g., in *Bohlen v. Germany* and the 2004 *Hannover v. Germany*) and the lengthy concurring opinion of Judge Yudkivska, joined By Judge Bošnjak, in *Benedik v. Slovenia* (cf. below §4.2.1.3).
1084https://hudoc.echr.coe.int/eng#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22}. Accessed 17 March 2022.
1085 These decisions are: ECtHR, *Ažukaitienė v. Lithuania*, judgment of 21 November 2019, App. no. 59764/13; ECtHR, *Sorvisto v. Finland*, judgment of 13 January 2009, App. no. 19348/04; ECtHR, *Mosley v. United Kingdom*, judgment of 10 May 2011, App. no. 48009/08.
1086 One decision was identified in this sense: ECtHR, *Pay v. United Kingdom*, judgment of 16 September 2008, App. no. 32792/05.
1087 These decisions are: ECtHR, *Bohlen v. Germany,* judgment of 19 February 2015, App no. 53495/09; ECtHR, *J.S. v. United Kingdom*, judgment of 3 March 2015, App. no. 445/10; ECtHR, *Mosley v. United Kingdom*; ECtHR, *von Hannover v. Germany*; ECtHR, *Ernst August von Hannover v. Germany*, judgment of 19 February 2015, App. no. 53649/09.
1088 See §3.2.1.1.
1089 See §3.2.1.2.
1090 See §3.2.1.3.

> "[t]here are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy *may be a significant, although not necessarily conclusive, factor*"[1091].

At the same time, however, the Court does not seem to have addressed the question of which other criteria – besides reasonable privacy expectations – should contribute to such assessments. For instance: Is the fact that a person is voluntarily taking part in a public event a benchmark in its own right to assess the applicability of Art. 8 ECHR, or is it a factor contributing to augmenting or diminishing one's expectation of privacy in public? The Court has never been clear in this respect; still, answering this point would be important to achieve a more consistent application of the standard at issue in the Court's jurisprudence.

The purview of reasonable expectations of privacy. Similarly, doubts have been raised among scholars as to which aspects of the multifaceted right to private life are covered by reasonable expectations of privacy. On the one hand, some have cautiously claimed that the test should embrace different components of the right to private life, with special reference to personal choice claims (i.e., the right to self-determination)[1092].

On the other, some seem to look at reasonable expectations of privacy as an independent profile within Art. 8, competing with other elements of the right at stake, like the "right to lead a private social life"[1093]. Nonetheless, there is not much in the Court's jurisprudence allowing discernment about which aspects of private life are covered by the reasonable expectations of privacy test. At most, the acknowledgement of a right to lead a private social life could be one aspect pertaining to one's expectation of privacy in the workplace and public venues. Generally, reasonable expectations should rather work as an indicator of how much we can expect to enjoy a right to self-determination, to gender identity, to lead a private social life in public places.

From the ontological perspective, the idea of reasonable expectation of privacy should be identified as a test having a *procedural* nature. In other words, it should be understood as a tool to assess whether the right to private life applies at all. It should thus refer to *all the substantial* components of Art. 8 of the Convention, as identified by the Court, e.g., the right to (gender) identity and personal autonomy, sex life and orientation, and the right to establish and develop relationships with other human beings and the outside world[1094]. Therefore, reasonable expectations of privacy should not be seen as a competing element with respect to the right to self-determination, or the right to lead a private social life.

Scope of application: Art. 8(1) or Art. 8 (2) ECHR? So far, the ECtHR has used the benchmark of reasonable expectations to determine whether Art. 8 of the Convention should apply at all in cases involving privacy interferences in the public arena. References to the concept in the jurisprudence are

---

[1091] ECtHR, *P.G. and J. H. v. United Kingdom,* §57; ECtHR, *Peck v. the United Kingdom,* §58; ECtHR, *Perry v. United Kingdom*, judgment of 17 July 2003, App no. 63737/00, §37; ECtHR, *Vukota-Bojić v. Switzerland,* §54 [emphasis added]. Cf. also ECtHR, *Köpke v. Germany*, judgment of 5 October 2010, App. no. 420/07.

[1092] Gómez-Arosteguei (2005), pp. 176-177.

[1093] Galič (2019), p. 282.

[1094] Cf. ECtHR, *Burghartz v. Switzerland*, §24; ECommHR, *Friedl v. Austria*, §44; ECtHR, *P.G. and J. H. v. United Kingdom,* §56; ECtHR, *Amann v. Switzerland*, §65.

indeed concentrated in preliminary sections focusing on the applicability of the right to private life[1095], although this is not always the case[1096].

This raises the question of whether the standard at stake is not only useful in the interpretation of Art. 8(1), but also in the proportionality test required by Art. 8(2) of the Convention. The dilemma here is posed by the use of the specifier "reasonable" to define the nature of the expectations. As noted with respect to *Katz*, the element of reasonableness hints at the constitutional *justification* for the interference, that is what should be deemed as acceptable in a democratic society[1097]. Of course, this wording hints at the necessity test enshrined in Art. 8(2) ECHR and suggests that the reasonable expectation of privacy test may imply some kind of balancing on its own in the European framework as well.

In reasonable expectations of privacy cases, indeed, the assessments performed under Art. 8(1) and 8(2) of the Convention may also be strictly intertwined: a finding of a strong reasonable expectation of privacy under the first paragraph may indeed translate into a stricter proportionality test in the second one. Some reflection on this point will follow in the analysis of the case law below.

Objective of the analysis. The preliminary remarks presented so far have provided a glimpse of the scattered application of the test of reasonable expectations of privacy in the ECtHR's case law. The incoherence in the scope, nature and contents of this normative benchmark has been leveraged by scholars to downplay the importance of reasonable expectations in the jurisprudence of Strasbourg[1098]. However, a more objective and consistent framework in the European system could arguably bring a useful contribution to how privacy issues are addressed today in public contexts such as smart cities. Therefore, the objective of the ensuing paragraphs is to provide an integrated analysis of reasonable expectation of privacy references in the case law of the Court, with the aim of systematising relevant criteria and later apply them to public IoT environments.

3.2.1.1. Surveillance in the Workplace

Communication monitoring. As announced before, the first case in which the Court employed the reasonable expectation of privacy test was *Halford*. The applicant was at the time the highest-ranking female police officer in the United Kingdom and had unsuccessfully applied several times for a promotion. After filing a claim for gender discrimination, she also alleged that members of her department had intercepted calls made from her office telephones, for the purposes of gathering evidentiary material for the discrimination proceedings. To establish the applicability of Art. 8, the Court highlighted that Halford could claim a reasonable expectation of privacy over her phone calls, based on *different reinforcing factors*[1099]. Firstly, there was no evidence of any warning that her calls would be liable to interception; secondly, the office was for her sole use, and one of the telephones at her disposal was explicitly designated for her private use. Thirdly, she had been reassured that that phone could be used to make calls for the purposes of her gender discrimination suit[1100].

Following *Halford*, different cases dealt with the electronic interception of communications in the workplace. In *Copland v. United Kingdom*, the applicant worked in a college of higher education (a statutory body administered by the State), as a personal assistant to the deputy principal. From the end

[1095] See, e.g., ECtHR, *Peck v. the United Kingdom,* §58; ECtHR, *Bărbulescu v. Romania*, §73; ECtHR, *Benedik v. Slovenia,* judgment of 24 April 2018, App. no. 62357/14, §101; ECtHR, *López Ribalda and Others v. Spain*, judgment of 17 October 2019, App. nos. 1874/13 and 8567/13, §89.
[1096] Cf. ECtHR, 19 February 2015, *Ernst August von Hannover v. Germany*, App. no. 53649/09, §52.
[1097] See §4.1.1. Gómez-Arosteguei (2005), p. 181.
[1098] See Galič (2019), pp. 280 ff.
[1099] ECtHR, *Halford v. United Kingdom,* §45.
[1100] Id.

of 1995, her telephone, e-mail and internet usage were subjected to monitoring at the deputy principal's request. According to the UK Government, this was in order to ascertain whether the applicant was making excessive use of college facilities for personal purposes. In this case too, the Court referred to the absence of warnings to the applicant that her calls would be liable for interception to establish that she had a reasonable expectation of privacy in that context[1101]. Nonetheless, the Court only briefly mentioned the concept, without going into the details of which other factors could be included therein.

In 2017, a Grand Chamber judgment intervened on the topic. The case *Bărbulescu v. Romania* concerned the decision of a private company to fire the applicant after monitoring his electronic communications and accessing their contents in the workplace. The applicant complained that his employer's decision was based on a breach of his privacy and that the domestic courts had failed to protect his right to respect for his private life and correspondence. Applying the reasonable expectation of privacy test, the Court first remarked that the use of instant messaging apps is one of the major forms of communication allowing people to lead a private social life[1102]. It also highlighted that the notion of "correspondence" under Art. 8 ECHR also applies to communications sent from a work computer.

Nonetheless, unlike previous cases, the Court took notice that the employer had instructed his employees to refrain from personal activities and interaction in the workplace[1103]. For this purpose, a system of internet-use surveillance had been put in place by the company, although it was not probably clear to the applicant whether he had specifically been targeted and whether the (intimate) contents of his communications were also monitored[1104]. Moreover, the applicant further pointed out that the social media account he used to exchange messages was private and the password was known only to him[1105]. Against this confusing background, the Grand Chamber chose again not to take a clear stance on the matter of reasonable expectations of privacy in the workplace, and maintained that:

> It is open to question whether – and if so, to what extent – the employer's restrictive regulations left the applicant with a reasonable expectation of privacy. Be that as it may, an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary[1106].

Based on these considerations, the Court established the applicability of Art. 8 ECHR, even though the question of the impact of the employer's instructions was left unaddressed. In the end, a breach of the right at stake was also established, since the national courts had failed to strike a fair balance between the interests at stake.

Video-surveillance at the workplace. Another set of cases focused on the use of video-surveillance in the workplace. In *Antović and Mirković v. Montenegro*, the Court examined the case of two university professors who complained about the installation of video surveillance in areas where they taught. They contended that they had had no effective control over the information collected and that the surveillance was unlawful. Once again, the Court applied the standard of reasonable expectation of privacy and firstly underlined that the surveilled areas were the *workplaces* of the professors, "where they not only teach students, but also interact with them, thus developing mutual relations and constructing

[1101] ECtHR, *Copland v. United Kingdom*, judgment of 3 April 2007, App. no. 62617/00, §42.
[1102] ECtHR, *Bărbulescu v. Romania*, §74.
[1103] Id., §75.
[1104] Id., §§ 76-78.
[1105] Id., §79.
[1106] Id., §80.

their social identity"[1107]. As in *Köpke*, the Court had found that covert surveillance in the workplace constituted a serious interference upon Art. 8, the same was reiterated for the non-covert video surveillance system implemented in the case at issue[1108]. Citing the Grand Chamber in *Bărbulescu*, the Court stated that even when employers explicitly set restrictions to workers' rights to privacy, this cannot reduce the latter's expectations to lead a private social life to zero[1109]. Therefore, the Court considered Art. 8 to be applicable and found a violation of the applicants' right to private life, as the implementation of video surveillance system did not have any legal basis in domestic law.

The issue of the use of hidden cameras in private offices was then tackled in *Haldimann* and *Akhlyustin*. In *Haldimann and Others v. Swizterland*, four journalists had recorded and broadcast the interview of a private insurance broker using a hidden camera, as part of a television documentary denouncing misleading advice offered by insurance brokers. The applicants were later condemned to pay fines for breaching the broker's right to private life and later lodged a complaint before the ECtHR, objecting that those sanctions amounted to a disproportionate interference in their right to freedom of expression.

In the first case of its kind, the Court found a violation of Art. 10 ECHR. Even if the broker was not a public figure and had not consented to being filmed, he could have claimed to have a reasonable expectation of privacy in relation to the conversations taking place with one of the journalists[1110]. Nonetheless, the importance of his privacy expectations was downsized by the Court, as the journalists' reports had not focused on the broker himself, nor were the conversations held in the latter's private offices[1111]. Based on these factors, the Court deemed that the interference with the broker's private life had not been serious enough, and could be overridden by the public interest in disseminating information about malpractice in the field of insurance brokerage.

Instead, *Akhlyustin v. Russia* concerned a regional electoral commissioner who had been monitored in his work office by a hidden camera, and later condemned at trial for abuse of power based on the footage obtained. At the outset, the Court observed that the applicant had not been warned that his office and communications could be subject to monitoring. Thus, he had a reasonable expectation of privacy in that context[1112]. In this sense, it was also relevant for the Court that the footage had been stored for further use, specifically for evidentiary purposes in criminal proceedings. All these things considered, the Court deemed that Art. 8 of the Convention was applicable, and later found that the surveillance system to which the applicant had been subjected was not "in accordance with the law"[1113].

The Court came back to the topic of video surveillance in the workplace with the Grand Chamber judgment *López-Ribalda and Others v. Spain*. The case concerned the implementation of a partly covert video-surveillance system in a supermarket. The footage revealed that some of the employees were stealing merchandise at the tills, which led to their dismissal. The applicants complained about the installation of the covert video-surveillance and the fact that Spanish courts had considered fair the use of such materials as grounds for termination of their contract. In its reasoning, the Court affirmed that different elements may indicate whether one's private life is at stake outside the boundaries of one's home or private (e.g., professional) premises. A person's reasonable expectations of privacy may be a

[1107] ECtHR, *Antović and Mirković v. Montenegro*, judgment of 28 February 2018, App. no. 70838/13, §44.
[1108] Id.
[1109] Id.
[1110] ECtHR, *Haldimann and Others v. Switzerland*, judgment of 24 May 2015, App. no. 21830/09, §60.
[1111] Id. *Contra* separate opinion Judge Lemmens, p. 18, note 2.
[1112] ECtHR, *Akhlyustin v. Russia*, judgment of 7 November 2017, App. no. 21200/05, §39.
[1113] Id., §46.

significant, although not necessarily conclusive, factor in this assessment[1114]. Examining the concrete context of application of the surveillance system, the Court importantly observed that the applicants' workplace:

> "[…] a supermarket, was *open to the public* and that the activities filmed there, namely the taking of payments for purchases by the customers, were not of an intimate or private nature. Their *expectation* as to the protection of their private life was thus necessarily *limited*"[1115].

As to whether personal data had been processed beyond what could be reasonably foreseen[1116], the Court remarked that Spain had a precise and detailed regulatory framework for CCTV surveillance[1117]. Besides, the applicants had been made aware that video cameras had been installed in the supermarket. While some of these were visible to the employees, others were not; thus, the applicants had a reasonable expectation that they would not be recorded by the cameras in the other areas of the shop without prior notification[1118]. Based on these considerations, the Court concluded for the applicability of Art. 8. Nonetheless, it pointed out that the applicants' expectations of privacy were rather limited: a further reference to this element appears also in the ensuing proportionality assessment under Art. 8(2), as will be shown next[1119].

Office and home searches. Another set of decisions focused on searches conducted on private premises, like professional offices and mobile devices found in the home. First of all, both *Peev* and *Steeg and Wenger* focused on offices searches performed at premises relating to public authorities (e.g., police stations and universities). In both cases, the Court performed the reasonable expectation of privacy test to determine the applicability of the right to private life[1120]. In *Peev* the Court found that the applicant (a criminologist working at a police station) had a reasonable expectation of privacy at least in relation to his cubicle, as it is normal practice in shared offices[1121]. This implicit arrangement of typical workplace relations had not been contradicted in any way by the employer's instructions[1122]. Importantly, the fact that the workplace was located in public premises could not in any way alter these evaluations, an argument that could be extended to any search conducted in public venues[1123]. Similarly, in *Steeg and Wenger v. Germany* it was found that the plaintiffs could not have expected to have their offices subjected to inspections, even if these were located in a university building. Therefore, Art. 8 ECHR was deemed applicable in both cases.

In *Garamukanwa v. United Kingdom* the Court took a different stance. The case concerned the dismissal of an employee (the applicant) who had harassed two of his co-workers. After a complaint was filed, the police started investigation against the applicant, and during a house search some incriminating material was seized from his phone. Based on this evidence, the applicant was later dismissed. In examining the case, the Court considered that the applicant could not claim to have a reasonable expectation of privacy because his "conduct took place *in public* and it was a *criminal offence*, which is normally a matter of legitimate concern to the public and ought to have been disclosed by him

---

1114 ECtHR, *López Ribalda and Others v. Spain*, §89.
1115 Id., §93.
1116 Id., §90.
1117 Id., §93.
1118 Id.
1119 Id., §125. See below §3.2.1.4.
1120 See ECtHR, *Peev v. Bulgaria*, judgment of 26 July 2007, App. no. 64209/01, §§34 ff.; ECtHR, *Steeg and Wenger v. Germany*, judgment of 3 June 2008, App. nos. 9676/05, 10744/05 and 41349/06, p. 10.
1121 ECtHR, *Peev v. Bulgaria*, §39.
1122 Id.
1123 Id.

to his employer"[1124]. In the Court's view, it was also relevant that at the time of the search the applicant had already been informed that an investigation against him had been initiated: therefore, he could not expect that the inculpatory material stored in his phone would remain private[1125]. In this sense, observed the Court, *Garamukanwa* differed from *Bărbulescu* or *López-Ribalda*, where it was found that the applicants had not been properly informed of the extent of the employer's monitoring operations[1126]. For these reasons, the complaint was found inadmissible.

3.2.1.2. Surveillance in public places

Surveillance at the police station. Despite its stronger relevance for the smart city context, the reasonable expectation of privacy test has not been applied so much in public places as in workplace contexts[1127]. A first set of cases in this pool of decisions focuses on surveillance in police stations. For instance, *P.G and J.H. v. United Kingdom* was the first case after *Halford* where the reasonable expectation of privacy test was applied. The case concerned an attempt to thwart a robbery. The police had installed some hidden audio-recording devices in an apartment with the aim to identify the conspirators. Later on, the authorities also recorded, covertly at the police station, some conversations with the suspects to secure audio samples of their voices and compare them with those previously caught in the apartment.

When the case landed at the ECtHR, the applicants (the suspects) claimed that their right to private life had been breached because they were not aware, nor had reason to suspect, that their voices were being recorded at the police station. To establish the applicability of Art. 8, the Court considered that the reasonable expectation of privacy was an important, but not conclusive factor[1128]. People are perfectly visible to others in public, even if observation is performed through technological means (e.g., a camera).

Monitoring someone by technological means in the public scene does not in itself trigger the applicability of Art. 8 ECHR[1129]. What actually raises private life considerations, however, is "any systematic or permanent record [that] comes into existence of such material from the public domain"[1130]. In the case at hand, a permanent voice record had been created of the applicants' voices with the precise aim of identifying them, and therefore Art. 8 was deemed applicable[1131]. Differently, in *Friedl*, the Court had deemed that photographs made of the applicant when participating in a public demonstration – although stored in a police file to initiate an investigation – did not raise any private life consideration because "no action had been taken to identify the person photographed on that occasion by means of data processing"[1132].

Another case concerning surveillance at a police station is *Perry v. United Kingdom*. The applicant had been arrested in relation to a series of armed robberies and released pending an identification parade. When he failed to attend that and several other parades, the police requested permission to record his image through a video surveillance camera. Before the ECtHR, the applicant complained that the police had covertly videotaped him for identification purposes and used that evidence in the prosecution against him. The Government argued that the police station could not be regarded as a private place

---

[1124] ECtHR, *Garamukanwa v. United Kingdom*, judgment of 14 May 2019, App. no. 70573/17, §§16, 26 [emphasis added].
[1125] Id., §27.
[1126] Id.
[1127] Among the cases that had been identified as belonging to this thematic pool, there are also *Friend and Others v. United Kingdom* and, partially, *López Ribalda v. Spain*, respectively examined in §§3.2.1. and 3.2.1.1.
[1128] ECtHR, *P.G. and J. H. v. United Kingdom,* §57.
[1129] Id.; cf. ECtHR, *Perry v. United Kingdom*, §38; ECtHR, *Leander v. Sweden*, judgment of 26 March 1987, App. no. 9248/81, §48; ECtHR, *Amann v. Switzerland*, §§65-67; ECtHR, *Rotaru v. Romania*, §§43-44.
[1130] Id.
[1131] Id., §59.
[1132] Id., §58.

and that the surveillance cameras were visible to the applicant and running for security purposes. Therefore, the latter could not claim any expectation of privacy in that environment[1133].

The Court agreed that the normal use of security cameras in public streets and premises (e.g., shopping centres and police stations) does not call into question Art. 8(1) ECHR. Reiterating that reasonable expectations of privacy are not a conclusive factor in determining the applicability of Art. 8[1134], the Court stated once again that the systematic and permanent record of one's data obtained through surveillance in the public scene may raise private life considerations[1135].

Also, disseminating the material beyond what could be normally foreseen may also subject security recordings to Art. 8[1136]. In this case, police officers had specifically regulated the cameras to capture a better quality image of the applicant, and inserted it in footage for a video identity parade[1137]. The material was also shown in a public court room as evidence and had damaged his defence, a circumstance that the applicant could not have foreseen at the time of the videotaping[1138]. Therefore, the Court considered that the applicant's reasonable expectation of privacy had been breached and that Art. 8 applied.

Surveillance by CCTV cameras in public streets. Peck v. United Kingdom is one of the most significant cases to analyse the value of privacy in public spaces. The applicant, who was suffering from depression, was portrayed by a closed-circuit television (CCTV) camera installed in a street while walking alone with a kitchen knife in his hand. He had subsequently attempted suicide by cutting his wrists (but the CCTV footage did not show this). Still, the videotape was later disclosed in the media and his images were broadcast widely.

Before the ECHR, he complained that the dissemination of the CCTV footage had amounted to a violation of his right to private life. He contended that such a disclosure had occurred in a manner which he could never have foreseen. Once again, the Court reiterated that if the (technological) monitoring of one's actions in public raises issues with Art. 8, the same does not apply when such activities generate a permanent record of the individual's data. Specifically, the Court observed that:

> The present applicant was in a public street, but he was not there for the purposes of participating in any public event and he was not a public figure. It was late at night; he was deeply perturbed and in a state of distress. While he was walking in public wielding a knife, he was not later charged with any offence. The actual suicide attempt was neither recorded nor therefore disclosed. However, footage of the immediate aftermath was recorded and disclosed by the Council directly to the public in its CCTV News publication. In addition, the footage was disclosed to the media for further broadcasting and publication purposes. […] The applicant's identity was not adequately, or in some cases not at all, masked in the photographs and footage so published and broadcast. He was recognised by certain members of his family and by his friends, neighbours and colleagues[1139].

For all these reasons, the Court considered that the applicant's videotape had been seen to an extent that far exceeded any exposure to a passer-by or to a security camera, or any expectation of the applicant at the time of the facts[1140]. Therefore, Art. 8 was deemed applicable in this case.

1133 Id., §39.
1134 ECtHR, *Perry v. United Kingdom*, §37.
1135 Id, §38: cf. ECtHR, *P.G. and J. H. v. United Kingdom,* §57.
1136 Id.
1137 Id., §40.
1138 Id., §§40-41.
1139 Id., §62.
1140 Id.

Lastly, in *Vukota-Bojić v. Switzerland,* the applicant was systematically monitored and videotaped in public locations by professionals hired by an insurance company. The footage did not relate to any particularly intimate activities, it was stored and selected with the aim of using it as evidence basis for an expert opinion and, ultimately, for a reassessment of the applicant's insurance benefits. In examining the case, the Court reiterated its now established jurisprudence on the (technological) monitoring of people's public movements and the permanent recording of such personal data[1141]. By applying those principles to the context at stake, it found Art. 8 ECHR to be applicable.

3.2.1.3. Dynamic IP addresses: Benedik v. Slovenia

Facts of the case. The case originated from a criminal investigation initiated by the Swiss police against the users of the so-called "Razorback" network, where child pornography material was exchanged through a "p2p" (peer-to-peer) system. Therefore, each user could access all files made available on the network and download them for their personal use.

During the investigations, the Swiss police recorded a dynamic Internet Protocol ("IP") connected to the network. Subsequently, it successfully located one of the IP addresses in Slovenia and transferred the information to the national law enforcement authorities. Without obtaining a court order, the Slovenian police asked a national Internet service provider (ISP) to disclose the personal data of the IP address subscriber. The police were then provided with the name and address of the applicant's father. Later, the competent investigating judge issued a court order to obtain the subscriber's identity and to search the applicant's family home. During this activity, the focus of the police immediately gravitated towards the applicant and some pornographic material was also seized.

Based on this evidence, the applicant was later convicted at trial. He unsuccessfully challenged this decision before all competent internal courts, claiming that the police should not have obtained his personal data without a court order. In particular, the Slovenian Supreme Court applied the reasonable expectation of privacy test to determine whether the applicant's online communications and traffic data were worthy of constitutional protection. It considered that the applicant had not in any way masked the IP address through which he had accessed the Internet, and thus had consciously exposed himself to the public and could not legitimately have expected privacy. As a result, the applicant's claims were once again rejected.

The applicant's claim and the court's assessment. Before the ECtHR, Benedik claimed that his right to private life had been violated because the Slovenian ISP had retained his data and disclosed it to the police without a Court order.

To ascertain the applicability of Art. 8, the Court referred to the concept of reasonable expectations of privacy[1142]. In line with the established case law, the Court highlighted that private life concerns arise any time personal data is processed beyond what is normally foreseeable[1143]. Like the Slovenian Constitutional Court, the ECtHR deemed that the applicant expected, from his *subjective* angle, that his online activity would remain private when exchanging pornographic material within the Razorback network[1144]. The Court also stated that "the fact that he did not hide his dynamic IP address, assuming that it is possible to do so, cannot be decisive in the assessment of whether his expectation of privacy was reasonable from an *objective* standpoint"[1145]. Therefore, the Court went beyond a purely subjective

[1141] ECtHR, *Vukota-Bojić v. Switzerland,* §§55-56.
[1142] ECtHR, *Benedik v. Slovenia,* §101, 115 ff.
[1143] Id., §103 [emphasis added].
[1144] Id., §116.
[1145] Id. [emphasis added].

conception of privacy expectations and indicated that the real question was whether the applicant could have reasonably expected to keep his identity, and not his dynamic IP address, private[1146].

In the Court's view, the applicant had never revealed his identity in relation to his online activity, he was not identifiable by the particular website provider through an account or contact data. His online activity therefore engaged a high degree of anonymity[1147]. This was confirmed by the fact that the assigned dynamic IP address, even if visible to other users of the network, could not be traced to the specific computer without the ISP's support[1148]. Lastly, the Court stressed the importance of the applicable legal and regulatory framework, as a relevant, though not necessarily decisive, factor in determining the reasonable expectation of privacy[1149].

In the case at hand, also from the point of view of the applicable legislation at the time, the applicant's expectations of privacy were not unwarranted[1150]. Therefore, the Court considered Art. 8 of the Convention to be applicable and later found a violation of the latter. Indeed, the national legal basis allowing the police to access IP address subscriber data was found to be lacking in clarity. A proportionality assessment was not even deemed necessary[1151].

Yudkivska's concurring opinion and Vehabović's dissent. The separate opinion of Judge Yudkivska, joined by Judge Bošnjak, criticised the "cautious approach" taken by the Court in relation to the reasonable expectation of privacy test[1152]. For the two judges, the Court had missed an invaluable opportunity to clarify the scope of the test in the digital age[1153]. Arguably, this decision could have impacted on the great majority of Internet users around Europe, with dynamic addresses being the most common identifier for online consumers nowadays[1154]. Instead, the Court had left open the issue of a reasonable expectation of privacy with regard to traffic data (metering or metadata)[1155].

Benedik enjoyed anonymity like all other internet users, as dynamic IP addresses can be linked to one's identity only if specifically disclosed by the service provider following a relevant request. Therefore, according to Judge Yudkivska, there had to be no doubt that his expectations of privacy were perfectly legitimate, regardless of the horrendous character of his criminal activity. For all these reasons, she believed that "the Court ought to have stated unequivocally that, given the technical anonymity of IP addresses, internet users have reasonable expectations of privacy when surfing the Web. Further processing of this metadata may only be carried out in accordance with a law that satisfies quality requirements"[1156].

On the contrary, Judge Vehabović was the only one not joining the majority in the finding of an Art. 8 violation. With specific reference to the reasonable expectation of privacy test, he did not believe that the subjective angle of the applicant should be taken under consideration where a criminal activity is at stake[1157]. Generally, criminals do not want their activities to be known. In this light, an expectation to hide criminal activity should not be considered as reasonable[1158]. Moreover, he highlighted that the

1146 Id.
1147 Id., §117. On anonymity online see ECtHR, *Delfi AS v. Estonia,* judgment of 16 June 2015, App. no. 64569/09, §148.
1148 ECtHR, *Benedik v. Slovenia,* §117.
1149 Id., §117.
1150 Id., §118.
1151 Id., §§132-133.
1152 Id., p. 45.
1153 Id.
1154 Id., pp. 46-47.
1155 Id.
1156 Id., p. 50.
1157 Id., p. 51. Cf. Justice Harlan concurring opinion in *White.*
1158 Id., p. 52.

applicant exchanged files through a public network account that was visible to others: "[t]he applicant therefore knew, or ought to have known, that his actions were not anonymous"[1159].

3.2.1.4. "Reasonable expectation of privacy": systematisation in the European framework

A subjective or objective test of reasonable expectations. Having reviewed the existing case law on reasonable expectations of privacy, this section will systematise the meaning and guiding criteria of the assessment. Connections with the USSC jurisprudence will also be highlighted where relevant.

In line with the evolution occurred in the USSC case law, the ECtHR seems to be gravitating towards an *objective* interpretation of reasonable expectations, although some incoherences remain. References to the illicit nature of the applicants' activities persisted in *Benedik* and *Garamukanwa*. In the former case, Judge Vehabović believed that the Court had wrongly taken into account Benedik's subjective belief that his paedo-pornographic searches would remain private. On the contrary, in *Garamukanwa*, the Court took the opposite approach, finding that the applicant could not have claimed to have a reasonable expectation of privacy in relation to a conduct that constituted a criminal offence[1160].

In both cases, however, this criterion did not seem to have a primary weight in the assessment. Rather, the Court mostly relied on objective factors affecting the applicants' expectations of privacy. In *Benedik*, the technical features of the technology (i.e., the use of dynamic IP addresses) were decisive, while in *Garamukanwa* the focus was placed on the fact that the claimant had been informed of the ongoing investigation against him. The same could be argued for cases of workplace surveillance, where an employer's instructions or warnings are always considered by the Court. Indeed, these also constitute objective indicators, which can lower (if not erase) applicants' expectations of privacy in the workplace.

The function of the broader regulatory framework in the test. Another notable indication in the ECtHR's case law is that "the applicable legal and regulatory framework might also be a relevant, though not necessarily decisive, factor in determining the reasonable expectation of privacy"[1161].

This argument is significant in a twofold manner. On the one hand, it suggests that the interpreter should go beyond the mere letter of the law and look for the overarching principles in the legal order to establish the level of reasonable expectations of privacy.

On the other, it provides an indicative answer as to the nature of the test itself. As prospected above, it is still not clear in the case law of the Court whether "reasonable expectations of privacy" should be understood as an overarching test or simply as one assessment factor among others. What emerges from the Court's statement is that reasonable expectations of privacy should rather be considered as a multi-factor test, whereby the applicable law plays a role in determining the level of the expectations themselves.

The broader regulatory framework should also be integrated in a *prognostic* test on the acceptability of certain surveillance practices, as underlined above for the USSC case law. For instance, overarching principles like the rule of law and the endurance of democratic institutions may be jeopardised by certain surveillance technologies, which should thus be rejected.

Voluntary exposure in public: An alternative to the test? When referring to the fact that reasonable expectations are not a conclusive factor in determining the applicability of Art. 8, the Court has on

---

[1159] Id.
[1160] ECtHR, *Garamukanwa v. United Kingdom*, §16.
[1161] ECtHR, *Benedik v. Slovenia,* §118. Cf. also ECtHR, *J.S. v. United Kingdom*, §70; ECtHR, *Peev v. Bulgaria*, §39.

some occasions referred to the willingness of the individual to expose themselves in public, e.g., by participating in public demonstrations:

> "(…) Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor"[1162].

Voluntary exposure in the public sphere would thus seem to be the actual alternative to the existence of reasonable expectations of privacy. Reasonable expectations of privacy can certainly be significant factor in determining whether Art. 8 ECHR applies, but there are situations where people voluntarily engage in activities that do not fall within the scope of private life *at all*. On these occasions, there would be no need to apply the test. The Court critically considers that applicants voluntarily "give up" privacy expectations by taking part in activities that are not strictly private (e.g., work, social interactions), but rather belong to the public sphere in the strict sense (e.g., political demonstrations). That was, for instance, the case in *Friedl* and *Friend and Others*.

In *Friedl*, the test was not even mentioned, and it was excluded that the applicant's behaviour could fall within the scope of Art. 8. In *Friend and Others* the test was merely mentioned, but the private nature of the activities at stake was immediately dismissed in relation to the applicability of the right to private life.

Factors in the reasonable expectations of privacy test. Based on the review of the case law, the reasonable expectations of privacy test can be conceptualised as a multi-factor test[1163], comprising the following factors:

(1) the relevant regulatory framework (e.g., legal rules, principles, workplace instructions, acceptable uses of the data, prognostic assessment on surveillance practices);

(2) target of the surveillance;

(3) means of surveillance, relevant only in connection with the

(4) further use of the data;

(5) the place and time of surveillance.

Of course, this classification is purely indicative and pursues the goal of achieving descriptive clarity in relation to the case law of the Court. The effort is to be as analytical as possible, but some factors are certainly subject to different categorisations. It is not excluded that other classifications are also possible, but this seems to be the most appropriate one from the analysis carried out so far.

Concerning the first factor, it has already been observed that the reference to the law should be taken in the broadest sense, so as to include not only written rules, but also the overarching principles of the legal order. Instructions in the workplace are also important, as they have been referenced by the Court in at least five cases[1164]. These seem to be significant in determining the level of privacy expectations, although the Court has not clearly specified in which sense. The explicit instructions of the employer concerning monitoring measures in the workplace may not bear such a weight to exclude

---

[1162] ECtHR, *P.G. and J. H. v. United Kingdom,* §57; ECtHR, *J.S. v. United Kingdom*, §69; ECtHR, *López Ribalda and Others v. Spain*, §89.
[1163] Cf. also Moreham (2006); Wilckins (1987).
[1164] See ECtHR, *Halford v. United Kingdom,* §45; ECtHR, *Copland v. United Kingdom*, §42; ECtHR, *Bărbulescu v. Romania*, §78; ECtHR, *López Ribalda and Others v. Spain*, §93; ECtHR, *Akhlyustin v. Russia*, §39.

the applicability of Art. 8 ECHR completely[1165]. What they may do (as will be suggested afterwards) is imposing a stricter or more flexible proportionality assessment under Art. 8(2) ECHR.

With regard to the target or object of the surveillance, the issue of the publicity or celebrity of the person concerned will not be dealt with here, as it has mainly interested case law on the freedom of expression. An in-depth analysis would not be overly useful in relation to the topic of this investigation, which is more focused on *pervasive* surveillance in smart cities rather than on targeted monitoring of celebrities and other high-profile figures by journalists. On the other hand, the Court seems to attach some relevance to the potential vulnerability of the person(s) subject to monitoring, as was the case in *Peck*[1166]. Even if this constitutes only a one-time reference to the criterion, it may strengthen an increased safeguarding approach of the Court in future occurrences.

As for the means of surveillance, it appears that the Court tends to take a *neutral* approach, making no distinction between instances where the individual was observed in public through analogical or digital means[1167]. Nor is it relevant whether the monitoring devices are hidden or not. In comparison with the US elaboration, this attitude may lead to fruitful results, as it allows issues of potential commercial diffusion of technologies to be eluded, which may lower individuals' expectations of privacy in public[1168]. What seems to be relevant though is the use of technologies that rely on the (automated) processing of personal data, which are apt to generate a permanent record of the monitoring activities. These are indeed liable to raise privacy concerns. Obviously, this element will prove to be crucial for IoT surveillance in smart cities, where the extensive use of digital monitoring technologies is a high indicator of the existence of (significant) interferences in the right to private life.

This last point is closely connected with an issue in the reasonable expectation of privacy test, as also highlighted in recent USSC jurisprudence. The further use of the gathered data. For privacy considerations to arise, it is not only necessary that technologies are used to generate permanent records of the applicants, but also that the data at stake is used to identify the interested parties. This was clear, for instance, in *Friedl* where the Commission excluded that the applicant's right to private life had been at stake because police forces had never taken the initiative to identify him from his photographs[1169].

Actually, the Court appears to take a strict understanding of identifiability, as opposed to the widely accepted elaboration in the data protection doctrine. Indeed, when referring to identification or identifiability, the ECtHR seems to have in mind only L-identifiers (e.g., name appearing on the passport), instead excluding other kinds of identifiers in the online sphere. Identification is leveraged by the Court in a twofold fashion. As a first step, the Court highlights the willingness of third parties to achieve identification (in the L-identifiability sense) to decide whether to perform a reasonable expectation of privacy test. While in *Friedl* the absence of identification initiatives was enough for the Commission to exclude the applicability of Art. 8, in *P.G and J.H.* and *Perry* the Court valued the fact that identification was the ultimate objective of the surveillance carried out at the police stations. Once the goal to identify the applicant is established, as a second step the Court may take into consideration the *difficulties* of uncovering the individual's identity. This is relevant, for instance, for cases involving online identifiers, as was the case in *Benedik*. Here the Court maintained that the applicant – although participating in a *public* network with a dynamic IP address – retained a high expectation of privacy in

[1165] Cf. ECtHR, *Bărbulescu v. Romania*, §80; ECtHR, *Antović and Mirković v. Montenegro*, §44.
[1166] ECtHR, *Peck v. the United Kingdom,* §62.
[1167] ECtHR, *Perry v. United Kingdom*, §38; ECtHR, *P.G. and J. H. v. United Kingdom,* §57; ECtHR, *Peck v. the United Kingdom,* §59 (and cited jurisprudence).
[1168] Cf. §3.1.4.
[1169] See ECtHR, *Peck v. the United Kingdom,* §61.

relation to his online activities, since he had not published his real identity anywhere, nor could the police trace back the IP address to him without the help of the ISP.

Furthermore, the Court often refers to the dissemination of individuals' records in public venues or their reuse for public purposes, e.g., publication in the media or use as evidence in criminal investigations or at trial. What seems to be lacking, however, is a more comprehensive reflection on the dangers of data aggregation and repurposing in the big data era, a perspective that is being explicitly addressed in the United States[1170]. Unsurprisingly, this aspect was lamented by Judge Yudkivska in her separate opinion in *Benedik*. Despite this missed chance, it would be desirable in the future that the Court undertakes this broader view, in order to comprise transfers also among private entities in the online sphere as a factor in the test.

Lastly, as already been observed in the Fourth Amendment jurisprudence, a discussion about the space/place of the surveillance is not without relevance. In the case law of the ECHR, the criterion does not seem to hold primary weight in deciding whether privacy expectation arise at all, as the Court does not frequently engage in an analysis of the *physical* features of the locations where the monitoring took place. It did so, for instance, in *Friend and Others*, where the essentially public nature of the behaviour at stake (fox hunting) excluded *a priori* the existence of reasonable expectations of privacy[1171]. More interestingly, it did so in *López-Ribalda*, where the Court deemed that the applicants had a limited expectation of privacy as they performed their work in an area open to the public (the supermarket) and in permanent contact with customers. Here, the nature of the location where the surveillance occurred is not that significant to establish the existence of privacy expectations, but rather to determine their *intensity*.

The Court takes a layered approach to privacy expectations that can arise outside the remit of the home and other private premises. In other words, privacy expectations are not the same in secluded offices[1172], shared offices[1173], university campuses[1174] and supermarkets[1175]. Precisely, it is this layered approach that allows us to establish a connection of the reasonable expectation of privacy test under Art. 8(1) ECHR with the proportionality assessment in paragraph (2).

Link between reasonable expectations and assessment in Art. 8(2) ECHR. In the proportionality assessment performed in *López-Ribalda*, the Court once again made reference to the physical features of the place where the surveillance had taken place:

> "The Court takes the view in this connection that it is necessary to distinguish, in the analysis of the proportionality of a video-surveillance measure, the various places in which the monitoring was carried out, in the light of the protection of privacy that an employee could reasonably expect. That expectation is very high in places which are private by nature, such as toilets or cloakrooms, where heightened protection, or even a complete ban on video-surveillance, is justified (see, to this effect, the relevant international instruments cited in paragraphs 61 and 65 above). It remains high in closed working areas such as offices. It is manifestly lower in places that are visible or accessible to colleagues or, as in the present case, to the general public"[1176].

Even if the Court does not state it explicitly, the function of the reasonable expectations of privacy test would not only be that of establishing the applicability of Art. 8, but also the *seriousness* of the

[1170] See, e.g., the opinions of Justice Sotomayor and Alito in *Jones* and the *Carpenter* case.
[1171] ECtHR, *Friend and Others v. United Kingdom*, §43.
[1172] See, e.g., ECtHR, *Steeg and Wenger v. Germany*; ECtHR, *Haldimann and Others v. Switzerland.*
[1173] See, e.g., ECtHR, *Peev v. Bulgaria.*
[1174] See, e.g., ECtHR, *Antović and Mirković v. Montenegro.*
[1175] See, e.g., ECtHR, *López Ribalda and Others v. Spain.*
[1176] Id., §125.

interference at stake. The time[1177], openness or secludedness of the environment, and the instructions given in the workplace are all factors that can impact on privacy expectations and thus on the significance of the interference. Warnings about work surveillance, or the openness of the environment to the public, does not reduce privacy expectations to "zero", but can mitigate their weight[1178].

Therefore, the preliminary assessment about privacy expectations is meant to impact on the approach taken in the proportionality test, the strictness of which may vary according to the intensity of the expectations of privacy assessed under Art. 8(1). It is therefore in this way that references in the Court's case law to expectations of privacy under Art. 8(2) assessments can be appreciated.

Concluding remarks. All in all, this Section delved into an in-depth analysis of the ECtHR case law on the topic of reasonable expectations of privacy. A coherent framework for the concept was constructed based on an integrated analysis of the references made to the concept, elaborating it as multi-factor assessment. The nature of the test itself was clarified, showing both its difference and connection to the proportionality test performed pursuant to Art. 8(2). Ultimately, this explanatory effort can bring conceptual clarity in how to assess privacy interferences in public smart city environments, and in the future case law. In the next Section, those principles and criteria will be applied to the smart city context itself.

3.3. Privacy expectations in public smart city environments

Preliminary remarks. At the outset, the background analysis on the rationales and scope of the right to private life in smart city environments suggests that individuals enjoy significant privacy expectations in public. In this Section, the focus will be on multiple-use public places (e.g., streets, squares), which are those that offer the greatest chances for citizens to interact with others and experience the collective value of privacy[1179]. On the contrary, specified-purpose environments (e.g., railway stations and airports) will be momentarily left aside because their management is usually underpinned by higher security stakes. In these venues, expectations of privacy may be assessed differently and so could the proportionality of some surveillance technologies therein applied[1180].

The role of consent and public surveillance signalling. The ECtHR does not seem to place much weight on individuals' consent when assessing their reasonable expectations of privacy. Similarly, people's awareness that surveillance is ongoing (e.g., due to employers' instructions) does have a bearing on their expectations of privacy, although it cannot completely annul them. In the smart city, these considerations confirm the minor role of consent as a basis for processing data in those environments[1181]. Individuals do not relinquish their privacy expectations only because they knowingly venture into public IoT environments. Neither should they assume the risk of losing their privacy by choosing to live in a smart city[1182]. In a fully digitised environment, information technologies have already become essential means to get by in society, and it is even more so in smart cities. In the near future, this phenomenon will become even more pervasive. Being connected, and thus being exposed to digital surveillance, is not much of a choice of the individual, but represents a societal necessity. This

[1177] For example, this factor was given weight in *Peck* where the Court referred to the fact that the applicant was walking in public late at night.
[1178] ECtHR, *Bărbulescu v. Romania*, §80.
[1179] Cf. §2.2.2.
[1180] Ferguson (2020), pp. 95 ff; Ashworth et al (2014), pp. 130 ff.
[1181] See Chapter I, §3.1.
[1182] Ferguson (2020), pp. 88 ff.

perspective distinctly emerges in the USSC jurisprudence, where the majority in *Carpenter* determined that CLSI information is not "truly shared" as one normally understands the term, and the same could be said for any other IoT device broadcasting (meta)data in sensor environments. Citizens do not voluntarily give up their own information as ubiquitous sensors automatically collect them in public[1183].

Likewise, it cannot be said that signalling the presence of surveillance technologies (e.g., CCTV cameras) completely erases people's reasonable expectations in public. It is true that transparency models can bring some privacy benefits, making individuals aware of the ongoing surveillance, but such approaches are destined to clash with problems of scale in cities[1184]. People cannot simply avoid CCTV for ever, nor areas where data collection occurs[1185]. Life in smart cities is often hectic, and people may not even think of taking alternative paths while dashing off to work or running chores. Therefore, citizens' awareness of ongoing surveillance activities cannot in itself have the effect of excluding any reasonable privacy expectation (and thus the applicability of Art. 8). The fact that surveillants disclose the use of monitoring technologies in public cannot reduce individuals' private social life to zero[1186].

The public activity exception. It was shown above how the ECtHR considers voluntary engagement in public behaviour as a means to exclude *a priori* the applicability of Art. 8 of the Convention, and thus the existence of any expectation of privacy[1187]. Nonetheless, the criticalities of this approach are evident in light of privacy's social and political value[1188]. Privacy (also in terms of anonymity) is often a crucial ingredient of democratic societies, an essential precondition to freely take part in political demonstrations. Excluding all privacy protections in those kinds of contexts at the outset would probably be detrimental for the development of a truly pluralistic public sphere[1189].

Identifiability and further data uses in three technological scenarios. A central criterion in the reasonable expectation of privacy test is reliance on personal data processing and the further use of such data. Specifically, the Court has often reiterated that the creation of permanent records of data proceedings from the surveillance of people's public movements can give rise to high expectations of privacy. These considerations alone are liable to cover many situations of IoT surveillance in public urban environments, which would thus fall within the scope of Art. 8 of the Convention.

This extensive interpretation of the right to private life may, however, be curbed by the strict approach of the Court with respect to identifiability, which is mainly understood as L-identifiability. We should consider that surveillance strategies (especially in the commercial sector) do not need to reach users' L-identity to achieve their goals. This raises the question of whether, in the Court's view, these processing operations would be excluded from the ambit of Art. 8 of the Convention. This might be the case of EFR technologies, which are currently being embedded in smart billboards to pick targeted advertising based on the facial expression of passers-by. While these applications do not need to L-identify individuals, or create a permanent record of individuals' data, they are liable to impact on their decisional autonomy (e.g., by proposing targeted advertising). Therefore, the Court's approach on this topic warrants revision, in view of embracing a broader conceptualisation of identifiability. These new applications should not be excluded *a priori* from the purview of the right to private life.

1183 Id., p. 89.
1184 Sharon et al (2021), p. 9.
1185 Id.
1186 Adapted from ECtHR, *Bărbulescu v. Romania*, §80; ECtHR, *Antović and Mirković v. Montenegro*, §44.
1187 See §3.2.1.4.
1188 See §2.2.3.
1189 Luxmoore (2019).

When L-identification is intended, many surveillance applications in smart cities seem to be covered by Art. 8 ECHR. For instance, with respect to Wi-Fi and MAC tracking[1190], both dynamic IP and MAC addresses seem to be surrounded by high expectations of privacy. If the Court has explicitly stated this with respect to the former, the same can probably be affirmed for MAC addresses as well. Indeed, it appears extremely difficult to trace back one to the owner of the device: there exists no centralised database of MAC addresses and these are also very easy to modify[1191].

Moreover, facial recognition can also trigger individuals' high expectations of privacy in public spaces. Here, identification underpins the whole processing operation: passers-by faces are compared against a database of warranted people (a sort of host list), and, when there is no positive match, individuals' data are immediately erased. While for people in the hotlists there is a serious invasion of privacy, the same could not necessarily be said for people that are not warranted by the surveillants, because there is no permanent record of their data. Nonetheless, the expectations of privacy of these individuals are also engaged solely by the fact of being exposed to the technology. Indeed, even if their data is immediately erased upon a negative match, they can for instance incur in negative consequences in the event of misidentifications.

Concluding remarks on expectations of privacy in public smart environments. Even in public, people's expectations of privacy are touched upon – often in a serious manner – by the implementation of surveillance technologies in smart cities. Although signalling may mitigate the level of expectations of privacy in public places, it cannot have the effect of reducing them to zero. The features of technologies employed by citizens and the dangers for re-identification compensate for the awareness of surveillance and make their expectations of privacy rather high. These expectations should be particularly intense with regard to activities of a political or relational nature. A prognostic test on the acceptability of certain police surveillance practices should also be integrated in this analysis.

4. Interim conclusions

In this chapter, the meaning, rationale and scope of the concept and right to privacy were extensively analysed, combining philosophical and legal theories. It emerged how privacy is essentially an indeterminate, vague concept, which is why some commentators have tried to downsize its importance. Nonetheless, it is precisely its multi-faceted and pluralistic nature that gives privacy much potential in addressing the issues brought about by digital technologies, which can either be magnified versions of old problems but also radically new ones. In this sense, broad approaches to the understanding and purview of privacy should be preferred to more definitive solutions. Put simply, there is not only one *privacy*, but many *privacies*. That is why no specific definition of privacy was embraced for the purposes of this analysis.

The fuzzy nature of privacy is also evident from the analysis of the nature of space and place. This second part of the inquiry showed why and how privacies should be protected in public urban environments. We can find or expect to have privacy literally everywhere, from the cherished boundaries of our homes to the benches of a major city square. If "privacy places" have always overlapped with public venues, digital technologies are now incentivising this process of boundary blurring between private and public. We bring sensitive details of our lives out in public through our smartphones, and our homes are increasingly transparent to the outside world. The fact that we can no longer rely on clear-cut markers (e.g., the home or the body) has a crucial impact on how we should

[1190] See Chapter I, §§2.4.2.2.
[1191] Mitchell (2020).

legally assess the applicability of the right to privacy. In many instances, the approach to be undertaken by the interpreter needs to gravitate towards more multi-layered methodologies. The absence of clear indicators suggesting the applicability of the right to private life requires engaging in preliminary balancing tests.

These exercises should be aimed at determining whether privacy rights are actually at stake, and potentially what the extent of the interference is. That is the function of the reasonable expectation of privacy test, which was systematised based on a review of the existing case law by the USSC and the ECtHR. Some methodological clarity on how to perform this first balancing effort was introduced by conceptualising the reasonable expectations of privacy as a multi-factor assessment. The considerations made were also translated in the smart city context. Having a more granular perspective on how strong individuals' expectations of privacy are is essential, as shown, to fine-tune the proportionality assessment of surveillance measures.

All in all, the analysis of this chapter has served the objective of establishing a clear methodology to identify privacy interferences and assessing their seriousness. In the next chapter, the focus will shift to the *second* balancing test, that of proportionality of surveillance measures.

IV. General Surveillance Frameworks

1. Introduction

A feature of modern societies. Like privacy, surveillance can be found pretty much everywhere. Broadly defined as the collection of information for purposes of control[1192], it has been seen – especially in its most trivial iterations – as a basic feature of human life[1193]. For instance, surveillance is in the mother monitoring her new-born's behaviour, or in the farmer's attempts to predict weather conditions to secure a successful harvesting. On a larger scale, surveillance has also been regarded as a key function of complex modern societies[1194]. Many actors need to gather and analyse information so as to anticipate others' future behaviour and reduce the risks of social interactions[1195]. For instance, this explains why national governments keep meticulous track of who is entering and leaving their territory, or why the police patrol "difficult" neighbourhoods in the city as a means of crime control[1196].

Good and bad surveillance. Against this background, it can be observed that surveillance, although never neutral in its applications, can be dual use[1197]. Monitoring technologies can be employed to pursue morally good objectives, allowing *inter alia* the basic functioning of society and its governance[1198]. At the same time, it also has undeniable negative connotations for its potentially worrying repercussions on individuals.

In recent years, the latter perspective has been highly dominant in academic fora and public discourse[1199]. Today, it is fairly easy to make a case against surveillance[1200], especially in the wake of the numberless scandals that have emerged in the last two decades of reckless intensification of surveillance practices. Surveillance's "bad reputation" is also evident in the imagery it evokes. Metaphors – like the Panopticon or Orwell's Big Brother – are still considered powerful tools to convey its mechanisms and dangers[1201]. There have also been many adjectives associated with surveillance, from "liquid" to "ubiquitous", "intrusive", "mass", "invasive", "interfering", "oppressive" or "violating", and so on. When based on smart technologies, it has even been described as a form of "pollution" [1202], "infection", or "biological warfare"[1203].

Outline. Against this background, this chapter will bring together different perspectives on surveillance. The research sub-question addressed in this chapter is: *Which theoretical frameworks can best conceptualise surveillance schemes in smart cities and which proportionality assessments do these require?* Firstly, a brief

---

1192 Lyon (2007, p. 14) defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction". See also Haggerty et al (2006), p. 3.
1193 Kuntze (2018), p. 39; Ball (2009), pp. 640.
1194 Bauman et al (2013), p. 8; Ball (2009), p. 640.; Andrejevic (2012), p. 92.
1195 Ball (2009), p. 640.
1196 On surveillance in the urban context, see Fussey et al (2012); Melgaço et al (2021).
1197 Floridi (2017), p. 392.
1198 The conceptual relation between governance and surveillance has been long acknowledged in literature, see e.g., Foucault (1991), p. 92; Henne (2019), pp. 233-245; Rao et al (2019), p. 471; Lyon (2010), p. 618; Lyon et al (2008), p. 4; Henschke (2017), p. 252.
1199 Marx (2015), p. 32; Stoddart (2012), p. 371.
1200 Rosenthal (2018), p. 308: "It is easy to condemn surveillance. Its benefits are often uncertain, yet it necessarily imposes a cost by compromising the privacy of those who become the objects of official scrutiny".
1201 Cf. Finch et al (2016); Zuboff (2015). *Contra* Haggerty (2006).
1202 Froomkin (2015).
1203 Murakami Wood et al (2021), p. 151.

overview of philosophical and sociological theories of surveillance will be provided[1204]. The legal investigation will include an extensive analysis of the case law of the CJEU and the ECtHR on (mass and covert) surveillance[1205]. The latest decisions will be studied through the lens of the proportionality principle, whose implementation is increasingly via problematic modern surveillance strategies, especially in the context of crime prevention. As a legislative framework on surveillance is still nof forthcoming in Europe, the findings of the two Courts will be systematised and applied to diversified instances of surveillance (i.e., mass, targeted, hybrid). Throughout the analysis, these legal, sociological and philosophical considerations will be translated into the smart city context.

2. Philosophical and sociological frameworks for surveillance

2.1. Foucault's Panopticon and Governmentality

The hegemony of the panopticon. Bentham's and Foucault's panopticon is one of the most powerful representations of surveillance to date. This is true to the point that, after the publication of *Discipline and Punish* (1975), "[f]or some time, surveillance and Panopticism seemed to be the same thing"[1206]. In Foucault's conceptualisation, Bentham's panopticon was the optimal architectural figure allowing for continuous and pervasive surveillance. The Panopticon was conceived as an annular building, with at the centre a tower punctuated with large windows looking onto the inner side of the ring. The periphery is divided into cells provided with two windows: one looking to the outside, allowing light to come in; the other facing the central tower. Then, a supervisor is placed in the central tower, and the cells filled with madmen, patients, condemned, workers, or pupils. Because of the backlighting, the supervisor can observe those in the cells standing against the incoming light; they are all "perfectly individualised and constantly visible"[1207]. The panoptic dynamic allows the guardian to recognise each spatial unit, and individualise and supervise each inmate[1208]. On the contrary, the latter cannot communicate with their inmates, thus securing order and averting any dangers of revolt or contagion[1209].

The principle underlying this arrangement is that power should be at once visible and unverifiable[1210]. Inmates will always see the central tower overseeing them, but they can never know whether they are being looked at in any particular moment, thus believing that it is always so. In this way, the panopticon is able to exercise a disciplinary power over the surveillees.

Nonetheless, the Panopticon should not simply be understood as a "dream building", but as an ideal way of defining power relations in people's daily lives[1211]. It is a model of a power exercised without any obstacle, resistance or friction, and as such it can be detached from any specific use and applied to any establishment[1212]. By reducing the number of surveillants and increasing that of surveillees, the panoptic mechanism can be integrated in any function (educational, medical, manufacturing, punishment) to magnify its efficiency.

Governmentality and pastoral power. The founding categories of *Discipline and Punish* gradually lost popularity in favour of Foucault's "analysis of governmentality". In the "Security, territory, population"

[1204] See §2.
[1205] See §3.
[1206] Vogelmann et al (2017), p. 6.
[1207] Foucault (2020, original work of 1975), p. 200.
[1208] Id., pp. 200-201.
[1209] Id.
[1210] Id., p. 201.
[1211] Id., p. 205.
[1212] Id.

lectures at the *Collège de France* (1977-1978), Foucault first came up with the term governmentality (*gouvernmentalité)*, derived from the French term *gouvernmental* which already held some currency at the time[1213].

Foucault defined the art of government as "the correct way of managing individuals", starting with oneself, then one's family and finally the state[1214]:

> To govern a state will therefore mean to apply economy, to set up an economy at the level of the entire state, which means exercising towards its inhabitants, and the wealth and behaviour of each and all, *a form of surveillance and control* as attentive as that of the head of a family over his household and his goods[1215].

More broadly, governmentality implies "a plurality of specific aims": ensuring that the greatest number of resources is produced; people having enough means of sustenance; individuals being able to procreate and establish families[1216]. The concept is also strictly connected to that of "security", which was previously used by Foucault to talk about the art of government itself[1217].

In fact, it was only in the last lecture at the *Collège de France* that this terminology was changed, likely because "security" had a strong authoritarian and statist connotation at that time[1218]. In the liberal State, security becomes the "goal and rationality of governance", being the necessary complement of liberty[1219]. Specifically, security is able to protect liberty because it is always oriented to the future and to the neutralisation of risks[1220].

This "benign" representation of power and security is evident in another key concept developed by Foucault in his lectures, that of "pastoral power". The idea stemmed from Christian tradition, where the relationship between the shepherd and his flock, and between leaders and those they lead, was conceived along the lines of the government of souls[1221].

Nowadays, the concept of pastoral power (and governmentality) has been reworked by scholars as a kind of "positive security"[1222]. This emerging concept comprises strategies aimed at improving urban safety and security by stressing positive attributes of living together, like "care", "protection" and "belonging"[1223]. In relation to smart cities, scholars have tried to emphasise this positive approach as a justification for security-related projects, like *De-escalate* in Eindhoven[1224]. Here, pastoralism is not only focused on excluding mechanisms or people's protection against unwanted behaviour, but it also relies on a positive conception of security[1225]. The technologies implemented in *De-escalate* securitise public space not only through surveillance and exclusion, but also through behavioural nudging and inclusion[1226], thus making the Stratumseind a safe space for everybody.

Governmentality and surveillance. How is Foucault's analysis of governmentality and pastoral power relevant for surveillance? The close interconnectedness between the art of government and the need for

---

1213 Bröckling et al (2010), p. 1; Valverde (2008), p. 16
1214 Foucault (1991), p. 92.
1215 Id. [emphasis added].
1216 Id.
1217 Murakami Wood (2013), p. 318.
1218 Valverde (2008), p. 29.
1219 Id., p. 29.
1220 Id., p. 28.
1221 Foucault (1991), p. 104; Valverde (2008), p. 19; Schuilenburg et al (2018), pp. 5, 7.
1222 Schuilenburg, Peeters (2018), p. 2.
1223 Id.
1224 Id.
1225 Id., p. 6.
1226 Id.

surveillance seems often implied in the *Collège de France* lectures. One of the meanings of governmentality indeed refers to the integration of knowledge in the mechanisms of government[1227]. Acquiring information on the targets of governmental projects is unavoidable for the success of these initiatives[1228].

This suggests that surveillance may not only be a necessity in society, but may at times be beneficial as well. Surveillance scholars have underlined how governance studies have discarded a vision which sees social control as a necessary by-product of governmental projects[1229]. That is why we should generally take an ambivalent normative stance on mechanisms of power[1230]. While these certainly involve persuasive and disciplining efforts towards their targets, they also look at individuals as subjects of rights and freedoms[1231]. An accurate normative position about surveillance can be effectively developed only when the specific governmental ambitions of the initiative are considered[1232]. In this sense, it is significant that citizens do no reject surveillance *in the abstract*, but often manifest concerns about practical implementations or potential applications of surveillance by given actors[1233].

2.2. Infrastructural and contemporary theories

Moving beyond the panopticon. Whereas architectural theories revolved around the metaphor of the Panopticon, subsequent infrastructural outlooks described the phenomenon of surveillance as a network of digital rather than physical technologies[1234]. Within this strand of literature, the contributions of Deleuze, Haggerty and Ericson, and Zuboff were particularly impacting.

Deleuze: from disciplinary societies to societies of control. Deleuze's *Postscripts for the Societies of Control* is one of the primary sources when discussing modern data-driven surveillance[1235]. Control over individuals is here identified as the primary technique to exercise power in information societies. While Foucauldian discipline was (preferably) exercised in enclosed spaces (e.g., schools, factories), control can be exerted *everywhere*[1236]. New modes of power based on control rely on numerical language and function like *modulations*, i.e., systems that will continuously re-modulate themselves according to the circumstances[1237].

Importantly, individuals are no longer the main subjects of surveillance[1238]. What matters in societies of control is people's representations through data (i.e., "dividuals")[1239], which means that surveillance does not necessarily focus on real individuals, but on their *dividuals*. These digital portrayals are built thanks to the digital trails (e.g., movements and purchases) that people leave behind[1240].

Ericson and Haggerty: The Surveillant Assemblage. Ericson and Haggerty are two major scholars of post-Foucaldian literature on surveillance. Being early critics of the panoptic metaphor, they drew on Deleuze's and Guattari's work to highlight the growing convergence of surveillance systems in

[1227] Vanolo (2014), p. 885.
[1228] Haggerty (2006), p. 40.
[1229] Id.
[1230] Id., p. 41: "[s]urveillance is neither good or bad".
[1231] Id., p. 40.
[1232] Id.; Graham et al (2003), p. 229.
[1233] Haggerty (2006), p. 41.
[1234] Galič et al (2017), p. 9.
[1235] Matzner (2017), p. 31; Galič et al (2017), p. 20.
[1236] Deleuze (1992, original work of 1990), p. 3; Matzner (2017), p. 31.
[1237] Id.
[1238] Matzner (2017), p. 31; Galič et al (2017), p. 20.
[1239] Id.
[1240] Galič et al (2017), p. 20. Cf. Krassmann (2017), p. 15.

contemporary society[1241]. In a highly influential paper, they named this emerging phenomenon "the *surveillant assemblage*".

They observe that surveillance is one of the main institutional features of late modernity, especially in cities[1242]. Surveillance dynamics in these environments do not fit within the traditional metaphor of the Panopticon, but rather that of the "assemblage". This concept describes a "multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together as a unique entity[1243].

When applied to surveillance, this notion highlights that numerous inconspicuous technologies and social practices coexist in surveillance[1244]. No technological solution has *in itself* opened the gate to contemporary surveillance. Rather, subtle modifications of existing technologies have allowed surveillance initiatives to be more interconnected[1245]. Control, governance, security, profit or entertainment constitute desires bringing surveillance assemblages together[1246]. These technologies isolate human beings from their physical environments and reassemble them in data flows, finding relevant patterns for comparison purposes[1247]. Data doubles thus become a tool in the hands of public and private institutions to discriminate among different groups[1248]. New segments of the population are being targeted: it is not only the poor or marginalised who are being monitored, but also the middle-classes, especially through consumer profiling[1249].

Later, Haggerty pushed forward these arguments to overcome the oppressiveness of the panopticon in modern representations of surveillance, which should arguably be understood as an ampler multi-faceted and complex phenomenon[1250]. Surveillance is now underpinned by a proliferation of purposes, many of which were not envisioned in the initial theorisation of the panopticon[1251]. Surveillance regimes may be devised to reach specific goals, but these often unfold in unanticipated ways, even with the contribution of individuals' creative insights.

People's data doubles are proliferating around powerful corporations, and the multiplication of points of observation breaks the unidirectional nature of the panopticon's gaze[1252]. Many surveillance efforts nowadays are not specifically directed at humans, although these remain marginally involved (e.g., in the case of disease or environmental surveillance)[1253]. For instance, the proliferation of cheap IoT sensors has made it possible to monitor varied natural events and dynamics, bringing profound societal benefits[1254].

Lastly, surveillance today does not rely on the awareness of its targets to perform its disciplinary work[1255]. Certainly, this dynamic is still operational, as in the panopticon (i.e., chilling effect);

1241 Haggerty et al (2000), p. 606. Felix Guattari was a psychanalyst that intensively worked with French philosopher Gilles Deleuze, author of the *Postscripts on the Societies of Control.*
1242 Id., pp. 605-606.
1243 Id., p. 608.
1244 Id., p. 610.
1245 Id., pp. 614-615.
1246 Id, p. 609.
1247 Id.
1248 Id., pp. 613-614.
1249 Id., p. 617.
1250 Haggerty (2006), p. 23.
1251 Id., p. 27.
1252 Id., p. 29.
1253 Id., p. 31.
1254 Id.
1255 Id.

nonetheless, monitoring technologies can still achieve their political and commercial purposes unbeknownst to their addressees[1256].

Finally, Haggerty argued that normative perspectives on surveillance should be extended[1257]. After Foucault, scholars have inherited a tendency to magnify the dystopian potentials of surveillance, and new developments are always presented as a harbinger of bewildering consequences for civil liberties[1258]. That is why scholars often miss the potential beneficial effects which may be brought by surveillance itself[1259].

Zuboff: Surveillance capitalism. Another trend in post-panoptic literature is the (neo)-Marxist take on surveillance, of which sociologist and philosopher Shoshana Zuboff is likely the most renowned representative[1260].

Zuboff analysed the features and founding logics of surveillance capitalism in her best-selling book *The Age of Surveillance Capitalism*[1261]. Surveillance capitalism is described as "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction and sales"[1262]. The model thrives on marketing "behavioural surplus". If, originally, the data generated by internet search engines (i.e., behavioural data) was exploited *only* to improve the quality of the search results, from one point onwards platforms like Google and Facebook found ways to use this data to send targeted advertising to individual users[1263]. These "raw" behavioural data were thus turned into *surpluses*. Behavioural data surplus, obtained at zero marginal costs, constituted new surveillance assets, and were critical in the pursuit of *surveillance revenues* and their translation into *surveillance capital*[1264]. As we will see later on, Zuboff's framework is particularly useful to grasp some of the aspects of the smart city paradigm[1265].

Surveillance studies. The scholarly attention towards surveillance has also manifested through the rise of surveillance studies, which stretches across social sciences, arts and humanities, all concerned with the empirical and theoretical analysis of surveillance practices in society[1266]. Despite its recent establishment, surveillance studies today possess an arsenal of new concepts and images, like "social sorting"[1267]. Coined by David Lyon, the term quickly became a shorthand[1268] to stress the novel classifying drive of contemporary surveillance, which extensively employs profiling technologies to all segments of the population[1269]. Together with other dominant concepts like the surveillant assemblage, social sorting aimed to mitigate sinister connotations around surveillance, portraying it as an unavoidable feature of human life[1270].

1256 Id., p. 35.
1257 Id.
1258 Id.
1259 Lyon (1994), p. 219
1260 Galič et al (2017), p. 24.
1261 Zuboff (2019). This book builds on the previous work of Zuboff (2015).
1262 Zuboff(2019), The Definition.
1263 Id., p. 74.
1264 Id., p. 94.
1265 See below and Chapter VI, §3.1.
1266 Lyon et al (2012), p. 1; cf. Falkenhayner (2021).
1267 Lyon (2003a), pp. 1 ff.
1268 Lyon et al (2010), p. 5.
1269 Lyon (2003b), p. 13.
1270 Id.

Sousveillance and self-surveillance. One of the most innovative concepts in surveillance scholarship is *sousveillance*, literally "surveillance from below" (from the French *sous,* "below", and *veiller*, "watch over")[1271]. While classic *sur*veillance implies a monitoring from above (usually by organisations), sousveillance defines strategies of "counter", "inverse", "reciprocal" surveillance, enacted by individuals towards organisations[1272]. The increased availability of technologies to the wider public may re-establish balance and equality in power asymmetries between surveillants and surveillees[1273]. However, it may also enable forms of "digital vigilantism", providing citizens with tools that make other people visible online for allegedly committing morally or legally reprehensible acts in public spaces[1274].

With the advent of wearables and the quantified self (QS), the term sousveillance has been used to identify not only actions of counter-surveillance, but also situations where individuals voluntarily and consciously take part in the role of the watched (e.g., self-surveillance)[1275]. In commercial contexts, "gamification" techniques are used to motivate user participation and instil in them a tendency of continuous self-monitoring and feedback[1276]. GPS-enabled smart watches record location and health data (e.g., blood rate, steps, etc.), and allow users to share their achievements and improvements on specific platforms[1277].

From the normative standpoint, these initiatives bet their success on conveying a general idea of democratisation and user empowerment[1278]. Nonetheless, legal and surveillance scholars have tried to bring a more multi-faceted perspective to the surface. Gamification is meant to replace the "bleak" references to necessity, security, and efficiency as traditional justifications for surveillance, providing for a lighter and more appealing legitimising narrative[1279]. This does not mean however that power dynamics are not at play in these systems. These strategies try to modulate users' preferences and performances, and steer them towards a very specific behavioural model[1280].

2.3. Theoretical framings for smart cities

Surveillance frameworks in smart cities. This first part of the analysis was devoted to some of the most salient theories of surveillance, which could help us grasp general surveillance risks in smart cities. While the main goal of this work is purely legal, insights from sociology and philosophy can provide a more refined understanding of current dynamics, and new perspectives for the legal analysis.

With the exception of Zuboff, many scholars seem prone to also accept the positive implications of surveillance. This goes beyond excessively dystopic and extremist positions on the matter and reiterate the non-absolute nature of the rights to privacy and data protection. In smart cities, surveillance can indeed foster the securitisation of public places, but it can also serve technical needs (e.g., the protection of critical IoT infrastructure) and a more environmental-friendly use of resources.

Arguably, surveillance is a necessary feature of smart cities, as knowledge is unavoidable for the governance of the urban sphere. This premise imposes a focus on interpretative efforts not necessarily on banning surveillance from cities altogether (although certain applications may not comply with

[1271] Mann et al (2003), p. 332. On sousveillance, see Galič et al (2017), pp. 31-32.
[1272] Newell (2018), p. 12. Some scholars also refer to the term sousveillance more in terms of 'self-surveillance', performed with the use of wearables capturing data about the body (i.e.,quantified self). See Kitchin (2015) The Data Revolution. SAGE Publishing, p. 130.
[1273] On the normative implications of sousveillance, *compare* Mann et al (2003), pp. 333-334 and Floridi (2015), p. 9.
[1274] Newell (2018), p. 12.
[1275] Timan et al (2017), p. 7. On IoT-enabled self-surveillance, see Friedland (2018) and Jülicher et al (2018).
[1276] Cohen (2015b), p. 1.
[1277] Albrechtslund, Lauritsen (2013), p. 312.
[1278] Cohen (2015b), p. 8.
[1279] Id., p. 5.
[1280] Id., pp. 4-5.

minimum human rights standards), but on how to best approach this phenomenon in its pervasiveness. This goal, as explained above, can be reached through a more rigorous and granular application of the principle of proportionality.

Foucault in smart cities. Although dismissed in various academic fora, the panoptic metaphor can still explain some aspects of surveillance in smart cities. If the panopticon is understood as a "dream building", some of its features can be seen at play in smart cities today. For instance, the objective of optimising available resources persists in surveillance. However, while traditional panopticism had its primary focus on individuals, contemporary surveillance also includes non-human targets.

Moreover, there is no panoptic "single gaze" in urban environments today. On the contrary, there is a *plurality* of gazes, or of data collection points (i.e., sensors). This does not mean, however, that such dispersed information is not brought together at one point. Application-level software in IoT systems is designed specifically to extract meaningful information patterns from collected data[1281]. The panoptic "gaze" thus lacks a physical gate in urban environments, but data aggregation still occurs at the digital level. This stresses the importance of considering also the cumulative effects of IoT surveillance systems in proportionality assessments.

Foucault's governmentality also describes a basic feature of smart city functioning. To achieve the optimal management of resources, the art of government needs to target the population as a whole, and for that purpose knowledge in terms of statistics is needed. Therefore, surveillance is an avoidable component of the management of complex environments and societies. The plurality of instruments and goals of governmentality is also important. The law is only one of the strategies that allows governmentality to achieve its multifaceted goals. This applies to smart cities as well, where legal strategies constitute only one piece of the puzzle of urban governance.

Among governance tools, Foucault's "assemblages of security" are surely pivotal. Indeed, this concept stresses the *preventive* shift in the management of urban security, which is future-oriented and risk-driven. Indeed, to control general phenomena impacting the whole population (e.g., crime), public authorities are no longer solely interested in administering the law *ex post* in individual cases, but also in preventing future risks *ex ante*. Managerial strategies stemming from the corporate sector have thus made inroads in the security domain.

Deleuze. Deleuze underlined the fact that humans are not the primary targets of surveillance. In smart cities, data collection is not always underpinned by a disciplinary goal (i.e., homogenising individuals), but rather by the objective of *adapting the environment* to individuals' needs. This explains the emergence of new forms of profiling like "atmosphere profiling" that existing data protection laws struggle to address[1282]. Disciplinary goals lose centrality also in light of the secondary use of individuals' data. This implies that people may suffer the consequences stemming from the processing of other individual's data. From a data protection standpoint, this position puts additional strain on the individual focus of existing legislation, as well as on the purpose limitation principle[1283].

Surveillant assemblages in smart cities. "Surveillant assemblage" is likely a metaphor that best captures the functioning of contemporary surveillance. Indeed, the impact on individuals' rights is almost never the

[1281] See Introductory Chapter, §3.2.4.
[1282] See Chapter V, §4.
[1283] See Chapter II, §2.

result of one single technology, but rather a blend of technologies combined with the specific social features of the implementation context.

The cumulative effects of interoperable surveillance technologies should be considered in this light. In data protection, for instance, this poses additional re-identification problems. What may not be personal data within one specific system, may become so by integrating different data sources and technologies, which makes the application of related safeguards particularly volatile.

Furthermore, the surveillant assemblage theory highlights the need to discern the "desire" to bring monitoring systems together. The underlying goal of the processing can indeed affect the applicable legal regime and its fundamental rights implications. In smart cities, however, such objectives are not always easily discerned. The Stratumseind case is a good example of this instability, where data processing occurs at the crossroads between environmental and security needs. That is why the relevant legal analysis should always integrate these contextual objectives.

Overall, sociological and philosophical frameworks add different layers of complexity to the legal analysis of surveillance in real-world scenarios like smart cities. If surveillance imposes itself as necessary to govern urban environments, discerning its implications for citizens, as well as its concrete goals (e.g., security vs. environment), is increasingly difficult and complicates the task of assessing its proportionality.

3. Legal frameworks for surveillance

Surveillance in legal scholarship. In recent years, the interest towards surveillance has grown not only in the field of surveillance studies, but also in legal scholarship. Especially after the 9/11 attacks on the Twin Towers, and the proliferation of monitoring strategies in the fight against terrorism, scholars have reflected on the impact of such activities on fundamental rights, such as privacy, data protection and freedom of expression[1284]. In the criminal field specifically, studies have converged on the increasing overlap between traditional repressive activities of law enforcement, and secret surveillance initiatives enacted by intelligence services[1285].

Surveillance under judiciary scrutiny: the case law of the ECtHR and the CJEU. Despite this renewed focus in literature, judges have been dealing with surveillance for a long time now[1286]. In the ECtHR's jurisprudence, the first case in this domain is *Klass and Others v. Germany* (1978). Here, the Court was clear in identifying surveillance practices as interferences in the right enshrined in Art. 8 ECHR:

> Clearly, any of the permitted surveillance measures, once applied to a given individual, [would] result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence[1287].

Indeed, there can be a multitude of interferences with the right to private life (comprising both the right to privacy and data protection) brought by surveillance technologies. The Court considers that the systematic collection and storing of data by law enforcement gives rise to an interference with individuals' right to private life, even if such data were collected in a public place[1288]. Gathering people's information in a secret register and disseminating it also falls within the scope of Art. 8(1) ECHR,

[1284] See Balkin (2008); Miller (2014).
[1285] See de Hert (2005); Vervaele (2005); Gruszczak (2016), pp. 149-167; McGarrity et al (2010), pp. 131-149.
[1286] De Hert et al (2020), p. 3. For an overview of the ECtHR case law, see ECtHR Press Unit (2022).
[1287] ECtHR, *Klass and Others v. Germany*, judgment of 6 September 1978, App. no. 5029/71, §41.
[1288] ECtHR, *Peck v. the United Kingdom,* §59; ECtHR, *P.G. and J.H. v. the United Kingdom*, §§57-59. See Chapter III, §3.2.1.2.

especially when the data refers to the individual's distant past[1289]. This is true not only when the information was collected in public, but also when it concerns only the person's professional or public activities[1290]. Throughout the years, the Court has examined issues of data collection in varied contexts, such as telephone tapping[1291], audio and video surveillance[1292], geolocation via GPS[1293], and mass and secret surveillance operations involving the systematic monitoring of communication metadata and content[1294]. In the EU framework, systems of unfettered data retention (e.g., former Data Retention Directive, PNR Directive, national systems adopted under Art. 15 e-Privacy Directive) have also been at the centre of the CJEU's so-called "privacy spring"[1295].

In relation to mass surveillance, the ECtHR has found that national regimes of this kind create an interference with the right to private life, as individuals cannot be aware of whether they are targeted or if they can challenge the implemented measures[1296]. Starting from *Klass*, this approach has been a "revolution" in the system of the Convention and the institutional functions of the Strasbourg Court.

Normally, the ECtHR cannot be qualified as a court ruling on laws *in abstracto*, but rather as a court ruling on the concrete cases submitted to it[1297]. Therefore, applicants before the Court usually have to prove their status of victims. Given the difficulties of claiming such status when one is targeted by secret surveillance, however, the Court exceptionally agrees to examine national laws in general, and not in their specific application to a given individual.

Gaps and outline. It is true that, over time, the ECtHR has built a framework to assess the legitimacy of surveillance measures, both at the mass and targeted level[1298]. Although many principles are by now established in its jurisprudence and have also been integrated in the CJEU case law, some aspects still need to be sharpened. For instance, proportionality assessments may benefit from a more granular typology of surveillance systems. Considering the plurality of objectives in smart city surveillance, it may also be useful to extend the insights of this case law also beyond security-related scenarios.

Against this backdrop, the legal analysis on surveillance will be focused on the relevant case law of the CJEU and the ECtHR. Firstly, the proportionality test devised by the two Courts to justify interferences caused by surveillance measures will be presented, highlighting their similarities and differences[1299]. Secondly, a thorough overview of the jurisprudence of the ECtHR and CJEU on the matter will be provided, with a special focus on recent decisions tackling unfettered interception and

[1289] ECtHR, *Leander v. Sweden*, §48; ECtHR, *Rotaru v. Romania*, §§43-44; ECtHR, *Shimolovos v. Russia*, judgment of 28 November 2011, App. no. 30194/09, §§64-66.
[1290] ECtHR, *Amann v. Switzerland*, §§65-67; ECtHR, *Rotaru v. Romania*, §§43-44.
[1291] See *inter alia* ECtHR, *Klass and Others v. Germany*, §44; ECtHR, *Malone v. the United Kingdom*, judgment of 2 August 1984, App. no. 8691/79, §64; ECtHR, *Halford v. United Kingdom,* §44; ECtHR, *Weber and Saravia v. Germany*, §§76-79.
[1292] ECtHR, *Bykov v. Russia*, judgment of 10 March 2009, App. no. 4378/02, §§ 81, 83; ECtHR, *Oleynik v. Russia*, judgment of 21 June 2016, App. no. 23559/07, §§ 75-79. On video surveillance, see in general the considerations and cited case law in Chapter III, §3.2.1.2.
[1293] ECtHR, *Uzun v. Germany*, §§51-53; ECtHR, *Ben Faiza v. France*, judgment of 8 May 2018, App. no. 31446/12, §§53-61.
[1294] See *inter alia* ECtHR, *Roman Zakharov v. Russia*, §§ 163-305; ECtHR, *Szabó and Vissy v. Hungary*, judgment of 12 January 2016, App. no. 37138/14, §§52-89; ECtHR, *Centrum För Rättvisa v. Sweden,* judgment of 25 May 2021, App. no. 35252/08, §§365-374; ECtHR, *Big Brother Watch and Others v. the United Kingdom*, judgment of 25 May 2021, App. nos. 58170/13, 62322/14 and 24960/15, §§ 424-427.
[1295] See case law cited in §3.3. The expression "privacy spring" was coined by Peers (2014).
[1296] ECtHR, *Klass and Others v. Germany*, §36. See further in the Court's jurisprudence ECtHR, *Kennedy v. United Kingdom*, §119; ECtHR, *Zakharov v. Russia*, §153, ECtHR, *Szabó and Vissy v. Hungary*, §32.
[1297] On this topic, see Kosta E (2020b).
[1298] An overview will be provided below, §3.2.
[1299] See below, §3.1.

data retention schemes[1300]. Thirdly, the issues raised by the approach of the two Courts will be examined, with regard to both proportionality and available remedies[1301].

3.1. Justifying interferences on the rights to privacy and data protection

The principle of proportionality is undoubtedly one of the cornerstones of the European human rights protection apparatus. In fact, both the ECHR, in its Art. 8(2), and the Charter, in its Art. 52(1), refer to the principle of proportionality as the general method to assess restrictions on protected fundamental rights[1302]. Based on these provisions, both the CJEU and the ECtHR have developed procedural steps in their jurisprudence to evaluate whether limitations on protected rights are justified with regard to the proportionality principle.

3.1.1. In the ECHR system

The proportionality test in Art. 8(2) ECHR. To determine if restrictions on fundamental rights are compatible with the Convention, the ECtHR has devised a triple proportionality test. Firstly, the interference on the right must be "in accordance with the law". This means that the measure limiting the exercise of the right protected must be provided by the *law*, understood in its broadest sense. Indeed, to accommodate the specificities of national legal systems that are part of the Convention – including both common and civil law frameworks – the legal basis does not need to be necessarily found in a legislative act adopted by the Parliament; it can also be an act of secondary law or a specific case-law developed by internal courts[1303]. Nonetheless, to be recognised by the Court as a valid legal basis, the measure must at least be foreseeable (i.e., sufficiently detailed) and accessible to citizens, who shall be in the position of being able to anticipate the consequences of his or her own actions[1304].

Secondly, limitation must be necessary to achieve one of the legitimate aims explicitly mentioned in Art. 8(2) ECHR, among which we find "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".

Lastly, the restrictions imposed on fundamental rights need to be "necessary in a democratic society". Based on this formula, the Court has introduced its own proportionality assessment. The necessity is here interpreted as a criterion of proportionality between the limiting measure and its stated objective(s)[1305]. It allows interference only if the substantial benefit for society is proportionate to the cost imposed on the right at stake[1306], an argument which may recall utilitarian or collectivist perspectives. This aspect is however mitigated by the "democratic society" criterion, which can considerably restrict the variety and number of measures that can be accepted for the sake of certain

---

[1300] See below, §§3.2 and 3.3.

[1301] See below, §§3.4 and 3.5.

[1302] It should be noted that the Charter, differently from the Convention, foresees one general provision detailing the criteria to assess possible interferences on protected fundamental rights. The drafters of the Convention, on the contrary, opted for incorporating these assessment criteria (recalling the principle of proportionality) only in the provisions referring to non-absolute rights, such as Arts. 8 (right to respect for private and family life), 9 (Freedom of thought, conscience and religion) and 10 (Freedom of expression), 11 (Freedom of assembly and association). For the purposes of this research, we directly pointed to Art. 8 as this is certainly the most relevant when it comes to evaluating the impact of security and safety measures in the digital context, which may indeed affect the right to privacy and data protection.

[1303] See, e.g., ECtHR, *Kokkinakis v. Greece*, judgment of 25 May 1993, App. no. 14307/88, §52; ECtHR, *Cantoni v. France*, judgment of 11 November 1996, App. no. 17862/91, §29; ECtHR, *Coëme and Others v. Belgium*, judgment of 22 June 2000, App, nos. 32492/96, 32547/96, 32548/96, 33209/96 and 33210/96, §145.

[1304] See Chapter I, §3.2.3. In the case law, see ECtHR, *Zakharov v. Russia*, §§228, 233; ECtHR, *Rotaru v. Romania*, §52; ECtHR, *S. and Marper v the United Kingdom*, §95; ECtHR, *Kennedy v. United Kingdom*, §151.

[1305] Hildebrandt (2013), p. 376.

[1306] Id.

public objectives. In particular, the measure must respond to a "pressing social need"[1307], which excludes intense limitations of fundamental rights based on mere convenience.

Balancing in the ECtHR case law. The idea of balancing is intensively evoked by the principle of proportionality. And yet, it does not seem to have been envisaged by the drafters of the Convention, which was originally focused on setting out minimum rules of conduct by the States[1308]. The formulation "necessary in a democratic society" in Art. 8(2) seems to incorporate a binary test (either a measure is necessary, or it is not), rather than a balancing one[1309]. At some point, however, the Court shifted its reasoning from prohibitions for States to the protection of subjective rights. The approach does not entail assessing the lawfulness and necessity of certain actions by the state, but balancing different rights or interests against each other[1310].

On the one hand, some experts expressed criticism towards this development, as it makes the Court's judgments much more contextual and circumscribed to the specific case[1311]. The assessment may be limited to weighing the interests of the two parties against each other, while the Court may avoid answering more general legal questions that could facilitate the interpretation of the Convention. Therefore, balancing is not considered to bring legal certainty for case outcomes[1312].

On the other hand, scholars have also argued that the model of balancing is actually incorporated in Art. 8(2) ECHR[1313]. While it is acknowledged that trade-offs between individual rights and collective objectives are inevitable, limitations upon fundamental rights are accompanied by crucial guarantees (like the legality principle). For instance, the existence of additional safeguards protecting the right at stake can impact on the (strict) necessity test. A measure may be deemed proportionate if appropriate safeguards are provided to mitigate interference on the protected right. Therefore, even if restrictions upon fundamental rights may not be justified in terms of mere trade-offs, they may be so in terms of balancing, namely if specific safeguards are provided to compensate – and reduce – the sacrifice imposed on such rights.

Overall, these analyses show how the core reasoning behind the necessity test in the ECtHR case law continues to be debated. This is all the more true if this assessment is read in connection with the proportionality principle enshrined in Art. 52(1) CFREU, which will be discussed next.

3.1.2. In the EU system

The proportionality test in Art. 52(1) CFREU. The concept of proportionality is pivotal also in the EU legal system. It is recalled not only as one of its foundational values in the Treaties (Art. 4 of Treaty of the European Union, TUE), but also as a guiding principle in assessing whether limitations on fundamental rights are legally justified pursuant to Art. 52 of the Charter, which reads:

> "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

[1307] ECtHR, *Olsson v. Svezia*, judgment of 24 March 1988, App. no. 10465/83, §67.
[1308] Van der Sloot (2016b), p. 440.
[1309] Id., p. 441.
[1310] Id. (referring to ECtHR, *Delfi AS v. Estonia,* §139).
[1311] Van der Sloot (2016b), p. 448.
[1312] Id.
[1313] Hildebrandt (2013), p. 376; Loi et al (2020), p. 80.

Interpreting this provision, the CJEU has devised a fourfold proportionality test that closely resembles that of the German Constitutional Court. Like the ECtHR, the CJEU demands that the measures interfering with the rights protected comply with the legality principle, being also foreseeable and accessible to citizens. Secondly, the Court verifies whether the measure actually responds to an objective of general interest of the Union. However, unlike the ECHR system, this criterion is appreciated in a much more flexible way, as legitimate aims are not preventively listed in the Charter nor theoretically defined by the Court, which only identifies them on a case-by-case basis[1314].

Moreover, Art. 52(1) requires the respect of the essence of the right, as well as an assessment of the necessity and proportionality of the measure. Both these requirements will be examined in the following subsections.

3.1.2.1. The "essence of the right" criterion

An additional requirement in the CFREU test. A difference between the ECtHR and the CJEU tests concerns the "essence of the rights and freedoms" criterion. This requirement is only explicitly mentioned in the framework of the Charter, and certainly echoes the philosophical debate on trade-offs involving human rights[1315].

This benchmark has been subject to significant doctrinal and jurisprudential analysis in the legal domain, both at the EU and national level. For instance, Brkan defines it as "the untouchable core or inner circle of a fundamental right that cannot be diminished, restricted or interfered with"[1316]. Interfering with the essence of a right involves a kind of *objective*, rather than *subjective*, violation, i.e., a breach that would hurt any individual or class of individuals, regardless of the specific circumstances of the case[1317]. The roots of the concepts are often traced back in the German legal system, where Article 19(2) of the Constitution provides that "[i]n no case may the essence [*Wesensgehalt*] of a basic right be affected"[1318].

While the notion has made inroads in other Member States' constitutional settings, the CJEU had its first recourse to the essence of the right in the landmark case *Nold*. There, the Court recognised fundamental rights as being part of European Community (now Union) law, and underlined that these can be limited only "on condition that the *substance* of these rights is left untouched"[1319]. In absence of any binding text in primary law, the Court gradually developed this autonomous concept[1320] while taking inspiration from both national constitutional traditions of Member States[1321] and the ECtHR case law[1322]. As a crowning of this jurisprudential path, the "substance" of fundamental rights was then translated into the Charter with a different wording, becoming the "essence".

Despite this final acknowledgement in EU primary law, the "essence of the right" criterion has long been subject to diverging interpretations. Specifically, two doctrines have been opposed: the relative (or exclusionary) theory and the absolute (or integrative) one. The difference between the two revolves around the relationship of the "essence of the right" with the proportionality assessment.

On the one hand, the proponents of the absolute theory conceive the essence of the right as being completely independent from the proportionality principle. Fundamental rights are conceptualised as

1314 CJEU, *Digital Rights Ireland*, §42.
1315 Loi et al (2020), p. 81; Pino (2006), p. 16.
1316 Brkan (2018), p. 333.
1317 Id., pp. 350-351.
1318 Id., p. 339; Ojanen (2016), p. 324.
1319 CJEU, *Nold v Commission*, judgment of 14 May 1974, Case C-4/73, §14 [emphasis added].
1320 Brkan (2018), p. 347.
1321 Id., pp. 341-344.
1322 Id., pp. 348-349 (discussing the inconsistency of the interpretation and application of the notion in the ECtHR's jurisprudence).

being composed of a nucleus and a peripheral part, which can be restricted exclusively under certain conditions[1323]. The proportionality test would thus apply only to peripherical limitations to fundamental rights, with the core of the right being totally immune from such restrictions, even in the presence of powerful overriding reasons[1324].

On the other hand, the relative theory tends to merge the "essence of the right" criterion and the proportionality assessment. "Essence" has only a declarative value because the legitimacy of *any* interference can be assessed through the lens of proportionality. In the EU legal framework, however, a literal interpretation of Article 52 CFREU suggests that an absolutist approach is preferred[1325]. From the *Digital Rights Ireland* judgment onwards, the case law of the CJEU has made increasing references to this criterion and confirmed the latter interpretative perspective[1326].

In fact, the implications of an absolutist conception of the "essence of the right" parameter first became tangible in the *Schrems* case. Here, the CJEU annulled the Safe Harbor scheme based solely on a finding of violation of the essence of the rights to privacy and judicial protection[1327]. With regard to the former, the Court found that a legislation allowing "the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life"[1328]. With regard to the latter, on the other hand, the Court considered that a "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection"[1329]. Therefore, the CJEU deemed that it was not necessary to perform a proportionality test, reinforcing the independent conception of the essence of the right in its relationship with proportionality.

Despite its importance, the CJEU has never determined the essence of a right at the practical and theoretical level[1330]. This is particularly evident in the case-law on the right to data protection as enshrined in Art. 8 CFREU. While in some cases the essence of the right has been identified with the principle of purpose limitation[1331], in others the Court has considered that the gist of the right was safeguarded by the mere provision of security measures aimed at protecting the integrity of retained data[1332].

Nonetheless, legal scholars agree that this may actually be the result of an intentional choice of the CJEU. Even with few opportunities to examine the respect of the rights' essence, the Court seems to suggest that this is necessarily a *contextual* concept and that it can only be determined on a case-by-case basis, in consideration of the factual circumstances of the case[1333]. The requirement could therefore be examined only with reference to a specific security or safety measure, which leaves a significant margin of appreciation to the interpreter when determining what the essence of the right is in each individual case. When thinking about the impact of digital technologies, this vague approach certainly presents its advantages, because it can unfold its potential in ever-new factual and legal situations.

1323 Id., p. 336.
1324 Id.
1325 Brkan (2018), p. 360.
1326 CJEU, *Digital Rights Ireland*, §§39-40.
1327 For a thorough analysis, see Ojanen (2016).
1328 CJEU, *Maximilian Schrems v Data Protection Commissioner*, judgment of 6 October 2015, Case C-362/14, §94.
1329 Id. §95.
1330 Peers et al (2021), p. 1635.
1331 Jasserand (2018), p. 155, note 28 (referring to CJEU, *Opinion 1/15*, §150).
1332 CJEU, *Digital Rights Ireland*, §43.
1333 Ojanen (2016), p. 326. Christofi et al (2019); Tzanou M (2017), p. 43; Brkan (2018), p. 363 ff (proposing a methodology to determine the meaning of the concept).

3.1.2.2. The proportionality assessment

The proportionality principle is the last criteria listed in Art. 52(1) CFREU. As already mentioned, the CJEU was heavily inspired by the German Federal Constitutional Court in developing the procedural steps of its proportionality test[1334]. Importantly, the idea of balancing is strongly incorporated in the technique of the Court, which is particularly sensitive when it comes to molding the strictness of its assessment to the severity of interference affecting the right[1335]. In other words, the Court attempts to take into consideration different variables in weighing protected rights and values: when the limitation imposed on the right is considerably serious, the Court tends to apply a stricter approach, thereby requiring foreseen restrictions to be outbalanced by strong safeguarding countermeasures.

With regard to the argumentative passages undertaken by the Court, the first step is represented by the suitability criterion, which requires the infringing measure to be abstractly suitable to reach the stated objectives[1336].

The necessity criterion then follows, according to which the rights protected cannot be limited beyond what is strictly necessary to achieve the pursued goals. It should be noted that the "democratic society" formula, present in the Convention, was not explicitly resumed in the Charter; nevertheless, it can be well integrated in the analysis in virtue of the so-called principle of equivalence present in Art. 52(3) of the Charter. The latter indeed provides that as long as the Charter incorporates rights that correspond to those protected in the Convention, "the meaning and scope of those rights shall be the same as those laid down by the said Convention". This means that the content of the rights protected by the Charter – and possible limitations thereof – need to be assessed also with reference to their meaning in the system of the Convention, where the interpretation given to such rights by the ECtHR plays a crucial role.

The strict necessity principle is often confused with the test of proportionality *stricto sensu*, which represents the last stage of the CJEU's judicial review. Almost indulging in a political task, the Court balances the infringed rights and the pursued values, questioning whether the legislator has made a correct use of its margin of appreciation. In other words, the Court engages on pure axiological reasoning when deciding if the sacrifice imposed on the rights at stake is disproportionate compared to the potential societal benefits of the measure.

In conclusion, it is important to stress how the principle of proportionality and in its applications in EU law can reveal something important about the very nature of the EU legal order. In proportionality, legal scholarship has seen the "symbol of European *teleological* legality, which is representative of a legal system mainly built on principles that need to be mutually balanced"[1337]. In its procedural form, the principle of proportionality unravels all its potential to perform ever-refining value balancing tasks with a high level of flexibility.

It is true that the malleable nature of balancing as a technique has often been regarded as enemy of other important principles, such as that of legal certainty and homogeneity of legal decisions. In this perspective, balancing has been framed as a tool in the hands of the judiciary to arbitrarily decide what the actual scope of fundamental rights is in concrete cases[1338]. However, it should be also noted that balancing has in itself the potential of fostering the predictability of decisions in practical situations

---

1334 Kostoris (2018), p. 75.
1335 CJEU, *Digital Rights Ireland*, §§47-48.
1336 In *Digital Rights* (§43), the data retention measures foreseen by the Directive 2006/24/EC had been considered theoretically apt to the objectives of the fight against terrorism and serious crime.
1337 Kostoris (2018), p. 75 [emphasis added].
1338 Pino (2006), p. 20.

where the need to uphold general principles and norms is to be reconciled with that of making punctual decisions in specific instances[1339]. Here the procedural technique of proportionality provides us with a reliable framework to build legal knowledge in a predictable fashion, with the chance of submitting the outcomes of balancing to public scrutiny[1340]. As suggested above, this is paramount since emerging technologies are leading to unprecedented changes and situations which cannot be fully addressed with existing legal provisions. When digital technologies lead us to undiscovered territories, balancing as argumentative technique can help us to see clearly what "justifies our beliefs" and how legal knowledge is produced[1341].

3.2. The ECtHR's case law on surveillance: An overview

The beginning of the ECtHR's surveillance case law. Klass v. Germany inaugurated the ECtHR case law on communication interception. This landmark case established not only that the interception of communications falls within the scope of Art. 8(1) ECHR, but also that covert surveillance measures may be accepted as necessary in a democratic society only "under exceptional circumstances"[1342].

In *Malone v. United Kingdom*, the same principle was later applied to the issue of metadata processing. While it was acknowledged that this interference was not as serious as the interception of communications' contents, the processing of metadata collected through metering fell within the scope of Art. 8, and it was assessed by the ECtHR in relation to the basic requirements of legality, legitimacy and proportionality [1343].

Systematising the requirements for legitimate surveillance. With *Huvig* and *Kruslin* came the first systematisation of the surveillance legitimacy requirements. The ECtHR observed that "it is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated"[1344]. Therefore, the legality requirement was further articulated by the Court, which distinguished "a *material* requirement of legality; an *accessibility* requirement of legality; a *foreseeability* requirement of legality and a *rule of law* requirement of legality"[1345].

Specifically, foreseeability acquires the utmost importance in cases of covert surveillance. As it is often difficult (if not impossible) for individuals to prove they have been targeted by intrusive measures, the potential impact of surveillance and necessary safeguards need to be foreseeable from the legal basis itself[1346]. That is why in *Huvig* the Court articulated six foreseeability requirements that will become pivotal in its case law on criminal surveillance[1347]:

1339 Durante (2013), p. 441.
1340 Id., p. 455.
1341 Id., pp. 447, 455-456.
1342 ECtHR, *Klass and Others v. Germany*, §48. A through and critical assessment of the case law analysed in this Section can be found in De Hert et al (2020).
1343 ECtHR, *Klass and Others v. Germany*, §§84, 153. De Hert et al (2020), p. 7.
1344 ECtHR, *Huvig v. France*, §32.
1345 Id., §26. Cf. ECtHR, *Kruslin v. France*, judgment of 24 April 1990, App. no. 11801/85, §27; ECtHR, *Lambert v. France*, judgment of 24 August 1998, App. no. 23618/94, §23; and ECtHR, *Perry v. United Kingdom*, §45; ECtHR, *Weber and Saravia v. Germany*, §84; ECtHR, *Uzun v. Germany*, §60.
1346 Cf. ECtHR, *Kennedy v. United Kingdom*, §155. Cf. Vogiatzoglou (2018), p. 565.
1347 Id., §34. These safeguards will be applied, *inter alia,* in ECtHR, *Amann v. Switzerland*, §76; ECtHR, *Valenzuela Contreras v. Spain,* judgment of 30 July 1998, App. no. 58/1997/842/1048, §46; ECtHR, *Prado Bugallo v. Spain*, judgment of 18 May 2003, App. no. 58496/00, §30; ECtHR, *Association For European Integration And Human Rights And Ekimdzhiev v. Bulgaria*, 30 January 2008, App. no. 62540/00, §§75-77; ECtHR, *Bykov v. Russia*, §78; ECtHR, *Kennedy v. United Kingdom*, §152; ECtHR, *R.E. v. the United Kingdom*, judgment of 27 October 2015, App. no. 62498/11, §§120-130; ECtHR, *Szabó and Vissy v. Hungary*, §56; ECtHR, *Ben Faiza v. France*; ECtHR, *Centrum for Rittvisa v Sweden*, judgment of 19 June 2018, App. no. 35252/08, §§113-114.

1) categories of people liable to be monitored;
2) the nature of the offences which may give rise to surveillance measures;
3) limits on the duration of such monitoring;
4) procedure to be followed for storing the data;
5) precautions to be taken when communicating the data to the judges and defence;
6) circumstances in which data is erased or destroyed;
7) [Eventual element] Judicial control;
8) [Eventual element] Notification to the targeted individual;6

Later on, the *Huvig* requirements were applied to cases that did not concern individual telephone tapping in criminal investigations, like *Weber and Saravia v. Germany*, *Liberty* and *Kennedy*. These applications concerned new secret services' powers of strategic monitoring of communications through catchwords. These were the first acknowledgements in the judicial realm of what would then be defined as "mass surveillance" in subsequent decisions.

A lighter proportionality assessment for GPS surveillance. The *Huvig* criteria for criminal surveillance have not, however, been applied consistently by the ECtHR. For instance, the Court examined the implications of GPS surveillance in *Uzun*[1348], where the Court operated a lighter proportionality test[1349].

The collection of GPS data was considered less invasive than other forms of surveillance, and thus the Court adopted lower foreseeability standards. If *Huvig/Weber and Saravia* requirements comprised eight criteria (two of which optional), *Uzun* referred only to the grounds for ordering the surveillance measures, their nature, scope and duration, the authorities competent to review them and the procedures to seek effective remedy against them[1350]. No explicit reference was instead made to the procedures to process the data, the precautions to be taken when communicating the data, and the circumstances in which the data should be destroyed or erased[1351].

Thus, the Court seemed to have established a link between the seriousness of the interference and the level of detail requested to the legal basis to satisfy the foreseeability requirements[1352]. The ECtHR also appeared to suggest that *ex ante* judicial or independent authorisation may not be always indispensable, and it could be compensated by *ex post* safeguards like judicial review, or the exclusion of evidence in the ensuing proceedings and subsequent notification[1353].

Instead, in *Ben Faiza v. France* the Court seemed to contradict the approach sustained in *Uzun*[1354]. Although the investigative measures were considered to be the same, the Court applied the *Huvig* requirements in their entirety[1355]. Such inconsistency may be explained by the fact that the operation was not considered particularly invasive, as it had not been applied in real time[1356].

1348 ECtHR, *Uzun v. Germany*, §52.
1349 De Hert et al (2020), p. 11 ff. The same approach was than reiterated in ECtHR, *R.E. v. the United Kingdom*.
1350 Id., §63.
1351 De Hert et al (2020), pp. 11-12.
1352 Id., p. 12.
1353 Id., pp. 12-13. However, this approach is not always consistent in the case law of the Court. See ECtHR, *Brazzi v. Italy*, judgment of 27 September 2018, App. no. 57278/11.
1354 Id., p. 18. See ECtHR, *Ben Faiza v. France*. This case concerned surveillance measures taken against the applicant, who was a suspect in a criminal investigation relating to drug-trafficking offences. These measures consisted of the installation of a GPS device on his vehicle, and the court order issued to a mobile telephone operator to obtain records of his incoming and outgoing calls, together with the cell tower pings from his telephones, thus enabling the subsequent tracking of his movements.
1355 De Hert et al (2020), p. 18.
1356 ECtHR, *Ben Faiza v. France*, §74.

Arguably, the ECtHR does not provide much guidance for distinguishing different levels of intrusiveness, and thus strictness of proportionality assessments. The situations that give rise to stronger privacy concerns are not well discerned, or may be based on flawed factual assumptions (e.g., the less intrusiveness of GPS surveillance, or the higher intensity of real time monitoring), which makes the case law of the Court extremely unpredictable in this respect.

Zakharov. Russia. In this Grand Chamber judgment, the Court reiterated the criteria that the applicant should fulfil to claim the victim status in secret surveillance cases[1357]. The Court departed from its general approach by accepting claims *in abstracto* and, to this end, considered the scope of the legislation allowing for surveillance.

Specifically, it evaluated whether the applicant could possibly have been impacted by surveillance, either because: (1) she belonged to specific *groups* liable to be targeted; (2) the law in itself directly affected *everyone*, as it established a system where literally everyone can have their communication intercepted[1358]. In addition, the Court took into account the system of remedies available to individuals being monitored. Where there is no effective remedy and the risks of abuse are magnified, the need for judicial scrutiny is higher and the claimant is allowed to challenge the law directly *in abstracto*, with no obligation of proving that the surveillance measure was applied to them[1359].

3.2.1. *Centrum För Rättvisa v. Sweden* and *Big Brother Watch vs. United Kingdom*

The ECtHR's latest word on secret mass surveillance. Centrum För Rättvisa v. Sweden and *Big Brother Watch v. United Kingdom* currently constitute the last word of the ECtHR in matters of bulk secret surveillance. The two decisions will be jointly examined, since many of the considerations made by the Grand Chamber in *Centrum För Rättvisa* were also replicated *verbatim* in *Big Brother Watch.*

Centrum För Rättvisa dealt with the Swedish foreign intelligence system, commonly called "signal intelligence". This expression refers to the practice of intercepting, processing, analysing and reporting intelligence from electronic signals, which may be processed to text, images and sound. The intelligence collected may include both the content of a communication and metadata (the data describing, for instance, how, when and between which addresses the electronic communication occurs)[1360].

Big Brother Watch originated from a series of applications filed to the Court in the aftermath of the so-called "Snowden revelations", which had uncovered the extent of surveillance activities carried out by the United Kingdom. Specifically, ten civil rights associations (including Big Brother Watch) submitted that the covert interception practices carried out by British secret intelligence services (i.e., the Government Communications Headquarters', GCHQ) violated their right to private life[1361].

Having used electronic means of communications, they could have been intercepted in the framework of the US-UK intelligence sharing programmes (e.g., Prism and Upstream), especially in light of the sensitivity of their activities involving whistle-blowers and victims of human rights abuses. The applicants focused on section 8(4) RIPA, which regulated the interception of external communications (both content and metadata) between the United Kingdom and other countries[1362].

1357 ECtHR, *Zakharov v. Russia*, analysed by Cole et al (2016).
1358 ECtHR, *Zakharov v. Russia*, §171.
1359 Id.
1360 ECtHR, *Centrum För Rättvisa v. Sweden,* judgment of 19 June 2018, App. no. 35252/08, §7, analysed by Vogiatzoglou (2018); van der Sloot et al (2019).
1361 See van der Sloot et al (2019), pp. 253-255.
1362 The RIPA foresees the interception of both internal and external communications. While the former is regulated at section 8(1) RIPA, the latter is addressed at section 8(4) of the same act.

After the first Chamber judgements, the two cases were referred to the Grand Chamber. In both decisions, the Grand Chamber established new requirements for the assessment of dragnet surveillance regimes[1363]. At the outset, the Court acknowledged the reality of surveillance in the digital age, which can rely on multiple means and does not usually target individuals[1364]. It also stated that bulk interception systems are predominantly used for *foreign* intelligence collection and the detection of new threats from both known and *unknown* actors[1365]. Considering that threats to States have also proliferated, these bulk interception systems constitute a "valuable technological capacity" for the Contracting Parties to address these dangers and thus they can claim a legitimate need for secrecy in this domain[1366].

Subsequently, the Court assessed the existence of an interference on the right to private life. It stated that bulk interception systems should be regarded as a "gradual process in which the degree of interference with individuals Article 8 rights increases as the process progresses"[1367]. Some recurrent stages were identified:

> (a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);
>
> (b) the application of specific selectors to the retained communications/related communications data;
>
> (c) the examination of selected communications/related communications data by analysts; and
>
> (d) the subsequent retention of data and use of the "final product", including the sharing of data with third parties[1368].

It was evident for the Court that unfettered surveillance systems presuppose that data pertaining to individuals and being of no interest whatsoever for national authorities can be collected. Therefore, a filtering process is necessary: this initial searching, mostly automated, often relies on different "selectors" (or filters, keywords), including "strong selectors" (like an email address) that directly target specific individuals[1369]. Only the material that is selected through these automated means gets to be examined by an analyst, and can be used as intelligence for national security purposes.

Importantly, the Court considered Article 8 ECHR to be applicable at the ensemble of these stages. Nonetheless, it also labelled the interference occurring at the first steps of the surveillance to be less serious than the one taking place at the last stages, where the focus of the authorities has shifted to particular individuals, or the content of a communication is being examined[1370].

The Court then assessed the justification of the interference. It recalled the six foreseeability requirements that had been applied to cases of criminal surveillance (and beyond) since *Huvig*[1371]. However, the Court noted the differences between the field of criminal surveillance and that of bulk interception, which according to the Court is often directed at *international* communications and underpinned by different goals (e.g., investigating crime vs. early detection and the investigation of

---

1363 The decisions are critically analysed, *inter alia*, by Mitsilegas et al (2022), pp. 27 ff.
1364 ECtHR, *Big Brother Watch and Others v. the United Kingdom*, §322.
1365 Id. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §236.
1366 Id.
1367 Id., §325.
1368 Id. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §239.
1369 Id., §§ 326-327. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §§240-241.
1370 Id., §330. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §244.
1371 Id., §335. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §249.

cyberattacks, counterespionage and counterterrorism)[1372]. Also, the ECtHR observed that bulk surveillance does not always end up targeting specific individuals.

Therefore, the Grand Chamber stressed the need to review its approach in bulk interception cases. The first two *Huvig* criteria were not considered to be readily applicable in this domain, as they indicate (i) the categories of people liable to be monitored, and (ii) the nature of the offences which may give rise to surveillance measures[1373].

Nevertheless, the scope of the surveillance still needed to be circumscribed, and the Court held that any process of bulk surveillance should be subject to "end-to-end safeguards" in order to minimise the risks of abuse [1374]. This meant that at each stage of the process, domestic authorities should assess the necessity *and* proportionality of the undertaken measures. Additionally, bulk surveillance should be subject to *ex* ante independent authorisation, limiting its scope and object. Supervision *ex ante* and *ex post* review should also be ensured.

Beyond *ex ante* authorisation, supervision *during* and *after* the operationalisation of surveillance should be foreseen. An independent authority should review the necessity and proportionality of the activities performed at each stage of the process[1375]. As for the notification regime, the Court recalled that *ex post* notification is a relevant factor in assessing the effectiveness of the remedies available to those who have been targeted by surveillance. This could be unnecessary, however, when the domestic legislation allows *any person* who suspects having been intercepted to file an application to the internal courts[1376]. A remedy independent from prior notification was even labelled by the Court as being more safeguarding[1377]. What matters the most is that the authority entrusted with supervision is independent from the executive and offers an adversarial process[1378].

Importantly, the Court underlined the fact that the compliance of a surveillance regime with the Convention can only be assessed globally. The system should be considered "as a whole", making sure that weaknesses are compensated by the other safeguards[1379]. Also, bulk interception needs to be authorised by an independent body from the executive.

This authority should in particular take into account the *purpose* of the interception, and the *bearers* (e.g., the filtering keywords) or communication routes liable to be targeted[1380]. Indeed, selectors – and strong selectors specifically – are one of the salient points in assessing the legitimacy of a blanket surveillance regime, as these are the parameters delimiting the actual purview of the monitoring operations[1381]. Not to frustrate the inherent needs of flexibility in the choice of the bearers, these should not necessarily be identified *a priori* in the warrant. Nonetheless, this authorisation should at least mention the types or categories of selectors that are likely to be used[1382]. Higher safeguards should apply when strong selectors are applied[1383].

Following this analysis, the Grand Chamber presented the following legitimacy criteria to be applied to bulk interception systems:

1372 Id., §§ 344-345. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §§258-259.
1373 Id., §348. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §262.
1374 Id., §350. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §264.
1375 Id., §356. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §270.
1376 Id., §357. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §271.
1377 Id., §358. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §272.
1378 Id., §359. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §273.
1379 Id., §360, 370. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §274.
1380 Id., §352. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §266.
1381 Id., §353. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §267.
1382 Id., §354. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §268.
1383 Id., §355. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §269.

1. The grounds on which bulk interception may be authorised;
2. The circumstances in which an individual's communications may be intercepted;
3. The procedure to be followed for granting authorisation;
4. The procedures to be followed for selecting, examining and using intercept material;
5. The precautions to be taken when communicating the material to other parties;
6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. The procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance[1384].

Applying these criteria to the system stemming from section 8(4) of the RIPA, in *Big Brother Watch* the Court unanimously identified the following shortcomings. Firstly, the bulk interception was authorised only by the Secretary of State, and not by a body independent of the executive[1385]. Secondly, the categories of selectors to select relevant materials for examination were not included in the application for a warrant[1386]. Thirdly, the use of strong selectors was not subject to prior internal authorisation[1387].

Likewise, the Court found that the regime for obtaining communication data from communication service providers was not in accordance with the law[1388]. However, the Court considered that the regime by which the United Kingdom could request intelligence from foreign governments and/or intelligence agencies had sufficient safeguards in place to protect against abuse and to ensure that UK authorities had not leveraged such requests as a way of circumventing their duties under domestic law and the Convention[1389].

The Court also found a violation of Article 8 ECHR in *Centrum För Rättvisa*. Although "quality of the law" requirements were respected, the scheme presented three shortcomings. Firstly, there was no clear rule on when intercepted material not including personal data should be destroyed[1390]. Secondly, no provision in Swedish legislation explicitly demanded to consider the right to privacy of individuals when resolving to transmit intelligence material to foreign partners[1391]. Thirdly, there was no effective *ex post facto* review[1392]. Therefore, the system did not meet the requirement of "end-to-end" safeguards.

3.3. The CJEU's case law on data retention: An Overview

EU Security policies after 9/11: The introduction of the Data Retention Directive. In the aftermath of 9/11, the EU has made efforts to strengthen its security-related policies, also under the influence of the United States[1393]. Especially after the terrorist attacks in Madrid and London, a pro-security lobby gained traction in the EU and supported the introduction of a legal framework allowing law enforcement agencies to access location and traffic data in the context of the fight against terrorism and serious crime[1394].

1384 Id., §361. *Compare* ECtHR, *Centrum För Rättvisa v. Sweden,* §275.
1385 Id., §377.
1386 Id., §381.
1387 Id., §383.
1388 Id., §§521-522.
1389 Id., §514.
1390 ECtHR, *Centrum För Rättvisa v. Sweden,* §342.
1391 Id., §330.
1392 Id., §364.
1393 See Argomaniz (2009), p. 120.
1394 Marin (2016), p. 212; Guild et al (2014), p. 3.

This resulted in the adoption of the Directive 2006/24/EC (the Data Retention Directive, DRD)[1395]. The DRD laid down rules for telecommunication service providers to retain communications metadata about their customers, for a period of six months to two years. These data –already retained by providers for billing purposes – could be transmitted to law enforcement agencies upon their request, to be used in proceedings related to terrorism and serious crime.

The introduction of the DRD triggered an unprecedented outburst among Member States and privacy activists[1396]. Since it applied to everyone without distinction, the DRD was considered as establishing an actual mass surveillance system in the EU. Many doubted the compatibility of the instrument with Union law and national constitutional frameworks, and its transposition was delayed in several Member States. Finally, in 2012 two preliminary references were lodged before the CJEU: one filed by the Irish NGO Digital Rights Ireland; the other by two Austrian citizens and the Carinthian government. Among the questions to the Court, the one about the compatibility of the DRD with the rights to privacy and data protection (Arts. 7, 8, 52(1) CFREU) is arguably the most relevant for our analysis.

Digital Rights Ireland. To verify whether the challenged legislation was justified in light of the Charter, the CJEU applied the test of Art. 52(1) CFREU. Preliminarily, the Court observed that both the rights to privacy and data protection were interfered with by the DRD. To establish an interference with Art. 7, it was not considered relevant whether the information about private life is sensitive or if the persons concerned had been inconvenienced in any way[1397]. Likewise, the Court deemed that the right to data protection was interfered with because the DRD provided for the processing of personal data[1398].

As for the justification of these limitations, the existence of a legal basis and of an objective of general interest did not pose any issue[1399]. Therefore, the CJEU went on to examine whether the essence of the rights protected was compromised by the measure. This was excluded for Art. 7, because the data collection only concerned metadata, and not the content of communications[1400]. Similarly, for Art. 8, the Court stated that provisions for data protection and security in the DRD safeguarded the essence of the right to data protection[1401].

With regard to the proportionality test, the CJEU observed that the seriousness of the interference required the performance of a particularly strict assessment. That was justified in light of "a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference"[1402].

Moving to the merits of the proportionality test, the Court first considered that the collection of metadata was *per se* suitable to pursue the predefined objectives and could be a valuable tool in criminal investigations[1403]. When it came to the strict necessity test, however, it held that despite the importance of the fight against terrorism and serious crime, such an objective could not "in itself, justify a retention measure such as the one established by Directive 2006/24" in light of the fight against serious crime[1404].

1395 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 L 105, 13.4.2006, p. 54–63.
1396 Marin (2016), pp. 213-214.
1397 CJEU, *Digital Rights Ireland*, §33, analysed *inter alia* by Marin (2016); Flor (2014).
1398 CJEU, *Digital Rights Ireland*, §38. On the interference upon the right to the freedom of expression, see §28.
1399 Id., §§41-44.
1400 Id., §39.
1401 Id., §40.
1402 Id., §47.
1403 Id., §49.
1404 Id., §51.

Because technological means of communication are ever more important in daily life, a surveillance measure entailing the retention of data about the entirety of the European population could not be considered strictly necessary[1405]. Most importantly, the Court criticised the absence of any link between the data retained and the goals of public security, as well as the lack of any objective criterion (e.g., temporal, geographical, subjective) limiting the scope of the measure[1406].

Furthermore, the DRD did not lay down substantial and procedural safeguards to limit subsequent access to data by law enforcement, for instance by not identifying the categories of serious criminal offences that could legitimise such processing[1407]. Also, the length of the retention was censured[1408]. With regard to data protection, the Court emphasised that the DRD did not establish enough safeguards to ensure the security and protection of the data. For instance, the Directive did not provide for specific rules adapted to the quantity of stored data, its sensitive nature, and the risks of unlawful access[1409]. The integrity and confidentiality of the data could be compromised, especially if communication service providers were left with an overly large margin of appreciation in deciding which technical-organisational standards of security to apply[1410]. Nor was there an obligation to store the data within the EU, which could jeopardise the effective supervision of an independent authority over the processing (Art. 8(3) CFREU)[1411]. Therefore, the Court deemed that the EU legislator had overstepped its margin of appreciation and annulled the DRD for its lack of compliance with the Charter.

Unfettered regimes of metadata retention in the e-Privacy Directive: Tele2/Watson. The annulment of the DRD did not put an end to the generalised retention of communications metadata. Indeed, Member States are still allowed to introduce similar measures pursuant to Art. 15(1) of the Directive 2002/58/EC (the e-Privacy Directive)[1412]. This provision allows legislative measures to be adopted that limit the right to confidentiality in relation to (traffic) data generated by electronic communication devices, thus making the collection of such information possible in order to safeguard national security (i.e., State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. In any case, such measures should be a necessary, appropriate and proportionate measure within a democratic society. In this sense, Art. 15(1) lists the retention of data for security-related purposes as an example of such restrictive measures.

Given the similarity of the two instruments, the e-Privacy Directive was also challenged before the Court after *Digital Rights Ireland* in the *Tele2 Sverige/Watson* case. Preliminarily, the Court examined the scope of the Directive (and of its own jurisdiction over it). The British Government and the European Commission had objected that only the national provisions pertaining to data retention by private service providers fell within the purview of the Directive, while those relating to the access to such data by law enforcement did not[1413]. Indeed, Art. 1(3) excluded the "activities of the State" in the areas of

1405 Id., §56.
1406 Id., §59.
1407 Id., §§60-62.
1408 Id., §§63-64.
1409 Id., §66.
1410 Id., §67.
1411 Id., §68.
1412 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 sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.
1413 CJEU, *Tele 2/Watson,* §§65-66, analysed *inter alia* by Pollicino et al (2017).

criminal law and public security, defence and State security from the scope of the Directive, including the economic well-being of the State when the activities relate to State security matters.

Interpreting the Directive systematically, however, the CJEU stated that both the retention of and the access to data by law enforcement fell within the scope of the instrument, otherwise the ratio and meaning of Art. 15(1) would have been deprived of any sense[1414].

At any rate, the Court observed that the restrictions allowed in Art. 15(1) of the Directive had to be interpreted strictly. Otherwise, there could be a risk of inverting the natural relation between general rules (i.e., confidentiality rights) and exceptions[1415]. Only a general objective like the fight against serious crime could justify an interference such as the one entailed by national legislations implementing Art. 15(1) of the e-Privacy Directive[1416]. At the same time, a general goal of that kind could not, in itself, justify such a generalised surveillance measure[1417]. Like the system of the DRD, these provisions implied the collection and storage of data relating to people having no connection whatsoever with illicit activities, and thus the objectives of public security pursued[1418].

Nonetheless, the Court granted that Member States could still adopt legislation allowing for the *targeted* retention of traffic and location data for the purposes of law enforcement and national security as a preventive measure, provided that the categories of data to be stored, the means of communication affected, the individuals affected, and the retention period adopted are limited to what was strictly necessary[1419]. Likewise, national legislation should lay down clear and precise rules indicating in which circumstances and under which conditions service providers must grant the competent national authorities access to the data[1420].

By refusing to directly annul Art. 15(1) of the Directive, the CJEU provided guidelines to achieve a Charter-compliant interpretation thereof. As in *Digital Rights,* it stressed the need for clear and precise rules ensuring that the limitation upon the rights protected is kept within the boundaries of what is strictly necessary; minimum safeguards should be provided for to protect individuals against the risks of abuse[1421]. This meant, for instance, that processing should be circumscribed by objective criteria establishing "a connection [even an indirect one] between the data to be retained and the objective pursued"[1422].

R*etention of civil identity data: Ministerio Fiscal.* In this case, the CJEU transposed the principles elaborated in its previous case law to the specific case of access to data that allows the civil identity details of owners of SIM cards activated in stolen cell phones to be identified. Specifically, the Court was attentive to distinguish this kind of interference from the ones examined in *Digital Rights* and *Tele2/Watson*. Indeed, accessing data with the sole purpose of linking specific SIM cards to their users constitutes a less serious limitation on the right to privacy, which cannot have the same implications as the combined processing of all one's communication metadata[1423]. Because civil identity data cannot give any indication on the date, time, duration and length of the communications made via these SIM

1414 Id., §73 ff.
1415 Id., §§89, 104.
1416 Id., §102.
1417 Id., §103.
1418 Id., §§105-106
1419 Id., §108.
1420 Id., §117.
1421 Id., §109.
1422 Id., §§110-111. These criteria might be, as mentioned in *Digital Rights*, of a geographical nature.
1423 CJEU, *Ministerio Fiscal*, judgment of 2 April 2018, C-207/16, §§60-61, analysed by Tracol (2019); Docksey (2019).

cards, the processing cannot be considered particularly intrusive. Therefore, such operations do not need to be directed solely at the investigation and prosecution of serious offences[1424].

3.3.1. *Privacy International* and *La Quadrature du Net*

Unfettered surveillance making inroads in the CJEU case law. In these two cases, the CJEU's Grand Chamber re-examined the question of how to correctly interpret Art. 15(1) of the e-Privacy Directive. British, French and Belgian Courts asked the CJEU to clarify whether the provision, read in light of the Charter, precluded the obligation imposed on service providers to indiscriminately retain the data of their customers and share them with law enforcement and national security agencies[1425].

The *Privacy International* case stemmed from a complaint filed by the namesake NGO before the IPT, challenging the lawfulness of the interception practices under the RIPA[1426]. The IPT lodged a preliminary ruling before the CJEU, asking whether this legislation, imposing the unfettered *transmission* of communication metadata to intelligence services on services providers, was compatible with the Charter and the requirements set in the Court's jurisprudence (i.e., *Digital Rights* and *Tele 2/Watson*).

In *La Quadrature du Net and Others* instead, some human rights organisations brought actions before the French Council of State, questioning the lawfulness of a series of national decrees imposing the obligation of indiscriminately retaining communication metadata on communication service providers[1427]. The French Council of State thus lodged several preliminary questions with the CJEU, asking whether a general data retention obligation, and the real-time collection and transmission to security actors of traffic and location data was compliant with the Charter[1428]. These proceedings were also joined with those stemming from the Belgian Constitutional Court, which had similar doubts on the compatibility of the domestic legislation with Art. 15(1) of the e-Privacy Directive with the Charter.

In both cases, the Court preliminarily examined the question of the scope of Union law with respect to national security matters. Because of the exceptions in Arts. 4(2) TEU and 1(3) of the e-Privacy Directive, some Member States had indeed claimed that bulk interception operations for national security purposes were essential State functions and did not fall within the scope of EU law[1429].

Relying on the considerations made in *Tele 2/Watson*, however, the Court reiterated that the scope of Art. 15(1) of the Directive extends not only to national legislation on data *retention*, but also to legislation on the subsequent *access* to data by law enforcement or intelligence services[1430]. Article 15(1) would be deprived of any practical effect if national legislation on metadata retention were interpreted as being excluded from the scope of the Directive[1431]. While Member States retain the prerogative to define their essential security interests, the mere fact that a domestic measure has been taken for national security purposes cannot make EU law inapplicable and exempt the Member States from their obligation to respect it[1432].

1424 Id., §62.
1425 See CJEU, *Privacy International,* judgment of 6 October 2020, Case C-623/17 and CJEU, *La Quadrature du Net and Others*, judgment of 6 October 2020, Joined cases C-511/18, C-512/18 and C-520/18, analysed *inter alia* by Mitsilegas et al (2022); Eskens (2021); Tznaou et al Vogiatzoglou et al (2020a); Vogiatzoglou et al (2020b); Vogiatzoglou et al (2020c). For an analysis of this case law and previous CJEU's decisions on data retention, see also Juszack et al (2021).
1426 CJEU, *Privacy International,* §19.
1427 CJEU, *La Quadrature du Net and Others*, §§56-57.
1428 Id., §68.
1429 CJEU, *Privacy International,* §32. *Compare* CJEU, *La Quadrature du Net*, §89.
1430 Id., §39. *Compare* CJEU, *La Quadrature du Net*, §96.
1431 Id., §42.
1432 CJEU, *Privacy International,* §44. *Compare* CJEU, *La Quadrature du Net,* §99.

Moving to the merits, the Court recalled that Art. 15(1) should be interpreted restrictively[1433], and that national legislation based on this provision entails a *particularly* serious interference with the right to privacy[1434]. Traffic and location data are indeed very sensitive, and their combined processing can reveal a great deal about someone's private life (movements, sexual orientation, religious beliefs, personal relationships).

With regard to the objectives of general interest that could justify such interferences, the Court introduced a more granular distinction, unprecedented in its case law:

> The importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats […] can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives[1435].

Against this backdrop, in *Privacy International* the Court deemed that not even an objective of national security could justify legislation entailing general *access* by security agencies to all retained traffic and location data, regardless of whether there is a(n indirect) connection between the data and the general objectives pursued[1436]. A transmission of data concerning all electronic communications users without distinction cannot be seen as strictly necessary and thus compliant with the principle of proportionality.

In *La Quadrature du Net* instead, the Court examined multiple iterations of metadata retention, access and analysis: (i) preventive metadata retention for "national security" purposes; (ii) metadata retention for "public security" purposes; (iii) preventive retention of IP addresses and data relating to civil identity for the purposes of combating crime and safeguarding public security; (iv) real-time metadata analysis by network service providers; (iv) real-time metadata collection by law enforcement agencies.

Firstly, the Court considered that national security objectives can legitimise more serious interferences on the rights to privacy and data protection than the ones allowed by public security goals and the fight against (serious) crime in general[1437]. Therefore, the unfettered retention of metadata of *all* communication service users is allowed only in the interest of national security and for a limited period of time, that is as long as the national threat is genuine and present, or foreseeable[1438]. The retention shall be subject to effective review by a court or an independent administrative body, which can ensure that the measure is enforced for the time strictly necessary and with the necessary safeguards against the risks of abuse[1439].

Secondly, when law enforcement agencies pursue actions to combat serious crime and prevent threats to public security, the *Digital Rights Ireland* and *Tele2/Watson* case law still applies. The Court rejected indiscriminate data retention and required clear and precise rules ensuring that the system of surveillance does not exceed what is strictly necessary. Objective criteria shall circumscribe the scope of

---

1433 Id., §59; *Compare* CJEU, *La Quadrature du Net,* §111.
1434 Id., §71. *Compare* CJEU, *La Quadrature du Net* §132.
1435 Id., §75; *Compare* CJEU, *La Quadrature du Net* §136.
1436 Id., §78. *Compare* CJEU, *Tele 2/Watson,* §119. Eskens (2021, p. 147) highlights the novelty of *Privacy International* with respect to previous case law, which had only dealt with legislation requiring generalized *retention* rather than *transmission.*
1437 CJEU, *La Quadrature du Net,* §136.
1438 Id., §137.
1439 Id., §§138-139.

the measure so that the retention only targets data pertaining to specific categories of people, geographical areas and time frames which present links, even indirect or remote, with the commitment of serious criminal offences (i.e., hotspot approach)[1440].

Thirdly, the CJEU examined the case of preventive retention of IP addresses and civil identity data. It noted that, although IP addresses are part of traffic data, they are generated regardless of any particular communication and are mainly exploited to determine the natural person who owns the terminal equipment from which an internet communication is made. Since normally only IP addresses of communication senders are retained, the Court considered these data to be less sensitive, as they do not reveal information about the recipients of the communication[1441].

Nonetheless, their indiscriminate collection still constitutes a serious interference on the rights to privacy and data protection, given that they can be used to reconstruct the user's complete clickstream and build complete profile of his or her behaviour and preferences[1442]. Also, IP addresses are not necessary for billing purposes as other categories of metadata are[1443]. Therefore, the Court held that only the objectives of fighting serious crime, protecting public and national security can justify such interference, which should always be limited to what is strictly necessary (e.g., in terms of retention periods and procedural safeguards to access the data)[1444]. As for civil identity data, the Court reiterated the position held in *Ministerio Fiscal*, considering that the processing of such data does not imply a particularly serious interference with the rights protected, and their unfettered collection can therefore be justified also in light of the fight against less serious criminal offences[1445].

Fourthly, the CJEU addressed measures of automated screening of all traffic and communication data upon LEA's request, applying the parameters indicated by the latter. For its indiscriminate nature, this interference can be justified only by the purpose of protecting national security, when the threat is genuine and present or foreseeable[1446]. Further guarantees should also apply. Pre-established criteria and models should be specific and reliable, as well as non-discriminatory, and should be kept up-to-date and cannot be drawn on sensitive data taken in isolation[1447]. At any rate, the individuals flagged by a positive match cannot be subject to the negative consequences of the latter only based on the automated processing of their personal data[1448]. Likewise, in situations where traffic and location data are collected and transmitted in real-time to law enforcement agencies, such a measure must be authorised by a court or another independent authority and can only be applied to specific persons previously identified as having links with terrorist threats[1449].

Concerning the notification requirements in these two cases, the CJEU explicitly held that national authorities engaging in real-time monitoring of traffic and location data need to notify the targeted individuals of the past surveillance, so as to allow them to exercise their right to effective remedy[1450]. In the context of automated analysis, national competent authorities are only obliged to publish general information about the existence of the measure. However, if during these activities an individual is

---

1440 Id., §§143-144, 147-148.
1441 Id., §152. Mitsilegas et al (2022, pp. 10-11) note also that the Court finally qualified IP addresses as "traffic data" but isolated them from other categories of traffic data to allow their indiscriminate retention.
1442 Id., §153.
1443 Id., §154.
1444 Id., §156.
1445 Id., §157. *Compare* the position held by the ECtHR, *Breyer v. Germany*, judgment of 30 January 2020, App. no. 50001/12.
1446 Id., § 177.
1447 Id., §§180-182. Cf. CJEU, *Ligue des droits de l'homme*, §§189 ff.
1448 Id., §182.
1449 Id., §§184, 188.
1450 Id., §190. Cf. CJEU, *Tele 2/Watson,* §121.

spotted as being potentially involved in terrorist activities, he or she must be notified individually that their data has been subject to additional scrutiny by security agencies[1451].

It should be considered that the CJEU's legal framework for data retention may soon (if not so already) become established case law. Indeed, the considerations made in *La Quadrature du net* and *Privacy International* have been recently confirmed in a Grand Chamber judgment, *G.D. v Commissioner of An Garda Síochána and Others*[1452], *SpaceNet AG*[1453] and *Spetsializirana prokuratura*[1454]. Its underlying principles have also been translated in the field of financial supervision in *VD and SR*[1455].

Appropriateness of general interest objectives in algorithmic surveillance. The principles established in this case law have not, however, been applied always consistently by the CJEU. In *Ligue des droits humains*, the Court assessed the legitimacy of the PNR Directive in light of Arts. 7 and 8 of the Charter. In this case as well, it evaluated the seriousness of the interference and its justification in relation to the objectives of general interest pursued by the legislation. The court labeled the surveillance regime established by the Directive as "continuous, untargeted and systematic" and also considered the employment of algorithmic means of processing therein[1456]. Although this could qualify as a mass surveillance system, comparable to those established by generalized data retention, the Court esteemed that it could be justified also in light of the fight against serious crime and terrorist offences[1457]. The Court also held that the PNR system could not be leveraged for intelligence purposes[1458]. This remark seems to contradict the hierarchy of general interests established in *La Quadrature du net,* which allows competent authorities to use collected data for purposes having greater weight than those having legitimised the original collection. This apparent departure from the previous case law can be explained in light of the specific provisions of the PNR Directive, which allows the processing of air passenger data only to counter serious crimes and terrorist offences. Nonetheless, it should be borne in mind that crime prevention and national security could well intersect when it comes to terrorist offences, which is something that is not taken into account by the Court.

Moreover, the CJEU introduced an important caveat in its assessment, specific to the use of algorithmic means of processing. It indicated that the rate of false positives resulting from the processing should be taken into account when assessing the justifiability of the overall system[1459]. The effectiveness and proper functioning of the surveillance regime should thus constitute an important factor in examining its appropriatedness in light of the specific general objectives pursued.

3.4. Mass surveillance in the European human rights system

Outline. The proliferation of surveillance technologies and practices has not gone unnoticed by the experts and public at large. Especially since the Snowden revelations, the public debate surrounding State and non-State monitoring activities has intensified, and diverse civil rights organisations have brought claims challenging their lawfulness before the judiciary. This has led to an "explosion" of decisions – both by the ECtHR and the CJEU – which have defined a general framework for

[1451] Id., §191.
[1452] CJEU, *G.D. v Commissioner of An Garda Síochána and Others*, judgment of 5 April 2022, Case C-140/20. See Saifert (2022).
[1453] CJEU, *Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH*, judgement of 20 September 2022, Joint Cases C-793/19 and C-794/19.
[1454] CJEU, *Spetsializirana prokuratura*, judgement of 17 November 2022, Case C-350/21.
[1455] CJEU, *VD and SR,* judgment of 20 September 2022, Joined cases C-339/20 and C-397/20.
[1456] CJEU, *Ligue des droits de l'homme v Conseil des Ministres*, judgement of 21 June 2022, Case C-817/19, §§110-111.
[1457] Id., §122.
[1458] Id., §§231-232.
[1459] Id., §§123-124.

surveillance in the European multi-level system of human rights. A set of more recent decisions seems, however, to have departed from the initial path and to be more welcoming towards pervasive surveillance[1460]. At the same time, more granular assessments have been introduced by the Courts, especially with regard to the distinction between different general interest goals for surveillance.

Against this backdrop, this Section will provide a critical assessment of the abovementioned jurisprudence, firstly highlighting the gradual acceptance of mass surveillance in Europe[1461]. Secondly, the focus will shift to the principle of proportionality, investigating its relationship with the concept of "mass surveillance", and exploring its possible iterations in the smart city context[1462].

3.4.1. Towards the acceptance of unfettered regimes?

Strasbourg: long-standing tolerance towards unfettered surveillance systems. One of the biggest challenges in preventive surveillance is circumscribing its scope. Because threats are still unknown, authorities cannot reasonably know *a priori* which data will be useful for their future activities[1463]. Thus, the application of the proportionality principle is critical at the data collection stage. Still to this day, the solution for national authorities has often been to collect *all* the available data, and only later veryfy which information can actually be useful to intelligence services and law enforcement.

In this regard, the ECtHR's approach has been to provide Contracting Parties to the Convention with a wide margin of appreciation in deciding what kind of surveillance system to put in place[1464]. The choice, of course, lies between unfettered and targeted surveillance regimes. Arguably, the ECtHR has always been tolerant towards unfettered surveillance schemes for national security purposes, although exercising its supervision on the matter. The choice of implementing a mass surveillance system thus falls within the margin of appreciation of the State, but the Court still assesses how the system is *operationalised*, and specifically if effective safeguards against abuse are provided for.

Luxembourg: National security and mass surveillance appear on the stage. On the contrary, the position of the CJEU in its first leading judgment on data retention (*Digital Rights Ireland*) appeared to be stricter. The general assumption underlying its reasoning was that of the strict incompatibility between unfettered surveillance systems and the principle of proportionality[1465].

Since *Privacy International* and *La Quadrature du Net*, however, the concept of national security has made inroads in the reasoning of the CJEU, and this has impacted on its balancing exercise. It is interesting to note that these decisions have been adopted in the timeframe between the Section decisions on *Big Brother Watch* and *Centrum För Rättvisa,* both of which dealt with foreign intelligence practices, and the subsequent Grand Chamber judgments. Probably under the influence of the ECtHR, the CJEU now seems to be more tolerant with systems of unfettered retention of metadata, although it still applies stricter safeguards to the matter. In *La Quadrature du Net*, *G. D.* and *VD and SR*, for instance, the Court stressed the risks of circumventing relevant safeguards by employing data collected for national security purposes in criminal proceedings.

[1460] Cf. Juszcak et al (2021), p. 243.
[1461] See below §3.4.1.
[1462] See below §3.4.2.
[1463] Neroni Rezende (2020a), pp. 196-197; Juszcak, Sason (2021), p. 243.
[1464] See *inter alia* ECtHR, *Klass and Others v. Germany*, §§49-50; ECtHR, *Leander v. Sweden*, §59; ECtHR, *Weber and Saravia v. Germany*, §106; ECtHR, *Big Brother Watch and Others v. the United Kingdom*, §§308, 387.
[1465] Marin (2016), p. 223.

Accepting mass surveillance? This change in perspective begs the question of whether the two Courts are "surrendering", so to speak, to a phenomenon of pervasive surveillance that appears more and more inevitable in light of the widespread use of mobile (IoT) devices[1466]. Although these last decisions on surveillance have been described as victories for privacy activists, others have more cynically underlined the fact that (unfettered) data retention has never been "off the table" in the European landscape[1467].

What seems to have changed, however, is the methodology in the ECtHR's assessment of the surveillance system with regard to Art. 8 ECHR. Indeed, while the CJEU still employs strict rule-based (or formal) reasoning in checking the proportionality requirements of metadata retentions laws, the ECtHR now relies on a more *holistic* test. In particular, the Court verifies whether end-to-end safeguards in mass surveillance schemes are respected "as a whole", referring to a benchmark that has had a long life in its jurisprudence (especially with respect to fair trial guarantees under Art. 6 ECHR[1468]).

It cannot be excluded that such methodology will not be adopted in the future by the CJEU as well, considering that the standard is also increasingly used in EU law as an open clause[1469]. Certainly, the two Courts have different roles in the systems where they respectively act. The ECtHR rules *ex post facto* in concrete cases, it usually disposes of a global view of the facts, and it can be thus drawn to make a global assessment of the case. Nevertheless, in cases of secret surveillance, where the Court judges *in abstracto*, it may be considered similar to the role played by the CJEU, which enucleates the abstract proportionality requirements that national legislation should have to comply with the Charter.

At any rate, it is certain that such a holistic approach is further lowering the threshold of compatibility of surveillance schemes with the Convention, thus leading to a more tolerant approach towards unfettered regimes of surveillance.

3.4.2. Proportionality and mass surveillance

Attuning proportionality factors in mass surveillance. Despite the challenges it poses, the principle of proportionality is still regarded as a valuable tool to determine *when* and *which kind of* surveillance is justifiable. Setting aside clear-cut cases, however, scholars often doubt as to its application in grey areas, where different proportionality assessments could be argued for[1470]. The recent case law of the ECtHR and CJEU on the matter certainly helps to attune proportionality evaluations in secret mass surveillance cases.

Diverse regimes for collection of and access to data are now envisaged according to the legitimacy goal pursued. Nonetheless, the issue with this approach is that numerous key concepts are not clearly defined either in the system of the Convention, or in EU law[1471].

Therefore, the following subsections will examine different criticalities and open questions in the current approaches of the two European Courts when assessing the proportionality of surveillance. Firstly, the meaning of "mass" or "bulk" surveillance will be reviewed, and a more granular taxonomy of surveillance types will be proposed to improve proportionality assessments[1472]. Secondly, by comparing different legitimacy goals (i.e., national security, law enforcement, economic wellbeing, environmental needs), differentiated margins of appreciation will be mapped, specifying whether

[1466] Cf. Judge Pinto de Albuquerque (2021), p. 172.
[1467] Juszcak et al (2021), p. 259. Cf. Mitsilegas et al (2022), p. 10; Tzanou et al (2022), p. 147.
[1468] Kostoris (2018), p. 87.
[1469] Id., p. 59.
[1470] Thomsen (2020), p. 374; Macnish (2015).
[1471] Judge Pinto de Albuquerque (2021), p. 170.
[1472] See §3.4.2.1.

stricter (or lighter) proportionality assessments should be applied in each context[1473]. Specifically, it will be determined whether and how necessity and proportionality requirements could apply beyond the security domain to regulate environmental and resource management-related surveillance in smart cities[1474].

3.4.2.1. The meaning of "mass surveillance": A taxonomy of surveillance

Contradictory terminology. One of the biggest issues in the ECtHR's approach to mass surveillance is the lack of a consistent terminology, which may reflect the lack of a clear understanding of the matter. The problem is not without legal consequences, considering that the Court has now devised a different set of requirements for bulk interception of communications in *Big Brother Watch*. In his partly dissenting opinion, Judge Pinto de Albuquerque considered this departure from the antecedent case law to be unjustified, as the *Huvig* criteria (initially tailored to targeted criminal surveillance) had also been applied in cases of unfettered intelligence gathering like *Weber and Saravia* and *Liberty*[1475].

By looking at the Court's case law on covert surveillance, it firstly appears that the term "mass", in reference to surveillance, does not always refer to the alternative between targeted and non-targeted measures. Indeed, in cases pertaining to targeted criminal surveillance (e.g., *Zakharov*), the Court assimilated the measure at stake to mass surveillance basically for its covert nature, broad scope and the absence of available remedies[1476]. This suggests that, at times, instances of targeted interception may actually be treated as mass surveillance by the ECtHR.

Moreover, in *Big Brother Watch* and *Centrum För Rättvisa*, the Court extended the same regime of bulk interception to the situation where the competent authorities filtered intercepted information through "strong selectors", i.e., keywords or identifiers related to a given individual. This process is actually comparable to targeted interception, but was still labelled by the ECtHR as "bulk" surveillance, and exempted from reasonable suspicions requirements and prior authorisation by an independent authority[1477].

Overall, in both decisions the ECtHR used the expression "mass surveillance" only to refer to interception operations carried out on "general" communication channels, not on devices belonging to specific individuals. Therefore, the criterion employed to identify the kind of surveillance at play was the *means* through which communications travelled, i.e., the bearers. On the contrary, the reasoning was insensitive to whether strong or "weak" selectors were applied in the interception, and thus whether specific individuals were targeted in the process.

In his separate opinion, Judge Pinto de Albuquerque censured this new approach[1478]. If the ECtHR implicitly assimilates targeted and non-targeted interception but constructs a different regime for bulk surveillance on the bearers, Pinto argues that the regime to be applied should continue to be the same, as bulk interception can also target specific individuals (i.e., through the use of strong selectors).

Critically, the means through which communications are intercepted can be an important criterion through which targeted and non-targeted surveillance can be distinguished. Monitoring measures performed on a device are certainly targeted, but the same does not go for surveillance carried out on the bearers. These operations can be directed either at specific individuals, or not. Therefore, the distinction between mass or bulk surveillance should not be focused on the *means* used, as argued by the ECtHR, but on the nature of the *selecting criteria* for the information. While the use of individual-

[1473] See §3.4.2.2.
[1474] See §3.4.2.3.
[1475] Judge Pinto de Albuquerque (2021), p. 173; Separate opinion by Judges Lemmens, Vehabović and Bošnjak (2021), §19.
[1476] ECtHR, *Zakharov v. Russia*, §178. Cf. van der Sloot et al (2019), p. 256.
[1477] Separate opinion by Judges Lemmens, Vehabović and Bošnjak (2021), §23.
[1478] Judge Pinto de Albuquerque (2021), p. 170. On NSA surveillance techniques, see Cayford et al (2015), pp. 643-650.

based criteria (e.g., strong selectors) necessarily leads to targeted surveillance, non-individual-based ones should be associated with non-targeted and thus mass/bulk surveillance.

Temporal restrictions to mass surveillance. In the case law of both the ECtHR and the CJEU, emerges the concern to temporally limit unfettered surveillance regimes. According to the CJEU, for instance, national security threats are different from the ones stemming from criminal behaviour in general, even those of a serious nature, which generate a general and permanent risk of tensions and disturbances to public security[1479].

However, if the premise is that national security risks emerge only as one-off threats, the argument may actually be detached from reality. The integrity of the State, both in its democratic institutions and critical infrastructure, is increasingly perceived as a *permanent* concern and a top priority in (supra)national agendas, especially in light of technological advancements. Nonetheless, the CJEU does not provide any objective evidence demonstrating the *exceptional* nature of national security threats, and thus of generalised data retention measures, in comparison to public security ones. Nor does it introduce maximum limits to the duration of such operations, or to their potential extensions[1480]. Therefore, it appears difficult to imagine how unfettered surveillance schemes do not become the rule: temporal criteria may not be the most apt to build an accurate taxonomy of surveillance.

A taxonomy: mass, hybrid, targeted surveillance. Integrating the insights of both the ECtHR and the CJEU, multiple criteria could be discerned to classify different surveillance schemes. Geographical, subjective and goal-oriented standards may go hand in hand with the practical means employed, as well as the criteria used to select relevant information. Temporal restrictions may also come into play, although they cannot be easily applied to mass surveillance.

Against this backdrop, surveillance could be best represented as a *continuum*, where targeted and mass surveillance stand at the two extremes of the spectrum. In between, two "hybrid" forms of surveillance could be identified (i.e., mass/hybrid and hybrid-targeted surveillance).

Firstly, mass surveillance is not restrained either by subjective criteria (it is not targeted at predefined individuals), or by geographical criteria. Especially when surveillance is implemented on electronic communications, it is difficult to restrain surveillance geographically, which explains why distinguishing between foreign and internal intelligence gathering often appears unfeasible[1481]. The CJEU appears to take into account this aspect. In a case on metadata retention, for instance, the Court indicated that surveillance by videocameras is not comparable to the generalized retention of location data, which is by nature more extended in scope[1482].

Secondly, there are forms of surveillance that cannot be restrained subjectively, but geographically and temporally. That would be the case of "mass-hybrid" surveillance, operated in public spaces underlined by high security concerns (e.g., airports). These systems retain some features of mass surveillance because they can be directed at *anyone* circulating within them, indiscriminately. In the urban landscape, a good example is EFR, which could be aimed at spotting anyone displaying suspicious behaviour in public venues.

Thirdly, it is possible to discern another category of hybrid surveillance, which shares some ties with classic targeted surveillance. This is "hybrid-targeted" surveillance, which includes live facial recognition in public spaces. Police forces employ such systems in open places (e.g., squares, streets) processing the

1479 CJEU, *La Quadrature du Net,* §§136-137.
1480 Cf. Juszcak et al (2021), p. 253.
1481 Venice Commission (2015), pp. 7-8.
1482 CJEU, *Spetsializirana prokuratura*, §45.

biometric data of all passers-by, thus making the interference with fundamental rights particularly critical. Nonetheless, surveillance is not targeted at each of these individuals, but only at those whose biometric templates are stored in predefined watchlists (comprising e.g., suspected or warranted terrorists or serious offenders). This makes live AFR through watchlists ontologically different from EFR (which entails a broader scope), but still very serious in terms of invasiveness of the interference.

Lastly, targeted surveillance measures traditionally used in the criminal field are directly targeted at individuals and often (but not always) performed on their own devices. Therefore, they are restricted both in terms of individuals targeted and means used.

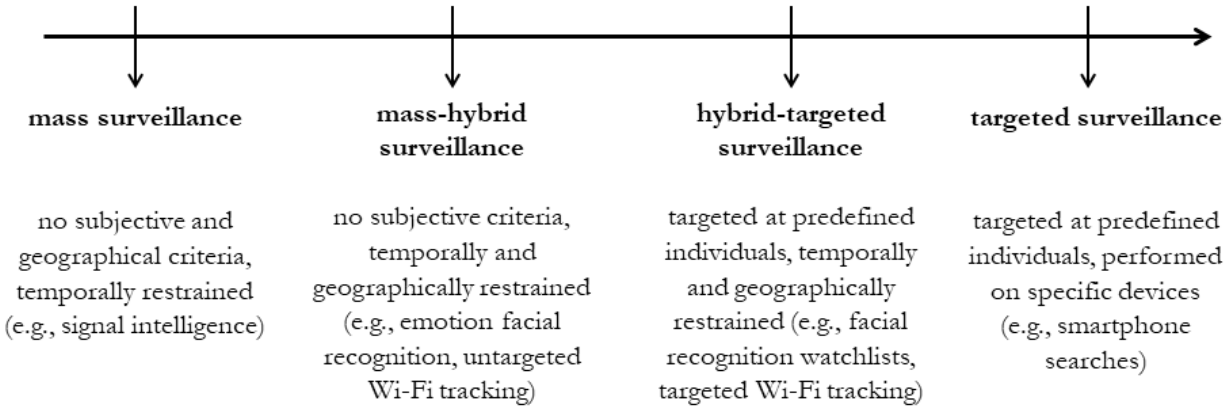

Fig. 3. Surveillance Taxonomy

3.4.2.2. Public interest in the Convention and EU law

Ill-defined and overlapping concepts. Arguably, the case law of the ECtHR and the CJEU is also lacking clear-cut definitions of the public interest goals that justify surveillance (e.g., national vs. public security). While these concepts are irreducibly vague, their definitional issues have major implications, as the two Courts now employ different proportionality standards according to the general objectives pursued by surveillance scheme. For instance, concepts like national and public security are ill-defined, potentially overlapping, and liable to cover manifold interests, also depending on Member States' interpretations of the matter[1483]. Also, the ECHR and relevant EU legislation do not define these notions coherently, and the two European Courts have not brought much clarity to the matter.

3.4.2.2.1. Legitimacy goals in the ECHR

Casuistic and extensive interpretation of Art. 8(2) legitimacy goals. Starting with the Convention system, it is well known that Art. 8(2) ECHR mentions "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" as legitimate goals for interference with the right to private life.

This list is large enough to comprise most government activity, and the ECtHR embraced a rather large interpretation of these terms, often maintaining that more than one clause could apply in the examined cases[1484]. With respect to national security, the Court has never further elaborated on the precise meaning of the concept, rather relying on a case-by-case assessment and often accepting the claims of Contracting Parties in that sense[1485]. For instance, the Court has deemed that espionage,

[1483] For instance, it has been underlined that for Iceland, fish represents an issue of national security.
[1484] Schabas (2017), p. 404; Cameron (2000), pp. 32, 55; Vogiatzoglou et al (2020d), p. 37; Harris et al (2014), p. 511.
[1485] Vogiatzoglou et al (2020d), p. 38.

terrorism[1486], subversion[1487], separatist organisations[1488], and inciting disaffection of military personnel[1489] could all be labelled as threats against national security. The expression "public safety" has instead been considered by scholars to be included under the umbrella of public security, together with the protection of health and morals [1490].

3.4.2.2.2. National vs. public security in the EU

Contradicting definitions. In the EU, national and public security can be invoked by Member States as exceptions to the main rules and freedoms in the internal market[1491]. Nonetheless, different pieces of legislation and case law define these concepts in a contradictory manner, especially in their mutual relationship.

Firstly, national security is labelled as the sole responsibility of Member States in Art. 4(2) TEU. The CJEU has provided a definition only in the *Promusicae v. Telefonica* case, where it specified the collective scope of the notion: "national security (…) constitutes activities of the State or of State authorities unrelated to the fields of activity of individuals"[1492].

In data protection law, Recital 12 LED includes not only the fight against crime in the concept of public security, but also the tasks conferred to LEAs of maintaining law and order, where necessary to prevent threats that may lead to a criminal offence. Likewise, the CJEU assimilates public security goals with the fight against serious crime in its jurisprudence[1493].

Nonetheless, Recital 19 of the Regulation on the free flow of non-personal data states that[1494]

> The concept of "public security", within the meaning of Article 52 TFEU and as interpreted by the Court of Justice, covers both the internal and external security of a Member State, as well as issues of public safety, in order, in particular, to facilitate the investigation, detection and prosecution of criminal offences. It presupposes the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society, such as a threat to the functioning of institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations, or a risk to military interests (…).

In both cases, the safeguarding of public security is arguably associated with law enforcement undertakings, also in the *preventive* sphere. It includes tasks entrusted to security authorities that go beyond the strict boundaries of ongoing criminal proceedings, like those directed at the maintenance of law and order. While this is coherent with the CJEU approach, the references to the activities taking place outside the remit of criminal investigations may be too nebulous, as underlined by the EDPS[1495].

If the definition of public security is *per se* vague in EU law, so is its relationship with "national security". In several pieces of EU legislation, the two concepts are jointly mentioned with no further

---

1486 ECtHR, *Klass and Others v. Germany*, §§48-50.
1487 ECtHR, *Leander v. Sweden*, §20.
1488 ECtHR, *United Communist Party of Turkey and others v. Turkey*, judgment of 30 January 1998, App. No. 19392/92, §§10, 48, 55.
1489 ECommHR, *Arrowsmith v. the United Kingdom*, decision of 5 December 1978, App. No. 7075/75.
1490 Vogiatzoglou et al (2020d), p. 37.
1491 Id., p. 40. See Arts. 346-347 TFUE.
1492 CJEU, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, judgment of 29 January 2008, Case C-275/06, §51.
1493 Vogiatzoglou et al (2020d), p. 46.
1494 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.
1495 EDPS (2015), pp. 5-6.

differentiation, which makes it difficult to draw a line between them[1496]. Sometimes, they are even conflated into one another.

This approach likely stems from the jurisprudence of the CJEU, which in *Tsakouridis* found that public security could be impacted by "a threat to the functioning of the institutions and essential public services and the survival of the population, as well as the risk of a serious disturbance to foreign relations or to the peaceful coexistence of nations, or a risk to military interests"[1497]. Consequently, Recital 19 of the Regulation on the free flow of non-personal data now seems to merge the two notions, by including *external* threats to the very integrity of the State under the umbrella of public security, i.e., the functioning of their (democratic) institutions, essential public services, survival of the population, military interests.

3.4.2.2.3. Issues in smart cities and beyond

Public vs. national security. This conflation between national and public security in EU law and the Convention appears to pose great challenges. It seems that an overlap between the notions of national and public security cannot be easily avoided.

For instance, diverse activities constituting threats to national security are often criminalised in many legal orders (e.g., terrorist offences). Which surveillance regime would apply in such cases, the lighter one meant for national security, or the stricter one designed for criminal matters? If the data were collected under national security purposes, could it be repurposed in related criminal investigations?

The vagueness of the concept of serious crime, partially addressed by the CJEU in *Digital Rights*, also remains underdefined in the ECtHR's jurisprudence. In their separate opinion on *Big Brother Watch*, Judges Lemmens, Vehabović and Bošnjak outlined the features of what is defined by the Court as "serious crime": (i) a sanction of imprisonment for three years or more; (ii) conduct involving the use of violence, resulted in substantial financial gain; (iii) the conduct was carried out by a large number of persons in pursuit of a common interest[1498]. In their view, such definition covers a broad scope of behaviours, which could raise doubts about the proportionality of potential surveillance measures applied to the individuals concerned.

Furthermore, the adopted notion of public security seems to have englobed aspects that are widely labelled as national security concerns in the doctrine. In particular, national security is said to comprise not only the protection of territorial integrity, of the population, and political independence from external armed attacks, or interference from foreign powers in domestic issues[1499]. It also incorporates the integrity of the economy, energy, environment, food, critical infrastructure and cybersecurity thereof[1500].

If the protection of critical infrastructure has been explicitly labelled as part of public security by the CJEU, it remains difficult to determine which surveillance regime should be applied to ensure the security of critical infrastructure and services in smart cities. If such matters were comprised under the label of public security, they would be subjected to the geographical limitations imposed by the CJEU on metadata retention. Specifically, the surveillance should be limited to areas of a high incidence of serious crime, like those visited by a high number of people, or strategic locations such as airports, stations and tollbooth areas (hotspot approach)[1501].

1496 Vogiatzoglou et al (2020d), p. 45.
1497 CJEU, *Land Baden-Württemberg v Panagiotis Tsakouridis*, judgment of 23 Novemeber 2010, Case C-145/09, §44.
1498 Separate opinion by Judges Lemmens, Vehabović and Bošnjak (2021), §29.
1499 Cameron (2000), p. 43.
1500 Viganò et al (2020), p. 158; Wendell (2018); Rudinow Saetnam (2018).
1501 CJEU, *La Quadrature du Net*, §150.

With regard to smart city infrastructure, however, this approach would ignore the issues brought by the increasing integration of IoT sensors in this context. Notoriously, embedding sensors in urban infrastructure has significantly broadened surface attacks for hackers and other malicious actors[1502], also exposing citizens to risks for their personal safety (e.g., in driverless vehicles). Urban infrastructure is much more interconnected, and delimiting surveillance measures such as data retention to well-defined physical areas appears very problematic from a security/safety perspective. Rather, for its worrisome implications, the protection of critical infrastructure in smart cities may call for a wider system of data surveillance.

3.4.2.3. What role for environmental and economic-oriented surveillance?

A void definition? The "economic wellbeing" of the State is one of the legitimacy goals mentioned in Art. 8(2) ECHR. This is the only provision comprising such a notion, although it could be easily extended to the others (i.e., Arts. 9-11)[1503]. The ECtHR has not defined its precise meaning and has rather relied on the claims of respondent States in this sense[1504].

Notoriously, the Court accepted that economic wellbeing interests could legitimise an interference on the right to private life in *Yordanova and Others v. Bulgaria*. The case involved the eviction of an unauthorised Roma settlement, and the ECtHR considered that there was "sufficient evidence of genuine plans for urban development in the area and health and safety hazards". Thus, it was "legitimate for the authorities, in the interests of economic well-being and the protection of health and of the rights of others [to proceed with the eviction]"[1505].

In *Zakharov* instead, the Court showed more reluctance in accepting the public interest goals listed in Russian legislation authorising secret surveillance measures. Specifically, the Court did not censure the goals themselves (e.g., the "economic and ecological security"), but criticised that no clear definitions and examples were given by the respondent State[1506].

Moreover, with specific regard to (covert) surveillance, stark scepticism can be detected towards the use of such monitoring techniques for the interests of economic wellbeing, which could legitimise economic and industrial espionage[1507]. Multiple actors could indeed exploit such arguments to legitimise surveillance when no real national security risks are at play.

Economic development, however, is one of the backbones of smart cities. What kind of measures impacting on private life could urban authorities undertake to sustain it, considering that "urban development plans" have been deemed to fall within the purview of interests of economic wellbeing? Certainly, it is not up to the ECtHR to lay down such definitions[1508]. Thus, in absence of theoretical indications, some urban-related scenarios will be hypothesised below.

Economic wellbeing in smart cities. Considering the collective rationale underlining the legitimacy goals listed in Art. 8(2), one could wonder whether purely individual commercial interests would be enough

[1502] Kitchin et al (2019c); Dodge et al (2019); Edwards (2016); Kitchin (2016a).
[1503] Schabas (2017), p. 405.
[1504] Id.
[1505] ECtHR, *Yordanova v. Bulgaria*, judgment of 24 April 2012, App. no. 25446/06, §115.
[1506] ECtHR, *Zakharov v. Russia*, §248.
[1507] Judge Pinto de Albuquerque (2021) Partly concurring, partly dissenting Opinion, p. 178; European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_EN.html. Accessed 12 May 2022; Venice Commission (2015), §§10, 73, 88.

[1508] Cf. ECtHR, *Zakharov v. Russia*, §248.

to justify serious interferences with the right to privacy. That would be the case of regulations allowing for the unrestricted use of emotional AI-equipped billboards in public spaces for targeted advertising. The same goes for schemes of unlimited repurposing of data collected in the public interest (e.g., location data) in the commercial sector (e.g., insurance).

When economic interests acquire a collective meaning in connection with other public interests (e.g., health, public safety), these may legitimise broad measures of data processing. For instance, this could be argued for operators of essential services. As defined by the NIS Directive, they constitute public and private entities in the energy, transport, banking, financial, health, water, digital infrastructure sectors: (a) that provide services that are essential for the maintenance of critical societal and/or *economic* activities; (b) whose service provision depends on network and information systems; (c) whose potential incidents would have significant disruptive effects on the provision of the service[1509].

Mass or mass-hybrid surveillance schemes could only be legitimised when the protection of critical infrastructure is at stake, depending on whether surveillance is needed on a city-scale or can be restricted to specific high-risk areas.

Environmental needs in smart cities. The protection of the environment is also included in modern conceptualisations of national security[1510]. Governments can indeed take measures to ensure the economic security of the State, but also of the environment, to avoid degradation, resource depletion, natural disasters, and pollution that threaten the security of the nation in any manner[1511].

Enhancing environmental needs would certainly favour a more open view on data collection in urban centres, although no environmental issue would arguably reach a level of seriousness such as to threaten the integrity of the country. The definitional conundrum surrounding public and national security affects environmental matters as well, complicating the task of determining which surveillance framework could be applicable in different scenarios.

As for economic wellbeing, much depends on the concrete policy goal pursued with the surveillance, although the CJEU case law tends to apply lighter proportionality assessments when environmental needs are involved[1512]. (e.g., Mass or mass-hybrid surveillance schemes may only be legitimised where environmental integrity is at stake (e.g., serious resource depletion or scarcity). On the contrary, objectives of mere resource optimisation and management could ground hybrid-targeted systems. This could be the case of hotspot checks in relevant infrastructures (e.g., smart grids, traffic management).

It should be considered, however, that it may be conceptually difficult to restrict environmental surveillance with individual-based criteria, which arguably makes mass or mass-hybrid regimes better suited to this case. Geographically, the data collection would be limited to a city scale (with specific areas of concern being difficult to identify). *Big Brother Watch/Centrum För Rättvisa* requirements would imply that the grounds for which bulk interception in cities could be authorised should be identified *a priori* on a legal basis, e.g., to avoid resource depletion. Data collection should be authorised *ex ante* by independent authorities. The circumstances in which individuals' data could be intercepted, i.e., the choice of non-individual-based selectors, should be directed at the detection of anomalies in urban patterns (e.g., identification of busiest areas, bus lines, potential network security breaches).

[1509] Arts. 5(2) and Annex II of the Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30 (the NIS Directive).
[1510] Wendell (2018), pp. 651-652.
[1511] Id., p. 651.
[1512] Jacobs (2006), p. 197.

Conversely, individual-based criteria (as in *Huvig*) could help delimit the surveillance to pre-known areas of intense energy consumption, targeting specific neighbourhoods and households. Such targeted or hybrid-targeted schemes could be applied only to pursue objectives of resource optimisation, which do not imply serious threats to the environment. However, this approach should be applied with caution, as the choice of relevant criteria may easily lead to discriminatory results (e.g., disproportionately affecting poor districts with inefficient or obsolete energy systems)[1513].

3.5. Legal remedies

Protection gaps in large-scale surveillance. Any surveillance regime, especially if broad in scope, needs to be combined with a sound oversight system, granting remedies for potential infringements of fundamental rights. In particular, secret surveillance poses great dangers for the rule of law, and (quasi-)judicial review of the operations is crucial to uphold transparency in democratic societies.

Nevertheless, research has shown how procedural laws at the national and supranational level lack mechanisms to challenge the impact of large-scale processing (including in smart cities)[1514]. Firstly, surveillance laws in the security field bear a certain degree of secrecy and indeterminacy, which hampers people's awareness of their being subject to monitoring. The lack of *ex post* notification mechanisms further downsizes individuals' chances to challenge surveillance.

At the supranational level, issues also stem from the institutional constraints of the ECtHR and CJEU. On the one hand, the ECtHR has been devised as a court ruling on specific violations of the Convention in concrete cases, thus excluding the review of general policies enacted by contracting parties (*in abstracto* claims).

On the other, the EU Treaties afford individuals limited chances to directly interact with the CJEU. Private individuals (i.e., non-privileged applicants under Art. 268 TFUE) are generally excluded from active eligibility to file actions for annulment before the Court pursuant to Art. 263 TFUE[1515]. Therefore, individuals (and civil society organisations) have been relying on preliminary rulings to indirectly challenge the validity of EU laws. This path, however, does also entail some practical limitations, as its efficacy depends on whether national laws allow such entities to initiate domestic proceedings on such matters, as well as on the willingness of national judges to present preliminary questions to the CJEU.

Outline. Against this backdrop, some solutions may already be available in the European legal framework. The ECtHR has developed a promising path to examine the legitimacy of surveillance laws at the general level, although certain issues remain. EU data protection legislation also embeds mechanisms that may help to challenge large scale data practices. Thus, this Section will firstly examine gaps in the current ECtHR surveillance case law on *in abstracto* claims. Secondly, potential remedies will be identified in EU legislation. Lastly, solutions for the smart city context will be proposed.

3.5.1. The limits of *in abstracto* claims before the ECtHR

The current ECtHR approach to in abstracto claims. Since *Klass*, the ECtHR accepts that the mere existence of secret surveillance legislation suffices for an applicant to claim victim status in alleged

[1513] The same is argued, with regard to *La Quadrature du net*, by Tzanou et al (2022). On the indirect discriminatory effects of algorithmic processing see also CJEU, *Ligue des droits de l'homme,* §197.
[1514] See generally van der Sloot et al (2021b).
[1515] They may do so in (rare) cases when decisions taken by the institutions (1) are formally addressed to them; (2) if they are not, they are of individual and direct concern to them; (3) they are of direct concern to them and do not entail implementing measures.

violations of the Convention. Such deviation from the scope of the Court's jurisdiction, allowing for the examination of *in abstracto* claims, is however subject to some limitations, which have been outlined in *Zakharov*[1516].

The Court assesses the admissibility of the claims by examining whether the applicant could possibly have been impacted by the legislation, either because he or she belongs to specific *groups* liable to be targeted, or the law in itself directly affects *everyone* due to its scope[1517]. When no internal remedies are provided, the applicant does not need to prove that he or she could have been subject to surveillance.

In *Big Brother Watch*, however, the Court characterised this requirement in a stricter fashion. When the national system *does* provide remedies, the applicant is eligible to file an application before the ECtHR only if he or she is able to show that he or she could have been impacted due to their personal situation[1518].

Legal issues. The admissibility system of secret surveillance claims before the Court relies on two critical assumptions: (1) the applicant (an individual, non-profit organisation or group) can be identified; (2) he or she is a victim of a ECHR violation[1519]. When confronted with more advanced techniques of surveillance (e.g., algorithmic surveillance), such interpretation clashes with the fact that (1) contemporary surveillance is not always directed at named individuals, (2) criteria for selecting relevant information/targets are very dynamic, (3) data collected about certain individuals may indirectly impact on the situation of others[1520].

Likely, the issue lies in the Court's struggle to abandon a more "individual-based" system of review claims, and fully embrace a "general" one, whereby no limits are posed to the examination of abstract allegations against national legislations. This resistance in accepting *actiones popularis* can be detected in how it remains anchored to the notion of "victim" and "harm", and the applicant's likelihood to have been targeted by the surveillance.

Moreover, the ECtHR does not seem to place great emphasis on the mere collection of data as an interference on privacy and data protection. In *Big Brother Watch*, the Court considered that while the mere storing of data amounts to an interference, its seriousness increases only as the bulk interception process progresses (e.g., when the content of an individual's communication is examined by public authorities)[1521]. Again, this approach may disregard the features of algorithmic surveillance, whereby data-related harms may not always be directly observable and measurable.

Furthermore, in *Big Brother* the Court seems to blend the *subjective* criterion of being a "victim" (Art. 34 ECHR) and the *objective* criterion of the exhaustion of domestic remedies (Art. 35 ECHR). Indeed, individuals placed in systems where such remedies are provided are burdened with additional strain when trying to access the ECHR system of protection. Specifically, they need to pass a "reasonable likelihood" test showing they have been victim of a Convention violation, something which is not required of applicants within systems devoid of any remedies.

[1516] See above §3.2.

[1517] ECtHR, *Zakharov v. Russia*, §171.

[1518] ECtHR, *Big Brother Watch v. United Kingdom*, judgment of 13 September 2018, App. no. 58170/13, 62322/14 and 24960/15, §392.

[1519] Kosta (2020b), p. 8.

[1520] Id., pp. 7, 10.

[1521] ECtHR, *Big Brother Watch and Others v. the United Kingdom*, §330. Before that, in *Friedl*, the Court had held that the mere storing of the applicant's photographs by the police did not engage Art. 8 ECHR, as the authorities had not pursued an attempt of identification. The same reasoning has been consistently applied by the Court in the domain of data collection by CCTV.

This may be problematic as being a victim of a Convention violation reflects a substantial and factual situation that should not be confused with the procedural requirement of the exhaustion of domestic remedies. Certainly, when such remedies are considered to be ineffective, the Court accepts claims that have not gone through all the stages of national review mechanisms. With respect to their status as victims of algorithmic surveillance, however, all individuals should be placed in equal position to access the Court's jurisdiction, regardless of the situation of internal remedies.

Practical limitations. Setting aside legal constraints, efforts to challenge surveillance laws can also be frustrated by practical difficulties. Firstly, individuals often lack the cognitive and financial resources to discern the impact of obscure surveillance programs, especially those relying on AI techniques.

Secondly, legal practitioners are often wary of engaging in strategic and public interest litigation in the field of privacy and data protection. Similarly, judges frequently display a cautious attitude with respect to the possibility of posing preliminary questions to supranational courts[1522].

Strategic litigation by civil society organisations has been seen as a promising path to increase accountability in the field of secret surveillance[1523]. To this day, however, even this solution suffers from empirical limitations. Research has indeed highlighted that such organisations often do not avail of the budgetary and personal resources to engage in lengthy litigation processes, and would rather leverage summary proceedings where matters are only marginally examined by judges[1524].

3.5.2. Possibilities for collective actions in EU law

Remedies in data protection law. Importantly, both the GDPR and the LED leave room for strategic litigation promoted by collective organisations[1525]. Firstly, Art. 80 GDPR foresees forms of collective representation of data subjects before a supervisory authority. It provides for data subjects having the right to mandate not-for-profit entities to lodge a complaint on their behalf. Also, Member States may discretionally allow organisations and associations to lodge complaints before a supervisory authority, regardless of a mandate being afforded to them by a data subject[1526]. Organisations and associations active in the field of data protection have already exercised such procedural rights in some notable judicial cases, even before the enactment of the Regulation. This suggests the potential positive impact of this provision[1527].

Secondly, Art. 55 LED takes a stricter stance on the matter. The provision is similar to Art. 80(1) GDPR and gives data subjects the right to mandate non-profit organisations to lodge complaints against the violation of their data protection rights. However, collective organisations are not allowed to initiate proceedings without any mandate from data subjects. Such a limitation, although explainable in light of the features of the criminal domain, bears the risk of undermining the accountability of public authorities in this field, where surveillance is often secret.

3.5.3. Potential solutions in smart cities

Improvements for the ECtHR and data protection law. The approach of the ECtHR in secret surveillance is promising with a view to achieving a more collective-oriented system of protection for smart city

[1522] van der Sloot et al (2021b), pp. 318, 328.
[1523] See Eijkman (2017).
[1524] van der Sloot et al (2021b), p. 327.
[1525] Pagallo et al (2017), pp. 67-70.
[1526] CJEU, *Meta Platforms Ireland Limited, formerly Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V,* judgment of 28 April 2022, Case C-319/20, §59.
[1527] See, for instance, CJEU, *Privacy International.* Before the Regulation, see CJEU, *Digital Rights Ireland.*

surveillance. Nonetheless, two improvements are necessary. Firstly, the seriousness of the interference caused by data collection should be enhanced. This would allow individuals and groups to claim their status as victims regardless of any concrete or demonstrable consequence of the data processing.

Secondly, the victim status should go beyond the potential inclusion in specific groups. As shown in the field of surveillance studies, monitoring efforts are no longer directed at specific population targets, but may concern anyone in society. Also, data collection does not necessarily impact on the individuals to whom the data refer to, and algorithmic profiling is highly dynamic.

It is evident that the "victim status" is particularly volatile nowadays, and thus should probably be downsized in importance by the Court. It is true that such proposition entails a significant departure from the initial architecture of the ECHR system, but the Court has already shown in its case law that there is room for such extensive interpretations.

In data protection, effective litigation in surveillance matters directly depends on the national implementation of EU norms. All Member States should rely on the possibility afforded in Art. 80(2) GDPR. As individuals targeted by algorithmic monitoring are not always identifiable, the role of organisations lacking data subjects' mandates should be enhanced.

As for the LED, an enhanced system of protection for security-related operations in smart cities could be achieved by implementing a similar remedy to Art. 80(2) GDPR. While Art. 55 LED does not provide for such possibility, this does not prevent Member States from granting a higher level of protection[1528]. In this way, traditional class action mechanisms foreseen in Art. 80(1) GDPR could be coupled with public interest litigation tools where a prior data subjects' mandate is not required. In smart cities, this would allow citizens and civil society organisations to challenge initiatives involving facial recognition and predictive policing initiatives that rely on personal data processing.

Lastly, practical barriers should also be considered. As civil society organisations are usually underbudgeted, funding opportunities for public interest litigation could be established. This solution is not unprecedented at the EU level and could be further implemented at the national/local level[1529]. As mass algorithmic surveillance is liable to introduce new power asymmetries, the provision of these funds could compensate the disadvantaged position in which citizens are placed as a result of being monitored in the urban sphere.

4. Interim conclusions

Surveillance as a continuum. This chapter sketched different conceptualisations of surveillance which could be useful for framing monitoring phenomena in smart cities. Drawing on the latest case law on surveillance by the ECtHR and the CJEU, surveillance has been characterised as a *continuum*, ranging from purely "mass" surveillance to "mass/hybrid" surveillance, "hybrid/targeted" surveillance, and traditional "targeted" surveillance. The proposed classification is meant to (at least partially) remedy the lack of clear definitions that are usually employed by the European Courts, and thus lay down the basis for more precise proportionality assessments.

Many scholars still doubt the compatibility of (quasi-)mass surveillance systems with the principle of proportionality in relation to the rights to privacy and data protection. In light of the pervasiveness of data collection in the *onlife* world, however, the two European Courts seem to be more tolerant towards unfettered regimes, as they have shifted the focus of proportionality from the moment of the *collection* to that of the *selection* of the relevant information.

[1528] Cf. Recital 15 LED.

[1529] van der Sloot et al (2021b), p. 329. See European Commission (2019); Digital Freedom Fund (2022).

Nonetheless, conflicting definitions of general interest goals in this jurisprudence still raise practical issues in smart cities. The protection of critical infrastructure and services could well fall within the purview of both *national* and *public* security. The same could go for surveillance pursuing the economic and environmental wellbeing, two objectives that are at times included in the concept of national security.

In smart cities, large data retention operations should undergo a prior validation of an independent authority (preferably of a jurisdictional nature in the security domain) assessing the *factual* need for surveillance at the city scale or in specific zones of the city itself. The competent authority should give concrete meaning to the legitimacy goal pursued by the measure and classify its weight in the proportionality assessment (national security/public security/environmental and economic wellbeing). The right surveillance framework (i.e., mass, hybrid/mass, targeted/hybrid, targeted) should then be chosen accordingly.

Lastly, power asymmetries in urban surveillance should be addressed by enhancing public litigation and class actions as legal remedies against individual and collective harms of surveillance. However, gaps have been identified in both the Convention and EU law. These systems do not seem to be fully equipped to address the individual and collective dangers of surveillance in smart cities. Practical obstacles (e.g., lack of funding and lengthy procedures) are also undermining the efficacy of such remedies. This shows that, despite its fundamental importance, legal analysis alone cannot counter the risks of mass surveillance in smart cities.

V. Surveillance Technologies and Practices

1. Introduction

The previous chapter dealt with general frameworks that may help to assess the overall justifiability of surveillance initiatives in smart cities. This chapter will focus on specific monitoring technologies implemented in the urban context. Specifically, the sub-research question addressed is: *Which IoT surveillance technologies in smart cities can affect individuals' rights to privacy and data protection and how should these be proportionally implemented?*

Four kinds of surveillance technologies and practices will be examined: facial recognition[1530], drones[1531], the use of environmental data[1532] and nudging[1533], the analysis of which does not pretend to be exhaustive. Nevertheless, the aim is to exemplify privacy and data protection issues stemming from the use of these and similar applications.

Relevant technologies have been selected by taking into account the interest sparked by these in public discourse and academia. Technical and normative criteria have also been considered. On the technical side, the scope was circumscribed to technologies that rely on sensors (including cameras) and are equipped with profiling software[1534] and systems of data centralisation and analysis, which is typical of IoT architecture[1535]. Therefore, for instance, traditional CCTV cameras were excluded, as they are not equipped with automated recognition capabilities. From the normative perspective, surveillance technologies were examined in contexts that could stress both their worrisome and positive implications.

In line with the methodology developed in the previous chapters, proportionality assessments will be the framework to analyse these technology applications. The assessments will not always target concrete marketed technologies but rather draw inputs from practical instances of implementation to provide the proposed arguments with a factual evidence basis.

2. Facial recognition technologies

Outline. This section will provide an overview of different iterations of facial recognition technologies. Subsequently, the risks that such technologies pose from a surveillance and fundamental rights perspective will be outlined. Lastly, two use cases will be reviewed, one related to the Clearview AI app, and the other to EFR.

2.1. Overview of the technology

Definition and applications. Facial recognition was defined by the Article 29 Working Party as the "automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorisation of those individuals"[1536].

The technology relies on several distinct sub-processes[1537]. Firstly, a two-dimensional image of a face is collected by a camera; then, a face is detected by the software within the picture. An image

[1530] See §2.
[1531] See §3.
[1532] See §4.
[1533] See §5.
[1534] See definition provided at Recital 71 GDPR.
[1535] For a description of the IoT, see Introductory Chapter, §3.2.4.
[1536] Article 29 WP (2012), p. 1.
[1537] As described in Article 29 WP (2012), p. 2.

normalisation step is then enacted: the algorithm tries to smooth variations across detected facial regions, e.g., converting to a standard size, rotating or aligning colour distributions[1538]. Indeed, faces within the focus of a surveillance camera might be captured in a wide range of lighting conditions and from different viewpoints, making it harder to recognise them with respect to standard passport photos, or mugshots (i.e., so-called controlled environments)[1539]. To perform this task, the algorithm needs to be trained on millions of photos to isolate face "landmarks" (repeatable features), like eyes, nose and mouth[1540]. A process of feature extraction follows, as the software isolates this information into a compact file, ranging from less than 100 bytes to a few kilobytes in size[1541]. A biometric template of the target's face is thus generated[1542].

Types of facial recognition systems. Once the biometric template is obtained, the facial recognition system may process it for three different purposes: (i) verification/authentication; (ii) identification; (iii) classification/categorisation[1543]:

(i) *Verification* systems (i.e., one-to-one comparison) are designed to confirm that the acquired faceprint matches with the one stored in the database. To this end, the system does not need to associate an identity with the person concerned, it just verifies that the facial features of the image captured by the camera correspond to those collected in the database, thus unlocking access to devices (e.g., smartphones), services (e.g., online banking), or premises.

(ii) *Identification* systems (i.e., one-to-many comparison) are built to check the detected facial image against a database of multiple templates, in order to uncover the identity of the targeted person. This is the classic use of the technology made by law enforcement agencies, which may look for specific individuals (suspects of crime, warranted people, victims) in public spaces.

In both cases facial recognition works thanks to an "an estimated match between templates: the one being compared and the baseline(s)"[1544]. Therefore, this means that verification and identification are *probabilistic*: A higher or lower probability that the targeted person is indeed the person whose template is stored in the database is deduced from the comparison.

(iii) *Classification* systems are employed to infer human defined characteristics from one person's facial features[1545]. This can be the case of software trained to assess people's gender or age, as well as emotional states[1546]. While these systems do not necessarily presuppose the identification of the targeted individual, they may *de facto* lead to this outcome, especially if the processing is coupled with identification capabilities or if it is linked with other data[1547].

2.2. Surveillance and fundamental rights risks

Data protection. Privacy, data protection and surveillance risks associated with deploying facial recognition technologies have been sparking a heated debate in academia, policy-making and public discourse[1548]. From a data protection standpoint, it is safe to say that operations carried out by facial

[1538] Id.
[1539] Castelvecchi (2020), p. 348.
[1540] Id.
[1541] Id.
[1542] Kindt (2013, p. 44) defines a biometric template as the "'reference biometric feature set' which will be stored and then used for later comparisons".
[1543] European Union Agency for Fundamental Rights (2019), pp. 7-8; EDPB (2022), p. 7.
[1544] EDPB (2022), p. 7.
[1545] Castelvecchi (2020), p. 349. On the issues raised by classificatory applications of facial recognition, see below §2.3.2.
[1546] European Union Agency for Fundamental Rights (2019), p. 8.
[1547] Id.
[1548] See O'Flaherty (2020); Lotte (2020); Access Now (2022).

recognition software entail the processing of biometric data, which as "special categories of personal data" are subject to a stricter lawfulness regime both under the GDPR (Art. 9) and the LED (Art. 10)[1549]. There are several data protection issues raised by facial recognition. Despite the advancements brought by deep learning technologies, facial recognition is still quite prone to errors, which places the general principles of fairness and accuracy of the processing under stress[1550].

Statistical inaccuracy may also be rooted in the selection of the source data used as a training set which may be subject to bias[1551]. Discriminatory implications of facial recognition tools may also stem from the intentional use of these systems made by public authorities, which may leverage it to monitor religious and ethnic minorities, or other marginalised and oppressed communities[1552].

Moreover, the use of biometric technologies can heighten data security risks. Because biometrics uniquely identify citizens potentially throughout all their lives, the loss of such data is likely to produce irremediable consequences for data subjects. Facial recognition software is also based on brittle algorithms which can be fooled quite easily, being liable to evasion attacks, poisoning attacks and deep fakes[1553].

Lastly, it is important to consider that public authorities often deploy facial recognition technologies through cooperation with private technology vendors; similarly, the face images used may have been initially stored by private communication providers (e.g., social media platforms). This may pose a problem of function creep, as data collected in the private sector domain is liable to be repurposed in non-related fields like law enforcement[1554].

Privacy and surveillance. These issues obviously intersect with the right to private life. Because collecting facial biometric templates allows for the "permanent" unique identification of the data subject[1555], deploying facial recognition can lead to the loss of anonymity in public spaces[1556]. This can also lead to a chilling effect[1557], undermining the full exercise of the freedom of expression and association, which are closely linked to the right to privacy itself. Particularly worrisome are the possible uses of facial recognition software during political or dissenting demonstrations, leading to the criminalisation of protesters[1558]. When employed by law enforcement, especially in preventive operations, facial recognition may also cause an overturning of the presumption of innocence, as anybody can be "scanned" even if they have no link whatsoever with criminal activities and networks[1559].

Of course, this raises a proportionality problem. At the present time, an all-encompassing framework on facial recognition is still missing in the EU, which poses stronger risks in terms of disproportionate implementations of these systems[1560]. This may regard law enforcement contexts, for which there are often no rules governing the inclusion of someone's image in a watchlist, or the actual deployment of *live* facial recognition in uncontrolled environments, or *ex post* application to pre-

[1549] Article 29 Working Party (2012), p. 4; EDPB (2022), p. 8.
[1550] European Union Agency for Fundamental Rights (2019), p. 9.
[1551] Lohr (2018).
[1552] On the Uighur minority in China, see Reuters (2020).
[1553] See Heaven (2019).
[1554] See below §2.3.1
[1555] See Bacchi (2021); Chandran (2019).
[1556] EDPB (2022), pp. 45-46; European Union Agency for Fundamental Rights (2019), p. 29.
[1557] European Union Agency for Fundamental Rights (2019), p. 30; O'Flaherty (2020), p. 171. *Compare* ICO (2019), p. 61.
[1558] Access Now (2021), p. 1.
[1559] See below §2.3.2.1.3.
[1560] Pending the adoption of the AI Regulation at the EU level, there is also a risk of fragmentation between Member States, cf. the Italian situation after the Law no. 205/2021, as described by Della Torre (2022).

registered camera footage. The activities of private sector actors, who may leverage facial recognition in publicly accessible places, is also unregulated. For instance, in Spain a notorious chain of supermarkets has been using such systems to detect people in their premises, and have been fined by the national DPA because of it[1561].

2.3. Illustrations

Against this background, the issues raised by facial recognition in urban environments will be analysed in two distinct applications: Clearview AI[1562] and EFR in public places[1563]. In both cases, proportionality assessments will be employed to ascertain the legitimacy of these use cases.

2.3.1. Clearview AI

Introduction. At the beginning of 2020, a New York Times report[1564] put a once little-known start-up, Clearview AI, under the spotlight. According to the report, this mysterious tech company had admitted selling a new facial recognition app to over 600 law enforcement agencies across the United States. Nothing new, one could argue: police have been using facial recognition for a while now. However, the Clearview app goes far beyond traditional facial recognition tools. If these have been historically limited to matching government-stored images (i.e., mugshots, driver's licence photos), Clearview now combines its technology with a database of three billion images published on the Internet. Clearview's engineers have designed a software that can automatically collect people's photos from a variety of websites ranging from employment to news and education, as well as targeting social networks like Facebook, YouTube, Twitter, Instagram and LinkedIn. This practice, going under the name of data scraping, is undoubtedly controversial from a privacy standpoint. Unsurprisingly, the "Clearview case" has prompted an outbreak of worldwide criticism from human rights advocates[1565]. Social network companies, such as Twitter and YouTube have also sent cease-and-desist letters demanding that Clearview stops data scraping from their websites.

On the other hand, Hoan Ton-That - Clearview's founder and CEO - has defended the lawfulness of the company data processing practices, as well as the accuracy of its facial recognition technology. He further highlighted that the Clearview app has been crucial in solving a number of cases involving shoplifting, identity theft, credit card fraud, murder, terrorism and child exploitation[1566]. From a general perspective, the Clearview case clearly falls within the global trend of re-use of data collected by the private sector for law enforcement purposes[1567]. Several transparency reports are now showing that law enforcement agencies are increasingly asking to access data stored by tech giants such as Facebook, Google, Microsoft. In many instances, government agencies have even begun purchasing personal data from private companies to circumvent legal safeguards surrounding law enforcement access to commercial databases (i.e., subpoenas or judicial warrants)[1568]. However, the Clearview case differs from other scenarios involving the disclosure of personal data from the private sector to law enforcement: personal data is not transferred to police forces on a case-by-case basis, against payment or pursuant to a legal obligation, but it is collected by a private company with the precise intention of

[1561] El País (2021).
[1562] See §2.3.1.
[1563] See §2.3.2.
[1564] Hill (2020).
[1565] Reich (2020).
[1566] Tarantola (2020).
[1567] See Ferguson AG (2017a); Mitsilegas (2015).
[1568] Brayne(2017), p. 995.

making it available, through an institutional arrangement, to government agencies for policing purposes.

The need for an EU law- based assessment. As Clearview AI (Clearview) also plans to sell its technology to European law enforcement agencies[1569], there emerges a pressing need to assess the impact that this disruptive facial recognition tool may have on individuals' rights in criminal proceedings. Different EU Member States are indeed starting to test or rely on real-time facial recognition systems, giving rise to several societal concerns, as acknowledged by some EU institutions[1570]. The need for a careful legal analysis of these issues also arises from the complexity of the EU data protection framework, comprising both the GDPR and the LED.

Since 2020, European data protection authorities have taken a stance with regard to Clearview's practices. The company has been indeed hit with multiple fines and orders due to their violation of EU data protection laws. In January 2021, the Hamburg data protection authority opened administrative proceedings against Clearview after a German citizen requested the deletion of his image from their database[1571]. Fines and orders from other national data protection authorities have followed, including France[1572], Italy[1573] and the United Kingdom[1574].

Against this background, it will be examined whether the use of the Clearview app in criminal investigations is compliant with the EU privacy and data protection framework. Firstly, the lawfulness of Clearview's data scraping practices under the GDPR will be assessed. Secondly, the use of scraped data by EU law enforcement agencies under the regime of the Directive will be discussed. In particular, this analysis will revolve around the role that Clearview would acquire, pursuant to the Directive, in data processing within the framework of partnership agreements concluded with law enforcement agencies across the Union. Finally, it will be assessed whether the Clearview app abides by the criteria set out in Article 10 of the LED on lawful processing of biometric data. In this last step, the focus will be on the strict necessity test, as defined by the CFREU and the ECHR.

2.3.1.1. Clearview's data scraping activities under the GDPR

What scraping means. Generally speaking, data scraping is a broad expression describing "a plethora of internet-based data-retrieval methodologies from vast and various sources, collected *without* the website owner's consent"[1575]. Unfortunately, the privacy and data protection issues raised by data scraping activities do not seem to have been analysed in detail in literature. In this specific case, the assessment of these particular data-processing operations requires us to answer a preliminary question, aimed at identifying the applicable EU legal instrument. As already pointed out, the EU data protection framework is composed of two distinct instruments: a general one, and one focused on data processing performed by law enforcement authorities for the purpose of tackling crime. Determining the applicable instrument in this case is not a trivial question, if we look at the *material* and *territorial* scope of the two regimes.

[1569] See Stolton (2020).
[1570] European Commission (2020) White Paper on Artificial Intelligence, p. 22; European Union Agency for Fundamental Rights (2019), pp. 17-18.
[1571] The Hamburg Commissioner for Data Protection and Freedom of Information (Hmb BfDI) (2021) Clearview AI Inc.
[1572] CNIL, 1 November 2021, *Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI.*
[1573] Garante della Privacy, 10 February 2022, *Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362].*
[1574] ICO, 18 May 2022, *Clearview AI Inc. Enforcement Notice.*
[1575] Campbell (2019), p. 3.

On the applicability of the GDPR or the Directive. When dealing with the material scope of the two frameworks, we first need to assess whether Clearview collects people's publicly available images to satisfy a purely economic interest, or to perform a law enforcement operation entrusted by the competent authorities. Only in the latter case in fact, data scraping activities would be excluded from the scope of the GDPR, pursuant to Article 2(2)(d)[1576], thereby falling within the scope of the Directive. At this initial stage, it is safe to argue that the company itself does not engage in preventive or investigative activities *on behalf* of any public authorities operating in the law enforcement context[1577]. This assertion is reinforced when read in conjunction with Clearview's privacy policy[1578]. In fact, in stating the purposes of its data processing activities, Clearview indicates that it

> collects publicly available images and *shares* them, along with the source of the image, in a searchable format with our users, who are all law enforcement, security and anti-human trafficking professionals in the United States. This enables *users* to: facilitate law enforcement investigations of crimes; investigate and prevent fraud and identity theft [emphasis added].

From the wording of the privacy policy, it is clear that Clearview's practices are primarily motivated by an economic interest, meaning that the company collects data to commercially exploit their value and provide its services to law enforcement agencies. Certainly, data collection is exclusively aimed at tackling crime in the law enforcement sector; however, Clearview does not act here as a competent authority within the meaning of the Directive. Data collection is first motivated by Clearview's interest in sharing – a more appropriate label would be *selling* – gathered data with its *users* (i.e., police agencies), those who are directly involved in the investigation of criminal offences. Therefore, although data collection is performed *to the benefit* of law enforcement, it is not done in the exercise of a delegated public power, as required by Article 3(7)(b) of the Directive[1579]. Taking all of this into account, it can be concluded that Clearview's data scraping practices are performed to benefit law enforcement, whilst primarily serving the company's commercial objectives. Consequently, they fall within the material scope of the GDPR[1580], whilst the Directive (and national legislation implementing it) cannot be considered applicable at this stage.

The territorial scope of the GDPR. Shifting the analysis to the territorial scope of the GDPR, different scenarios shall be taken into consideration. Firstly, the applicability of the Regulation needs to be assessed through the lens of the "establishment's" criterion, set out in Article 3(1) GDPR[1581]. Pursuant to this provision, the Regulation applies to personal data processing in the context of an establishment of a controller or processor in the Union, regardless of where the processing takes place. If Clearview were to offer its services to law enforcement agencies in EU Member States, Clearview would most likely establish itself in at least one EU Member State to better oversee its marketing operations in

---

[1576] Art. 2(2)(d) GDPR is complemented by Art. 1(1) of the Directive, which limits the scope of the Directive to personal data processing performed by law enforcement authorities for the purposes of preventing, investigating, detecting, prosecuting criminal offences and executing criminal penalties. Still, the Regulation does not exclude from its scope all data processing for law enforcement purposes, which are explicitly mentioned at Art. 23 GDPR. Hence, data transfers from private parties not acting as competent authorities to law enforcement agencies generally fall within the scope of the Regulation.

[1577] For the opposite scenario, where private citizens take part in law enforcement activities through a police-designed app, see Milaj et al (2020).

[1578] Clearview AI (2020) Privacy Policy.

[1579] Purtova (2018b), p. 64.

[1580] Id., p. 63.

[1581] The notion of establishment is provided in Recital 22 GDPR. It should be noted that the EDPB (2018, pp. 4-12) clarified that the threshold for the identification of a 'stable arrangement' can be quite low when the controller's centre of activities concerns the provision of online services. Before the GDPR, the criterion was interpreted extensively in CJEU, *Google Spain,* §§50–53.

Europe. Here, the presence of a single employee or agent of Clearview might be enough to trigger application of the GDPR, if the company's representative(s) acted with sufficient stability[1582]. The EU local establishment would not be required to take any role in the data processing, insofar as its activities could be considered as being "inextricably linked" to such processing.

Secondly, even if Clearview decides not to set up an EU office, its processing operations could still fall within the scope of the Regulation, according to the so-called "targeting" criterion. If their data processing activities were related to the monitoring of data subjects in the Union, the GDPR would apply as far as the targeted behaviour also takes place within the Union (Art. 3(2)(b) GDPR)[1583]. The meaning of this provision is further clarified in Recital 24 of the Regulation, which reads: "in order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including *potential subsequent* use of personal data processing techniques which consist of *profiling* a natural person, particularly in order to *take decisions* concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes [emphasis added]". Although the use of the Clearview app is mainly directed at the *identification* of individuals involved in criminal investigations taking place in EU Member States, its processing activities may also involve *tracking* individuals who are in the Union. First, the images retrieved by the AI system are presented with their sources, i.e., a link redirecting the user to the website storing the data. Of course, this also allows law enforcement – at a later stage – to track the online behaviour of people subject to monitoring, thus profiling them with the aim of detecting their preferences and habits, but also their location and movements[1584]. Moreover, as images are mainly scraped in social media, they can also assist investigators in reconstructing a detailed picture of one's own personal life. Indeed, social media pictures come with a great deal of contextual elements (e.g., background, company, location) from which sensitive information on the data subject can be inferred. Metadata associated with the pictures can also play a role in ascertaining the potential location of individuals. Therefore, it is possible to conclude that Clearview may engage in processing activities related to the monitoring of data subjects in the Union within the meaning of Article 3(2)(b) GDPR; the Regulation would thus apply to its data scraping operations, even if they did not take place in the Union.

2.3.1.2. Assessing sensitive data scraping under Article 9 GDPR

Lawfulness of the processing under GDPR rules. Having established the (potential) applicability of the GDPR, the lawfulness of data scraping practices under the EU data protection regime shall be assessed. As the processing operations mainly concern a special category of personal data, the analysis will revolve around the stricter requirements laid down in Article 9 GDPR[1585]. In its privacy policy, Clearview explicitly states that their collection of facial images is grounded on their public availability on the Internet. Such operations may seem to be compliant with Article 9 GDPR, which allows data controllers to process special categories of data "which are manifestly made public by the data subject". Actually, the issue may be more complex than it first appears. Indeed, the meaning of the expression

[1582] See EDPS (2017a), p. 5.
[1583] See Greze (2019), pp. 110-114.
[1584] See Recital 71 GDPR.
[1585] See Recital 51 GDPR. At this stage, it might not be clear whether facial images – if being merely stored in Clearview's databases – could qualify as biometric data. To be considered biometrics, the image should be processed by an algorithm transforming the analogue information into digital information (data) based on the person's facial features. However, such images could still be treated as a special category of personal data, revealing the ethnic origin of a natural person, or potentially his/her religious beliefs etc.

"publicly available" has not been fully clarified in the Regulation, nor in literature[1586]. Still, some considerations may be put forward when assessing the Clearview app. In this case, the analysis will exclusively focus on social media websites, as they represent the main source of data for the system's search engine.

When private companies scrape data from social media, they still need to comply with the policies of the targeted websites. To understand whether a site allows for web-scraping, its robots.txt file must be checked first. The file can be accessed by adding "/robots.txt" right at the end of the link of the concerned website[1587]. As we perform this rather simple procedure, we observe that most social media websites do not allow for data scraping, unless written permission is issued. Unsurprisingly, all major social media platforms have already sent cease-and-decease letters to Clearview, demanding that they stop all data scraping activities in their domains[1588].

Furthermore, data scrapers need to also respect individuals' privacy settings. Social media websites usually give users the option to choose with whom they want to share the details of their daily lives. Therefore, a picture cannot be considered as being "publicly available" only because it was posted on social media[1589]. For instance, when a picture is published on a private profile, the data cannot be freely collected by the scraping company. In this case, the user did not intend to make her personal information available to the general public, and even less so to law enforcement. Nevertheless, such considerations seem not to inform the current functioning of the system. For example, during an extended interview with Clearview's CEO, a CNN journalist ran his producer's picture into the app, which found images from her Instagram profile, even though that account was private and accessible only to her followers[1590].

In the same interview, Hoan Ton-That reported a case in which the face of a child predator had been detected by the Clearview app in the background of a gym selfie posted by a third person on his social media. This case brings our attention to another scenario, which questions the "public availability" of the images stored in the company's databases. In some instances, the pictures may not have been made public by the interested data subject; they may also have been taken in contexts where the portrayed individual could have claimed to have a reasonable expectation of privacy. In all these cases the legal basis set out in Article 9(2)(e) GDPR cannot be seen as fulfilled, and data scraping operations should be considered unlawful.

Having examined how initial data scraping activities may violate the GDPR provisions, the scope of the Directive's application will now be analysed, which would regulate data sharing operations within the framework of partnership agreements between Clearview and EU law enforcement agencies.

2.3.1.3. Subsequent use of GDPR data in private-public partnerships

A grey area between the GDPR and the Directive. The relationship between the GDPR and the Directive undoubtedly sits in the penumbra of EU data protection law. Even though certain provisions attempt to regulate the interrelationship between the two regimes, a significant degree of uncertainty still persists in the context of information sharing between private parties and law enforcement authorities[1591].

[1586] Kindt (2018), p. 528.
[1587] Octoparse (2019).
[1588] In response, Clearview invoked its First Amendment right to scrape publicly available data, see Fan (2020).
[1589] Conversely, Article 29 WP (2017b, p. 10) pointed out that when the concerned person posts images on other kinds of publicly available websites, he or she is clearly willing to make the information available to the general public, and thus potentially to law enforcement.
[1590] O' Sullivan (2020).
[1591] Purtova (2018b), p. 62.

Whereas private-to-public data transfers performed on a case-by-case basis are still subject to GDPR rules, the same cannot be said for information sharing schemes taking place in the framework of *structured* institutional arrangements between concerned parties[1592]. Depending on the configuration of the agreement between private and public entities, two different scenarios need to be examined. On the one hand, Recital 11 of the Directive clarifies that when private entities or bodies are bound "by a contract or other legal act" to law enforcement agencies, they process data *on behalf* of competent authorities and become *processors* under the Directive[1593]. In this case, GDPR applies to initial data collection activities – as we have argued – and the Directive regulates data processing within the context of the PPPs concluded by the company.

On the other hand, when the private and public parties determine the objectives of the processing *as equals*, Purtova contends that a situation of joint controllership is established[1594]. In this case, the private entity fully acquires the status of "competent authority" within the meaning of Article 3(8) of the Directive, which could then also extend its applicability to previous data collection activities[1595].

In summary, the actual scope of the Directive ought to be assessed on a case-by-case basis, depending on the exact terms of the partnership agreement that could involve Clearview and the law enforcement agency concerned. The key determinant lies in the weight given to the company in setting the goals, limits and means of the processing within the PPP. Although, precise predictions are difficult to make, some hypothesis on the case at hand could still be postulated. For instance, to qualify as a joint controller, Clearview should have actual power regarding *when* and *under which circumstances* processing activities are carried out in the context of real criminal investigations or pre-emptive operations. This means that the company should also be able to perform both the necessity and proportionality assessments, as any other law enforcement authority in real-time situations[1596]. Setting aside the considerable legitimacy issues that such scenarios would give rise to, we suggest here that the current configuration of legal agreements concluded by Clearview in the US could rule out a situation of joint controllership in the European Union. From the available US reports, it appears that Clearview is acting as a simple provider of a facial recognition service to competent authorities. Thus, police officers are the ones, who decide when to run a picture in the system in concrete cases. Conversely, there is no evidence in the news of Clearview refusing to match an uploaded image with those stored in its databases.

It appears that Clearview would become a processor under the Directive when providing its services to police departments under a stable partnership agreement. Although a situation of joint controllership cannot be completely ruled out, such a scenario would certainly be the least desirable from a democratic perspective.

2.3.1.4. Assessing Clearview under Article 10 LED

Legal requirements under the LED. Interestingly, facial images *per se* do not constitute biometric data under the EU data protection legislation[1597]. According to Article 3(13) of the Directive, data is considered to be biometric only if: (a) it results from *specific technical processing*, meaning that the mere storage of such data does not necessarily require the application of the specific regime; (b) it allows for

[1592] Purtova (2018b) p. 65.
[1593] Recital 11 LED.
[1594] Art. 26 GDPR; Art. 21 LED.
[1595] Purtova (2018), p. 66.
[1596] Id, p. 65.
[1597] See Kindt (2018), pp. 529-534. It should be noted, nonetheless, that facial images *per se* are covered by the protection of Article 8 ECHR, see e.g., ECtHR, *von Hannover v. Germany,* §§76-78; ECtHR, *Peck v. the United Kingdom,* §§60-62; ECHtR, *Bogomolova v Russia*, judgment of 20 June 2017, App no 13812/09, §52.

the *unique identification* of a natural person. Thus, the initial data can hardly be considered biometric in itself; it is rather the use of specific means of processing to submit the data to this particular regime.

Pursuant to this legal definition, it is contended here that the processing of facial images by Clearview – and potentially by criminal justice authorities of EU Member States – must be qualified as biometric data, and therefore subject to the particular safeguards of Article 10 of the Directive. As in our case, facial images are processed in the context of a criminal investigation, the biometric processing is clearly aimed at the identification of a precise individual. It is well-known that identification *per se* represents an unavoidable pre-condition of many (if not all) law enforcement activities. Here, Clearview's processing concretely allows for such identification, as it matches facial images with social media profiles and websites that may easily lead to the identity of data subjects. Besides, facial images are collected here not for mere storage purposes; they are also processed for biometric comparison by an AI system, and can therefore be considered as the result of specific technical processing. Having qualified the data processed by the Clearview app as biometric, it will be assessed whether – or under which circumstances – the use of such tool may be compliant with the requirements set out in Article 10 LED.

Lawfulness of the processing. Article 10 of the Directive allows for the processing of biometric data only: (a) when authorised by European Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; (c) where such processing relates to data which are manifestly made public by the data subject. As for the first condition, the deployment of the Clearview app could be grounded either on EU or national legislation, specifically regulating the processing of biometric data for real-time identification purposes in the criminal justice sector. In particular, if biometric processing is based on Member State law, it should be allowed only when essential to protect the vital interests of the data subject or another natural person, or when the data has manifestly been made public by the data subject[1598]. If the second scenario has already been examined in the context of the present contribution[1599], the former may refer to situations where there is an immediate danger for the life and personal integrity of individuals (e.g., to prevent a terrorist attack), or a need to protect the vital interests of victims of serious criminal offences (e.g., in the case of human trafficking, child pornography).

Strict necessity test. Article 10 of the Directive allows for the processing of biometric data only when it is strictly necessary. For the purposes of this assessment, the strict necessity test – being an aspect of the broader principle of proportionality – should be interpreted in accordance with Article 52(1) of the Charter, which is applicable within the scope of EU law. As we are dealing with an encroachment on the rights to privacy and data protection, we shall also refer to Article 8(2) of the ECHR, which adds that any limitation to the rights at stake must be strictly necessary "in a democratic society". Even if the Charter uses a different wording, the *democratic society* requirement present in the ECHR is integrated into the analysis[1600]. Accordingly, the case-law of the ECtHR will be taken into account when examining the strict necessity criterion. The content of the (strict) necessity principle has been clarified by the CJEU in its *Schwarz* case:

[1598] Article 29 WP (2017b), p. 7.

[1599] All considerations made concerning the "public availability" of facial images under GDPR are valid also in the law enforcement context.

[1600] The respect of democratic values is inherent in the EU legal order and it is mentioned in Article 2 TEU. Also, Article 52(3) of the Charter provides that, when the Charter protects rights corresponding to those guaranteed by the ECHR, the meaning and scope of such rights shall be interpreted as those enshrined in the Convention.

> in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage *measures which will interfere less* with the rights recognised by Articles 7 and 8 of the Charter but will *still contribute effectively to the objectives* of the European Union rules in question.[1601]

In assessing the necessity of a limitation to the fundamental rights protected, the nature and the scope of the interference prompted by the measures taken by the authorities need to be evaluated first. In this case, different factors suggest that the interference with the rights to privacy and data protection may be particularly serious, thereby being subject to a more severe review[1602].

Firstly, creating a database of three billion facial images for policing purposes clearly amounts to the creation of a blanket surveillance scheme, which means that citizens that do not have any connection whatsoever with criminal activities are likely to be placed under screening by law enforcement. European supranational courts have highlighted the risks of unfettered surveillance, which is likely to engender a constant feeling of being monitored, stigmatised or treated as suspects with no apparent reason in the minds of the people involved[1603]. Furthermore, as biometrics allows authorities to uniquely identify citizens throughout the course of their entire lives, the indiscriminate collection of such data strongly undermines people's anonymity in public places. In turn, this may also impact on the exercise of other fundamental rights and freedoms, such as the freedom of expression, information and communication, or the freedom of assembly and association[1604]. These risks may even be magnified for some vulnerable groups: the technology is often less accurate when it comes to identifying females and darker-skinned people, as the design of facial recognition systems might still be affected by racial and gender biases. Overall, the deployment of this facial recognition tool, combined with an enormous database of privately collected images, seems to generate a significant limitation to people's rights to privacy and data protection. Hence, its use by law enforcement should be strictly regulated and monitored.

Secondly, the envisaged measure should not go beyond what is strictly necessary to fulfil the proposed objectives (here, the fight against crime). To satisfy this requirement, the assessment of the app shall focus on the existence of "clear and precise rules governing its scope and application"[1605]. Even if such rules were laid down in the European context, it can be argued that the use of the Clearview app – as it stands today – would be highly problematic in the Union. While pointing out potential issues, how the use of the app may be circumscribed in some instances will be indicated.

The main issue that comes with the adoption of the Clearview system concerns the size of its database, which contains – for the most part – images of people that have never been involved in criminal activities or with law enforcement. Since its *Digital Rights* judgment, the CJEU demands surveillance measures in the law enforcement context to be differentiated and restricted according to objective criteria presenting a link with the goals pursued[1606]. With regard to the persons whose data are being retained, the use of the Clearview app seems to be significantly at odds with the requirements of the Court, and the contrast is probably irreconcilable. As strongly reiterated by the company's CEO, the force of the app lies in its capacity to search beyond government-based databases: its use is therefore overtly aimed at identifying people that would normally be far from the gaze of criminal

---

1601 CJEU, *Schwarz v Stadt Bochum*, §46 [emphasis added].
1602 CJEU, *Digital Rights Ireland*, §§47-48; ECtHR, *S. and Marper v the United Kingdom*, §102.
1603 Cf. CJEU, *Digital Rights Ireland*, §37; ECtHR, *Big Brother Watch v. United Kingdom*, judgment of 13 September 2018, App. no. 58170/13, 62322/14 and 24960/15, §225.
1604 See Chandran (2019).
1605 CJEU, *Digital Rights Ireland*, §54; ECtHR, *Rotaru v. Romania*, §§57-59; ECtHR, *S. and Marper v the United Kingdom,* §99.
1606 CJEU, *Digital Rights Ireland*, §57; CJEU, *Maximilian Schrems* §93; CJEU, *Tele 2/Watson,* §110; CJEU, *Opinion 1/15*, §191. *Compare* ECtHR, *Big Brother Watch v. United Kingdom*, judgment of 13 September 2018, App. no. 58170/13, 62322/14 and 24960/15, §314.

justice authorities, and therefore could not be tied to the objectives of the fight against crime by any objective criterion[1607].

When applying the strict necessity test, one major question also concerns *who* is going to be able to access the data. In this case, the use of the app should be governed by clear rules circumscribing the range of people authorised to access the data in the context of criminal investigations[1608]. Due to the sensitivity of the data, access to the software should be restricted to police officers having a certain rank or level of experience. Especially when the application is employed in its version for mobile devices, patrolling officers should be properly trained to recognise the situations where the real-time identification of an (suspect) individual may be adequate and proportionate. These decisions are particularly sensitive and should be made with extreme promptness.

As suggested above, the availability of a facial recognition tool for mobile devices, such as smartphones, is particularly relevant in our assessment. For instance, an indiscriminate use of the app by patrolling officers for real-time identification purposes may not be in line with the strict necessity criterion in most cases[1609]. Indeed, in its Opinion on the application of the necessity principle in the law enforcement context, the WP29 stressed the importance of considering the precise circumstances in which the limitation of the rights at stake takes place. In particular, the unregulated deployment of data-driven investigative techniques can be questioned in situations where individuals may claim to have a certain expectation of privacy, even in public places[1610]. With the Clearview app literally in police hands, the scope of urban surveillance may expand beyond the capacity of the tools already embedded in fixed infrastructure (i.e., CCTV), and take advantage of all kinds of mobile devices equipped with a camera. With no precise regulation on the matter, such a system of blanket surveillance may easily go beyond what is strictly necessary to tackle crime in the urban area, thus infringing citizens' rights to privacy and data protection in unnecessary ways.

Furthermore, the current functioning of the Clearview system seems not to comply with EU legislation in terms of data retention periods. For instance, Article 5 of the Directive requires Member States to set appropriate time limits for the erasure of personal data or to establish a periodic review to assess the need for storing personal data. This provision is complemented by Recital 26, which emphasises that personal data should not be kept for longer than necessary for the purpose for which they are processed. The CJEU also acknowledged the need to limit data retention periods in several cases[1611], in accordance with the case-law of the ECtHR[1612]. In the case at hand, Clearview's privacy policy does not provide any indication of the data retention period of facial images stored in the company's databases. It simply states that data subjects have a right to have their data erased when the appropriate conditions are met[1613]. It is not yet clear whether the company and concerned EU law enforcement agencies will establish precise time limits for data storage in their partnership agreements. For the time being, facial images stored in Clearview's databases will supposedly be kept there for an indeterminate period of time. Interestingly, this observation seems to be corroborated by an anecdote from a CNN journalist, who, while uploading his photo in the Clearview app, found a picture of

[1607] This issue has arisen also with respect to other kinds of government-based databases that were not originally set up for law enforcement purposes, see Kindt (2018), p. 528. The same goes for law enforcement databases that store images whose source is unclear, see Sacchetto (2020), p. 10.
[1608] CJEU, *Digital Rights Ireland*, §62.
[1609] Kindt (2018, p. 528) expresses similar concerns regarding the continuous biometric comparison for identification purposes performed by smart CCTV cameras in public places.
[1610] Article 29 WP (2014e), p. 10; Borgia (2021), pp. 16 ff.
[1611] CJEU, *Digital Rights Ireland*, §§63-64; CJEU, *Opinion 1/15*, §§209-210.
[1612] ECtHR, *M.K. v France,* judgment of 18 April 2013, App. no. 19522/09, §§44-46; ECtHR, *Zakharov v Russia*, §§254-255.
[1613] Clearview AI, EU/UK/Switzerland Deletion Request Form.

himself published by an Irish local newspaper when he was 15 years-old[1614]. One could wonder what the interest of storing such old pictures could be. These may not properly reflect one's appearance anymore, and identification goals could be equally (or better) served by more recent pictures of the monitored subject. Actually, the accumulation of different (and maybe obsolete) images for the same person – associated with the relative sources – brings to surface the *tracking* purposes embedded in the system, which go beyond mere *identification* goals. In this perspective, the monitoring abilities of the system could be restrained only by defined rules that filter the images that may be stored in the databases and set precise time-limits for retention.

Lastly, one might wonder whether the goals pursued by law enforcement in the Union could be achieved by less intrusive tools, which could still prove to be genuinely effective. As clarified by the EDPS, not every measure that might be useful for certain purposes can be seen as "desirable" or strictly necessary in a democratic society[1615]. Furthermore, when the proposed measure involves the processing of sensitive data – as in this case – the threshold to be applied in the effectiveness assessment should be higher.

When thinking of the scope and intensity of urban surveillance, one could contend that the extensive use of CCTV cameras – although questionable under many ethical aspects –already plays a significant role in criminal investigations[1616]. Existing measures may thus be already satisfactory, or could be better implemented, while being less intrusive upon the rights protected. Privacy enhancing technologies are available for video-surveillance to minimise the impact on citizens' private lives (e.g., privacy masking). Alternatively, the deployment of facial recognition tools for law enforcement purposes may arguably be supported by a pressing need to fight particular forms of serious crime. In this case, however, the deployment of the technology would still need to be thoroughly circumscribed from a range of different angles. From this perspective, the systematic and unfettered use of social media pictures of people who have never been involved in criminal activities seems to put the Clearview app at irreconcilable odds with the requirements laid down by the CJEU in the field of surveillance.

Appropriate safeguards. A component of the broader proportionality test is the assessment of foreseen legal safeguards, which are key in counterbalancing the risks to fundamental rights of the envisaged surveillance measure[1617]. The Directive requires the processing of biometric data to be surrounded by "appropriate safeguards", also underlined in Recital 37: among them, there is the provision of "stricter rules on the access of staff of the competent authority", which we have already examined.

According to the WP29, legal safeguards can also consist of additional substantial or procedural requirements accompanying the use of the tool[1618]. Firstly, data processing should be restricted to the investigation and prosecution of a limited range of criminal offences. In *Digital Rights*, the CJEU examined this requirement in the context of the strict necessity test, considering that the mass data retention measure posed such a severe interference on the rights to privacy and data protection, but was limited to the fight against serious crime[1619]. This means that, if the Clearview app were to be

[1614] O' Sullivan (2020).
[1615] EDPS (2017a), p. 17.
[1616] See Ashby (2017).
[1617] EDPS (2017a), p. 5.
[1618] Article 29 WP (2017b), p. 8.
[1619] CJEU, *Digital Rights Ireland*, §60.

adopted by law enforcement agencies in Europe, its use could certainly not be extended to tackling forms of petty crime, such as pickpocketing[1620].

Secondly, from a procedural standpoint, use of the software by law enforcement should be dependent on prior review by a judicial or other independent authority, which would assess the strict necessity of the biometric processing in the concrete case[1621]. Otherwise, the app could be exploited in situations of significant urgency (e.g., to prevent an imminent danger for the vital interests of many persons), but any access should then be subject to review *a posteriori* by competent national authorities. Anyhow, the data subject should retain its right to have the outcome of the automated processing of his or her personal data reviewed by a human agent, as provided for by Article 11 of the Directive[1622].

Lastly, the implementation of the measure should be accompanied by additional data security measures[1623], ensuring the confidentiality and integrity of the collected data. In this case as well, news reports have cast doubts on the company's ability to protect its databases. In February 2020, Clearview suffered a data breach that resulted in its entire customer list being stolen[1624]; in April, hackers got access to the company's repository containing the app's source code, secret keys and credentials[1625]. Although, Clearview claims that its security standards are compliant with GDPR requirements, it will probably have to step up its game in terms of security, if it plans to market its technology in Europe.

2.3.1.5. Concluding remarks

Following our considerations, the use of the Clearview app by Member States' law enforcement agencies appears to be deeply problematic with regard to the rights to privacy and data protection, as protected in EU primary and secondary legislation.

As enshrined in Article 7 of the Charter, privacy is traditionally conceived as a tool of *opacity*[1626], granting "protection against arbitrary or disproportionate intervention by public authorities in the sphere of the private activities of any person"[1627]. In turn, the right to data protection, which is designed in Article 8(2) as a tool of *transparency*, legitimises the processing of personal data insofar as the requirements laid down by law are satisfied[1628]. Although distinct in their underlying logic, privacy and data protection share a strong conceptual link[1629] and are both key in addressing data-driven forms of surveillance. As acknowledged by the CJEU in *Digital Rights* and *Tele2/Watson*[1630], both rights are instrumental to the exercise of other fundamental rights (e.g., the freedom of expression), which enable the flourishment of our constitutional democracies, and ultimately of our personal identity. The Court has repeatedly declared that even the objective of the fight against (serious) crime cannot, in itself, justify an indiscriminate collection and use of citizens' personal data in a democratic society[1631], as could happen in the Clearview case. That is why the CJEU will need to persist in enhancing the principle of

1620 ECtHR, *Zakharov v Russia*, §244.
1621 Cf. CJEU, *Digital Rights Ireland*, §62.
1622 Cf. Art. 22 GDPR.
1623 Arts. 4(1)(f), 29 LED.
1624 Swan (2020).
1625 Whittacker (2020).
1626 De Hert et al (2006), p. 62.
1627 CJEU, *Nexans v Commission*, judgment of 14 November 2012, Case T-135/09, §40.
1628 De Hert et al (2006), p. 62.
1629 CJEU, *Volker und Markus Schecke*, §47.
1630 CJEU, *Digital Rights Ireland*, §28; CJEU, *Tele 2/Watson,* §§93, 101.
1631 CJEU, *Digital Rights Ireland*, §51; CJEU, *Tele 2/Watson,* §103.

proportionality[1632]: only this way will the asymmetries of power brought by opaque and pervasive surveillance schemes be kept under constant review.

With regard to secondary legislation, we observed that bulk data scraping practices may violate GDPR provisions, as facial images cannot always be considered to have manifestly been made public by the data subject just because they were posted on social media. The same goes for when the data processing becomes subject to the rules of the Directive, namely once the company has concluded a partnership agreement with a law enforcement agency in the Union. In this context, Clearview could acquire the status of processor pursuant to the Directive, while keeping its role as a controller under GDPR for initial data collection activities.

Even admitting the lawfulness of Clearview's data scraping initiatives in these limited instances, the subsequent use of these privately formed databases by law enforcement in the Union remains critical. Certainly, the deployment of the tool may be regulated in ways that would allow its use by police officers only in limited scenarios (e.g., for the investigation of serious criminal offences). However, the very reliance on such a large database of social media pictures, available *in bulk* to law enforcement, may be at odds with the requirements of the CJEU. The use of publicly available data of a particular data subject, which can certainly be searched for and accessed by law enforcement for investigative needs is one thing. Providing law enforcement agencies with an enormous number of immediately available facial images at once, pertaining to citizens who may never find themselves in situations that could lead to a criminal proceeding is a whole different story.

If law enforcement were provided with such a powerful and invasive tool, preventing abuses and limiting the app's use to what is strictly necessary may become a challenging undertaking for EU and national authorities. Arguably, the mere "convenience" may not be enough to legitimise a generalised system of surveillance – like the one Clearview is planning to sell us – if we wish to preserve the restraints on power that are at the core of our democratic societies.

2.3.2. Emotion facial recognition

Combining facial and emotion recognition technologies. In recent years, commercial players and law enforcement agencies are starting to couple the deployment of AFR with emotion recognition technologies[1633]. Specifically, the latter build on affective computing[1634] and AI to sense and acquire information about human emotional life[1635]. A wide range of physiological inputs – such as facial movements, vocal tone, gait, respiration, heart rate, gaze direction – can be processed by machine learning algorithms to infer people's affective inner states[1636]. When these tools are combined with facial recognition software, the system is designed to deduce the individual's emotional condition primarily from his or her facial muscle movements. Emotion facial recognition (EFR) thus falls within the category of biometric *classification* systems, as they aim to categorise individuals based on their cognitive and physiological states.

2.3.2.1. EFR in the law enforcement domain

Applications of EFR in the security domain. Nowadays, the applications of EFR are varied in the security context[1637]. In criminal proceedings, EFR is being tested to detect liars during police interrogations:

[1632] Art. 52(1) CFREU.
[1633] The following analysis has been adapted from Neroni Rezende (2022).
[1634] Affective computing comprises both "the creation of and interaction with machine systems that sense, recognise, respond to, and influence emotions". See Daily et al (2017), p. 213.
[1635] Mc Stay (2020), p. 1.
[1636] Article 19 (2021), p. 15.
[1637] On different applications beyond the security domain, see Mc Stay (2020).

often marketed as more refined descendants of polygraph machines, software like CM Cross, EmoKit, Miaodong and Sage Data rely on facial expression images, vocal tone, heart rate and similar datapoints to determine interviewees' emotions during police questionings[1638].

On the other hand, "early warning" systems are leveraged by the police in preventive activities to spot suspicious individuals in public venues. One famous example is the US Transportation Security Authority's 2003 Screening Passengers by Observation Techniques (SPOT) programme, which in the aftermath of 9/11 aimed to find terrorists by scrutinising airline passengers displaying fear or stress[1639]. In China, a research paper published by the Hubei Police Academy examines the value of facial expression to identify "dangerous people" and "high-risk groups" who do not have prior criminal records. The author of this research proposes to build a database of video images of offenders before and after they have committed crimes, in order to train an algorithm to pick up individuals involved in illicit undertakings[1640]. In this kind of situations, the claim is that offenders suffer high psychological pressure and cannot really hide their true inner states[1641].

The reasoning behind preventive EFR systems already finds application in different software, such as Alpha Hawkeye, CM Cross, Joyware and Shenzhen Anshibao, specifically designed to detect light vibrations on faces and bodies to infer mental – and especially aggressive – states[1642]. While it is evident that Chinese-based companies are heavily betting on the success of these tools, it should be highlighted that European law enforcement authorities are not immune to the charm of EFR. For instance, the Horizon 2020 EU-funded iBorderCrtl programme shortly trialled in Hungary, Latvia, and Greece is worth mentioning[1643]. With the aim of ensuring faster and more efficient border controls, AI-equipped cameras scanned travellers' faces for signs of deception while they responded to border-security agents[1644].

Outline. In light of the growing interest towards these technologies in the security context and beyond, an assessment of EFR use in public places for the purposes of law enforcement will be proposed. This analysis is very topical, considering that the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) is now undergoing the ordinary legislative procedure[1645]. That is why, before setting the terms of the investigation, an overall picture of the rules that have been put forward in this prospective piece of legislation, in relation to both AFR and emotion recognition technologies, will be presented.

2.3.2.1.1. Facial and emotion recognition technologies in the proposed EU AI Regulation

The text of the Proposal. Recital 38 of the proposed Artificial Intelligence Act (hereinafter "the Proposal") highlights the significant degree of intrusion on fundamental rights – such as privacy and data protection, effective remedy and fair trial rights – caused by the use of AI systems in the law enforcement context. Because of the power imbalance that exists between public authorities and

[1638] Article 19 (2021), p. 21.
[1639] Crawford (2021).
[1640] Article 19 (2021), p. 19.
[1641] Id.
[1642] Id.
[1643] iBorderCrtl (2016), critically assessed by Sánchez-Monedero et al (2020).
[1644] Article 19 (2021), p. 19; Gallagher et al (2019).
[1645] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final. Critically assessed by Vaele et al (2021); Papakostantinou et al (2021).

individuals that could be subject to surveillance,[1646] the Proposal classifies these systems as "high-risk" when employed in this domain, thereby submitting them to a "stricter" regime in terms of obligations impending on manufacturers. The Recital enumerates different kinds of technologies that fall within this discipline, including individual risk assessment software, lie detectors and "deep fakes" tools.

How biometric systems are regulated in the Proposal. While emotion *facial* recognition in itself is not specifically tackled in the Proposal, two of its building technologies (AFR and emotion recognition technologies) are. AFR is defined by the Proposal as "remote biometric identification system", a notion that, according to the text, should be interpreted functionally so as to refer to "an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without the prior knowledge of the AI system's user whether the person will be present and can be identified"[1647].

A distinction is made between real-time and post biometric identification, where the former identifies systems involving the use of "live" or "near-live" materials, such as CCTV footage. This kind of application is regulated in Article 5 of the Proposal, which lists (tendentially) prohibited AI practices. Using a negative formulation, the provision bans the use of AFR in publicly accessible[1648] places for law enforcement purposes, unless specific conditions apply.

While observing the principle of strict necessity, AFR can be deployed only for the following grounds: (i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or threat of a terrorist attack; (iii) the detection, investigation and prosecution of a serious criminal offence for which the European Arrest Warrant does not demand the so-called dual criminality requirement[1649].

In addition, the provision lays down further parameters inspired by a risk-based approach informing the whole Proposal that should guide users' case-by-case assessments on the opportunity of deploying live facial recognition: (a) the nature of the situation that gives rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system; (b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

Importantly, Article 5(2) of the Proposal also recalls the applicability of the proportionality principle, with specific regard to temporal, geographic and personal limitations in the use of the technology. In any case, implementation of AFR in publicly accessible places for law enforcement purposes should be subject to prior authorisation by a judicial or independent administrative authority, on the basis of a "reasoned request" including objective evidence or clear indications as to the necessity and proportionality of its deployment.

[1646] Ienca and Malgieri (2021, pp. 7-8) note that the scheme of classification of high-risk AI system seemingly revolve around three main criteria: (i) the type of AI system; (ii) its domain of application and (iii) its human target. This implies that if AI systems featuring limited risks are employed in extremely sensitive contexts and used for practices falling under the unbearable risk list they would be prohibited. This mechanism emerges clearly in the case of EFR that is labeled as low risk when employed, for instance, in the commercial context, and as high-risk when used in law enforcement or education. The Consultative Committee on the 108+ Convention (2021, p. 6) highlighted the sensitivity of the law enforcement context, also in light of the power asymmetries between public authorities and data subjects.

[1647] Recital 8 of the Proposal.

[1648] See Recital 9 of the Proposal for the notion of "publicly accessible place".

[1649] See Art. 2(2) of the Framework Decision 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision, OJ L 190, 18.7.2002, p. 1–20.

In urgent cases, use of the system may be commenced without prior authorisation and subsequent intervention of an independent authority is allowed only during or after the use. Finally, the Proposal leaves a space for national regulation on the matter by Member States, which are asked to provide for detailed national rules for the request, issuance and exercise of necessary authorisations, the criminal offences legitimising the use of the technology and the authorities that could use such systems[1650].

Furthermore, emotion recognition technologies are explicitly comprised in the scope of the Regulation under Article 1(c) of the Proposal. They are defined as an "AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data"[1651].

Differently from live AFR, (biometric) emotion recognition *per se* is not targeted by many provisions in the Proposal. Depending on the functionalities concretely embedded in the system, EFR applications may thus be subject to different layers of rules in the framework of the Regulation. The Proposal only regulates a specific instance of facial recognition technologies in the law enforcement domain, namely those that perform strict identification operations by comparing biometric inputs with templates pre-stored in dedicated watchlist databases (i.e., the so-called "one to many" comparison). Software processing facial image data may then fall within this regime only if it integrates this kind of functionality, and the same applies also to EFR systems. It is known, however, that EFR and more broadly biometric categorisation systems do not always involve identification of targeted individuals.

When these applications are often leveraged in the commercial contexts, for instance, singling out individuals is not always foreseen[1652]. On the contrary, identification becomes key to most – if not all – activities of law enforcement authorities[1653]. In EFR policing uses, one-to-many identification may not be a direct function of the software, but it is certainly an objective pursued by law enforcement agencies employing such systems, and it may be performed "manually" at a subsequent moment. That is, identification may be carried out first-hand by human police officers having stopped the individual targeted by the software. In this latter case, EFR would not strictly fall within the scope of the rules laid down in Article 5 of the Regulation. Nonetheless, as will be argued later on, where identification objectives are still pursued, it would be appropriate to apply this regime.

Emotion recognition is lastly mentioned in Article 52 of the Proposal, which foresees transparency obligations for certain AI systems. Because of the specific nature of law enforcement activities, when emotion recognition tools are available for the public to report a criminal offence, the provision excludes that technology providers should design the systems in such a way that individuals are aware of their interaction with the artificial agent[1654].

In conclusion, it is noteworthy to mention that Article 2(4) of the Proposal foresees a significant limitation to the scope of the Regulation in specific law enforcement scenarios. In derogation to the rules laid down in Article 2(1)(c) of the Proposal, Article 2(4) exempts public authorities in a third country or international organisations from complying with the standards set out in the Regulation, provided that these entities use AI systems in the framework of international agreements for law

[1650] Cf. Art. 10 LED.

[1651] Art. 3(34) of the Proposal.

[1652] In this case emotion facial recognition technologies are also referred to as "soft biometrics". See McStay (2020), p. 4. Examples of this kind of applications involve EFR embedded in billboards and shopping malls cameras to register people's emotional reactions to adverts displayed in public venues.

[1653] Kotsoglou et al (2020), p. 87; Neroni Rezende (2020), pp. 382-383.

[1654] Art 52(1) of the Proposal. Under Art. 52(2), this applies also to biometric classification.

enforcement and judicial cooperation with the Union or more Member States. Regrettably, this provision seems to ignore the hierarchy of the sources of the law within the EU system[1655]. While international agreements concluded by the Union must respect EU Treaties but not secondary law, those autonomously concluded by Member States are entirely subject to the principle of the primacy of EU law. Hence, how could a Regulation exempt public authorities from respecting European human rights standards (enshrined in EU primary law) in extraterritorial operations carried out in the framework of international agreements to which the Union is not a party? A reversal of the hierarchy of EU legal sources appears to be in place here, and this dangerously creates a hole in the application of human rights safeguards in extraterritorial scenarios.

2.3.2.1.2. Room for emotion facial recognition in Europe?

The terms of the analysis. Given that the use of EFR technologies is increasing worldwide, and instances of its application have also been witnessed in Europe,[1656] a legal assessment of the technology against the European human rights framework comprising both the CFREU and the ECHR, seems appropriate[1657]. The analysis will be articulated in two steps. First, the question of whether EFR can at all be deemed compatible with the CFREU and the ECHR will be addressed.

Primarily, the conditions set out by Article 52(1) CFREU to justify the interferences on CFREU rights will be examined, with a focus on the "essence of the right" criterion. Then, the proportionality principle will be applied to establish whether, regardless of the outcome of the first evaluation, EFR can be considered compliant with the other requirements of Article 52 CFREU.

This analysis will mainly take preventive activities of law enforcement in public urban spaces as a reference setting. As suggested, normative benchmarks for this assessment will leverage the rights to privacy and data protection, given the strict inapplicability of other fair trial rights in the preventive phase.[1658] This choice presents several advantages. Firstly, both rights apply to data-driven preventive activities of security agencies by explicit legislative provision, i.e., Article 1(1) of the Directive 2016/680/EU (the Police Directive)[1659]. Secondly, privacy and data protection present strong conceptual links with other fundamental rights even in the criminal context, as the former are often framed as instrumental rights[1660]. This is true, for instance, with regard to the freedom of thought that, as we will see, is also called into question by emotion recognition technologies.

Indeed, the freedom of thought and the right to privacy seem to revolve specifically around the protection of *thoughts* when it comes to preserving the inner self of the individual. Certainly, the association of these entitlements to mere (involuntary) emotions may not seem totally fitting. As a premise for the assessment, however, it can be argued that emotions actually akin to thoughts. The link between emotions and thoughts has indeed been explored from both the philosophical and cognitive perspective[1661]. Given their similarities, it is reasonable to assess the impact of EFR against the abovementioned rights, whose span of protection should equally cover thoughts and emotions alike.

1655 On the positioning of the international agreements concluded by the Union within the hierarchy of the sources of EU law, see Adam et al (2014), pp. 149-156.

1656 See, e.g., European Parliament (2021).

1657 The European framework has been rightly described as a multilevel system of protection of fundamental rights. See Kostoris (2018), p. 68 ff.

1658 Cf. Neroni Rezende (2021), p. 375, note 63. On the qualification of data stemming from EFR processing as personal data and thus the applicability of the EU data protection framework, see Ienca et al (2021).

1659 See, e.g., Art. 1(1) LED.

1660 Rouvroy et al (2009), p. 50; Hildebrandt (2010), pp. 36-37.

1661 In philosophy, see Nussbaum (2001), p. 33. In cognitive research, see Feldman Barrett (2017), pp. 1–23; Science Daily (2017).

Lastly, the rights to privacy and data protection share a "common concern" with the presumption of innocence, that is the protection of the individual against undue stigmatisation. While this fair trial right is not specifically designed for the preventive phase, a strong upholding of these other "kindred rights" may achieve an anticipated application or coverage in this domain as well. From this perspective, one last section will explore the possible tensions between the use of EFR technologies and the rationale behind the presumption of innocence.

Lawfulness of the interference. First of all, when assessing the legitimacy of a measure that limits fundamental rights, the existence of a legal basis should be verified. The need for a legal basis grounding (and framing) the encroachments on the rights protected clearly emerges at the level of both primary and secondary legislation in the EU. This is echoed in Article 8(2) ECHR, which should be taken into consideration in light of the so-called "equivalence clause" (Article 52(3) CFREU). At the level of secondary law, the lawfulness requirement is one of the foundational principles of EU legislation on data protection, and is indeed recalled by Article 4(1)(a) LED. The use of EFR technologies should then be explicitly foreseen in a further legal basis of national or EU law.[1662] This text should in particular determine the grounds and purposes of the implied data processing operations, pursuant to the purpose limitation principle, another tenet of EU data protection law.[1663]

When interpreting the lawfulness principle in compliance with the jurisprudence of the ECtHR, the "quality of the law" doctrine should also be taken into account. For this requirement to be satisfied, the Court demands the legal basis in question to be at once "foreseeable" and "accessible".[1664] The quality of the law requirement has also been examined within the specific context of preventive and covert surveillance measures.[1665] The ECtHR has specified that the meaning of foreseeability here is not the same as in other domains. Specifically, "foreseeability" means that the law should simply be clear enough to inform citizens of the *circumstances* in and the *conditions* upon which public authorities are empowered to resort to these measures.[1666] In particular, the legal basis for surveillance should precisely frame the margin of discretion afforded to public authorities in resorting to these tools, as a safeguard to potential abuses.

General interest. A second requirement to be met refers to the general objectives pursued through the use of the surveillance tool. This criterion has never posed significant challenges in the law enforcement context, and the same goes for EFR technologies. On the one hand, Article 8(2) ECHR explicitly mentions national security, public safety and prevention, and prosecution of crimes as legitimate aims justifying encroachments upon the right to private life. On the other, the CJEU has recognised the prevention, investigation and prosecution of criminal offences and the protection of national security as objectives of general interests under the Charter.[1667]

[1662] Noteworthily, Recital 41 of the Proposal for the AI Regulation excludes that the latter can be understood as providing for a legal basis for the use of the technologies and related data processing operations tackled in the text.
[1663] Art. 4(1)(b) LED.
[1664] For a reconstruction of how the case law of the ECtHR and CJEU evolved in this respect, see De Hert et al (2020).
[1665] See, e.g., ECtHR, *Zakharov v Russia*, §229; ECtHR, *Big Brother Watch and Others v. the United Kingdom*, §306.
[1666] ECtHR, *Big Brother Watch and Others v. the United Kingdom*, §333; ECtHR, *Zakharov v Russia*, §229; ECtHR, *Malone v. the United Kingdom*, §67; ECtHR, *Huvig v. France*, §29; ECtHR, *Kruslin v. France*, §30; ECtHR, *Rotaru v. Romania*, §55; ECtHR, *Weber and Saravia v. Germany*, §93.
[1667] Cf. CJEU, *Digital Rights Ireland,* §§41-42; CJEU, *La Quadrature du Net,* §122.

Essence of the rights to privacy, data protection and freedom of thought. If these cumulative criteria are satisfied, the analysis should then turn to the "essence of the right" requirement[1668]. With respect to privacy, for instance, it is well acknowledged that one of the constitutive elements of the right is the protection of one's thoughts and inner states (i.e., so-called mental privacy), which also comprises the freedom *not* to manifest one's thoughts[1669]. The protection of the mind and the individual's self-determination serves as common rationale for privacy and the freedom of thought, which are even jointly conceptualised in some constitutional frameworks[1670]. Also, in the structure of the freedom of thought, people's inner mental space is covered by an absolute protection in Article 9 ECHR, with only external manifestations being subject to possible restrictions[1671].

By pretending to capture the most intimate aspects of one's life into datapoints, in absence of any will of the individual to share them, it is possible to argue that EFR technologies engage the very substance of the right to mental privacy and the freedom of thought. Importantly, the outcomes of the processing do not need to be accurate to engender an interference on the rights at stake[1672]. Especially with regards to privacy, the argument could also be extended to the freedom of thought, the right may be considered to be violated even if the invasion entails falsely attributing some opinion to a person.[1673] In EFR, the contents of the mind are reified and used as basis for decision-making, unbeknownst to or against the will of the subject. Being unaware of where this kind of invasive processing may intervene, individuals are also exposed to the chilling effects of surveillance and can be subtly manipulated into avoiding unordinary behaviour. Therefore, they may also be restricted in their freedom of self-determination, expression and assembly in any public place, in such a way that no overriding interest could justify.

Besides, it has also been submitted that the core of fundamental rights is essentially connected to human dignity, which may even work as a grounding basis for an independent conceptualisation of their essence.[1674] Indeed, The Explanations to the Charter seem to equate the need for respecting human dignity with the core essence of the rights protected.[1675] Generally, in the case of AFR, it has been purported that the fact of transforming the human face into an item for objectivisation and measurement touches upon the very dignity of the individual.[1676] When this biometric processing reaches out to emotions – the most private element of our personal life – it can be argued that people

---

[1668] For a legal analysis of the essence of the right criterion, see Chapter IV, §3.1.2.1.
[1669] Koops et al (2017a), pp. 531-532; Mantovani (2013), p. 588, note 6.
[1670] Koops et al (2017a), p. 531.
[1671] Schabas (2017), p. 420.
[1672] The scientific community is quite divided on whether EFR technologies are accurate and can actually "read our minds". As reported by Murgia (2021) the EFR company 4LittleTrees claims around 85% of accuracy. On the contrary, Affectiva claims an accuracy of more than 90%, as indicated by Heaven (2020), p. 504. Nonetheless, these results should be taken with a grain of salt. Indeed, one of the major underlying issues concerning the accuracy of these technologies seems to be data annotation. Before the EFR system is trained, datasets need to be labelled by humans choosing whether a given individual in a picture is expressing feelings of fear, happiness, etc., often without any context. Even in this case, experts disagree about whether humans are always able to correctly read others' facial expressions. In this sense, a panel of experts led by psychologist Lisa Feldmann Barrett has recently reviewed more than 1000 contributions on the matter, concluding that there is little to no evidence that people can reliably infer someone else's emotional state from a set of facial movements. See Heaven (2020), p. 503; Chen et al (2018).
[1673] Prosser (1984, original work published in 1960), p. 107; Schoeman (1984), p. 16.
[1674] Brkan (2018), p. 365.
[1675] See Explanation on Article 1. Explanations relating to the Charter of Fundamental Rights OJ C 303, 14.12.2007, p. 17–35.
[1676] McStay (2020), p. 3 (citing Wiewieorowski (2019) Facial recognition: A solution in search of a problem? European Data Protection Supervisor. edps.eur).

are susceptible to being deprived of their own dignity, provided that this kind of "emotion reading" carried out by the machine is non-consensual or covert.[1677]

With regard to the essence of the right to data protection, it may prove useful to refer to the *Schrems* case. In this decision, the Court considered that the right to judicial protection was compromised in the Safe Harbor regime because any effective remedy to the access, erasure or review of individuals' data was lacking. The existence of legal remedies to injustices is the logical premise to the effectivity of any fundamental right, and this need is explicitly recalled in the Charter with special regard to the right to data protection. Article 8(3) provides that compliance with data protection rules should always be subject to the control of an independent authority. Because of the specific features of EFR technologies, it is safe to argue that an effective review of this kind of biometric processing would be impossible or very difficult, thereby making the safeguard of Article 8(3) CFREU practically ineffective.

The difficulties in challenging the decisions of EFR systems stem from doubts concerning the science underlying emotion recognition technologies. From a psychological perspective, these find their roots in the work of Paul Ekman, who in the 1960s developed a theory according to which all human emotions can be reduced to a small number of "micro-expressions".[1678] Today, the mistrust towards the scientific foundations of this approach has significantly increased, to the point that emotional AI – and consequently EFR – has often been labelled as "pseudoscience".[1679] Among the most critical arguments against Ekman's work is the supposedly discriminatory nature of his findings, which would be blatantly ignorant of social, cultural and contextual factors impacting on the display of emotions.[1680] Against this background, it could be asked whether any effective remedy against a supposedly arbitrary or highly mistaken profiling of the data subject – possibly involving racial discrimination – is conceivable.

Where the very scientific foundations of the technology are unclear or highly questioned, which criteria should be employed to perform a sound review of the data processing? Would it ever be possible to achieve a reasonable outcome in such a process? According to which scientific standards should it be determined? In other words, the idea that it would be possible to ensure an effective review of data processing operations carried out by EFR technologies seems to be highly questionable. As highlighted by Tzanou, the "hard core" of the right to data protection – but the argument could be extended to the right to privacy and the freedom of thought – would be "what needs to be protected", i.e., the final values that are protected by such rights: dignity, informational self-determination and individual autonomy. In light of what is mentioned above, these values may be irreparably jeopardised by the use of EFR technologies in (urban) public spaces. In other words, there is an *a priori* incompatibility between these tools and the European human rights framework.

Still a need for a proportionality assessment? As has been noted, when a shortcoming is detected in assessing one of these first compatibility requirements, there is no need to perform a proportionality test. In the case of EFR, it can be argued here that such technologies should be banned because their use is simply incompatible with the essence of the right to privacy, the freedom of thought and the right to data protection.

Nonetheless, a proportionality assessment of EFR may still be useful. Considering the significant economic interests behind the development of the emotional biometrics industry and its implicit

[1677] Different might be the case in which the user voluntarily decides to interact with emotional AI, see McStay (2018).
[1678] See Crawford (2021); Thomas (2018).
[1679] Article 19 (2021), p. 6; Mc Stay (2020), p. 2.
[1680] Crawford (2020); Article 19 (2021), pp. 15-16; Sedenberg et al (2017), p. 2; Korte (2020). For empirical evidence, see Chen et al (2018).

acknowledgement in the Proposal for AI Regulation, limiting ourselves to proposing a ban on the technology would probably not make a great practical contribution to the ongoing debate. Also, if end-users of the technology (e.g., law enforcement agencies) did not consider the essence of the rights at stake to be interfered in, these would still need to carry out a proportionality assessment of the technology at hand. To this end, the next Section will engage with such a test. This analysis will reveal that, even if the use of EFR in law enforcement were compatible with EU human rights standards, its acceptable deployments in real case scenarios would be highly limited.

Proportionality test: Suitability and necessity. The proportionality principle is the last requirement listed in Article 52(1) CFREU. Notably, the CJEU was heavily inspired by the German Federal Constitutional Court in developing the procedural steps of its proportionality test, which first comprises an assessment of the suitability and necessity of the measure. In the specific context of data-driven technologies, the EDPS also clarified that the necessity test calls for an "assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal"[1681]. Thus, the assessment of the strict necessity – but also of the suitability of the technologies – requires a factual evidence basis.

Against this background, it is useful to recall an often-cited initiative, the US Transportation Security Authority's 2003 Screening Passengers by Observation Techniques (SPOT) programme. The software employed was directly built on a system set up by Ekman, which could automatically detect the six fundamental micro-expressions studied by the psychologist on a large scale. Ekman's method was then further leveraged to train "behaviour detection officers". During the implementation phase, the programme was highly criticised not only for its supposedly embedded racial biases, but also for its lack of effectiveness and credibility[1682]. Specifically, officers involved reported that passengers were flagged and interviewed randomly, and the low number of arrests made was totally unrelated to terrorist offences, which were the main targets of the initiative[1683]. Even more worryingly, it was claimed that the programme itself was leveraged to cover racial profiling practices[1684]. Eventually, the US Transportation Security Authority decided to limit funding for behaviour detection activities for the future, claiming that no evidence could support the suitability and effectiveness of the system which had costed the government 900 million US dollars[1685].

Moreover, the suitability of policing initiatives leveraging EFR could also be called into question from another perspective. When deployed in public spaces, especially those passed through by a significant number of people, AI cameras would presumably collect countless different inputs. To review them, police departments in charge would need to allocate a considerable amount of trained personnel in dedicated control rooms. This would be a necessity imposed from both practical and legal requirements. On the one hand, indeed, human review would be crucial to exclude people from further scrutiny who have been targeted due to evident errors of the machine. On the other hand, Article 11 LED would in any case require a human in the loop before any negative decision – such as being subject to a search – is taken with regard to the individual. Thus, regardless of the level of accuracy reached by the machine, any effective EFR initiative would also have to be supported by human resources, often lacking in underbudgeted law enforcement agencies. Hence, one could wonder if

[1681] EDPS (2017a), p. 5.
[1682] Schwartz (2019).
[1683] Id.
[1684] Ackerman (2017).
[1685] US Government Accountability Office (2013). Afterwards, however, the US government has not completely given up emotional biometrics initiatives in the aviation security field, see Hogdson (2019).

deploying EFR in urban policing would be more financially burdensome than directly sending patrolling officers looking in strategic venues. Decisions on the deployment of EFR should consider the financial affordability and sustainability of such programs when compared to traditional stop and frisk practices. In such assessments, it should also be taken into consideration that CCTV cameras in uncontrolled environments may provide lower quality images, which in turn might affect the accuracy of the processing and the effectiveness of these initiatives[1686].

Proportionality Stricto Sensu. The last argumentative passage of the CJEU's test is the proportionality principle in its strictest application. Almost indulging in a political task, the Court balances the impinged rights and the pursued values, questioning whether the legislator has made correct use of its margin of appreciation. When the limitation imposed on the right is considerably serious, it tends to apply a stricter approach[1687], thereby requiring the foreseen restrictions to be outbalanced by strong safeguarding countermeasures.

It should be preliminarily highlighted that in the case of EFR use in public spaces, a very strict proportionality assessment would be needed in light of the seriousness of the interference at stake. Three elements push us towards this direction: (i) the kind of data and processing involved; (ii) the scope and context of the surveillance measure; (iii) the absence of notification mechanisms for individuals interacting with EFR systems.

First of all, EFR technologies imply the automated processing of biometric data. Here, sensitivity invests both the kind of data and means of processing employed, and major safeguards against abuse by public authorities are expected[1688].

Secondly, the scope of the envisaged interference should be taken into consideration. The use of EFR in uncontrolled environments can indeed capture the data of any individual passing within the range of the camera indiscriminately[1689]. This scheme thus involves the collection of biometric data on a large scale, and the significance of such interference is magnified in public urban spaces where individuals do not often have the chance either to opt-out or to control the processing[1690].

Thirdly and finally, the lack of notification obligations for public authorities has been identified in the CJEU's case law as a criterion by which the seriousness of the interference can be assessed. That is because the absence of notification is "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance"[1691]. Such danger is greatly present for EFR implementations in the security domain. Indeed, Article 52(2) of the Proposal exempts users of biometric categorisation systems from notifying targeted individuals of their *interaction* with an AI system when the technology is used for detecting, preventing and investigating criminal offences.

While this derogation from the general transparency regime seems coherent with the latest ECtHR's approach to bulk surveillance systems[1692], its compatibility with the CJEU's view is less clear. In

---

1686 European Union Agency for Fundamental Rights (2019), p. 3.

1687 Cf. CJEU, *Digital Rights Ireland*, §48. Within the ECtHR's case law see ECtHR, *Segerstedt-Wiberg and Others v Sweden*, judgment of 6 June 2006, Appl. No. 62332/00, §88.

1688 Id. para. 54. See also Ienca et al (2021), pp. 9-10.

1689 The notion of uncontrolled environments covers "places freely accessible to individuals, where they can also pass through, including public and quasi-public spaces such as shopping malls, hospitals, or schools". Consultative Committee (2021), p. 5.

1690 ICO (2021), p. 9; see Consultive Committee (2021), p. 6 (discussing the role of consent in AFR use by public authorities).

1691 CJEU, *Digital Rights Ireland*, §37.

1692 While the ECtHR has acknowledged that subsequent notification is a relevant factor when assessing the effectiveness of remedies (see ECtHR, *Zakharov v Russia*, §234; see also ECtHR, *Klass and Others v. Germany*, §§68-71; ECtHR, *Weber and Saravia v. Germany*, §135), it has also considered that in bulk interception systems remedies that do not depend from previous

Tele2/Watson indeed, the Court has considered that when access to retained data is granted to law enforcement, targeted individuals should be notified of such processing and of the right to effective remedy, once such notification is no longer liable to jeopardise the investigations[1693]. Translating this condition into the EFR context may not require law enforcement authorities to notify *every* individual of their exposure to an EFR system, but it may impose notification to every subject that has been labelled as dangerous by the technology once this can no longer affect the efficacy of investigations. In absence of any clear indication on this point, however, the absence of notification can certainly be taken into consideration as a factor demanding the application of a stricter proportionality assessment of EFR security deployments.

The need for a close scrutiny of EFR can also be argued from the angle of its fundamental difference with AFR identification. What strikes most, in fact, is the lack of personal criteria of scope limitation in EFR applications. In these scenarios, law enforcement agencies are not looking for someone that is already known or warranted by the police and inserted in pre-populated watchlists; they are pursuing the "unknown unknowns", scrutinising anyone that displays suspicious behaviour compatible with their being involved in criminal undertakings. This parameter of "scope-limitation" is thus excluded from the proportionality assessment. Instances of preventive EFR could then be associated with a "mass-hybrid" form of surveillance featuring characteristics of both targeted and unfettered surveillance systems[1694]. On the one hand, the EFR surveillance initiatives are susceptible to being circumscribed from a temporal and especially geographical perspective, being deployable in restricted chosen venues for limited periods of time; on the other, EFR cameras can capture anyone within their visual range, even though the people pinpointed may have no connection whatsoever with the commission of criminal offences[1695].

Overall, two main elements support the application of a very strict proportionality assessment. First, the greater intrusiveness of EFR technologies in the law enforcement domain. Second, in comparison with AFR, the inapplicability of personal limitations to the deployment of these technologies. To exemplify the repercussions of adopting a stricter approach with EFR, it could be useful to look at the proportionality requirements already set out for remote biometric identification in public spaces by the Proposal for the AI Regulation. At the moment of writing, the Proposal is undergoing an ordinary legislative procedure before the competent EU institutions[1696]. With the outcome of this process still unknown at present, the analysis certainly bears some degree of a speculative nature[1697]. This is all the more uncertain considering the joint Opinion of the EDPB and the EDPS, rejecting the regime laid down in Article 5 of the Proposal and calling for a ban of the AFR technology altogether. With regard to EFR specifically, the EDPB and EDPS have also indicated that "the use of AI to infer emotions of a natural person is *highly undesirable* and should be prohibited"[1698].

Regardless of the outcome of the legislative procedure that the Proposal is undergoing, this analysis may hopefully bring some theoretical and practical contribution to the debate on the regulation of EFR

---

individual notification may even provide better guarantees (see ECtHR, *Big Brother Watch*, §358). On notification in the ECtHR's surveillance case law, see De Hert et al (2020), pp. 26-29.

1693 CJEU, *Tele 2/Watson,* §121.

1694 For a taxonomy of surveillance, see Chapter VI, §3.4.2.1.

1695 The same happens when social media databases are integrated in AFR software, enabling the identification of people that have not been inserted in watchlists. See Neroni Rezende (2020), p. 385.

1696 2021/0106(COD) Artificial Intelligence Act, Legislative Observatory.

1697 EDPB-EDPS (2021b), p. 3.

1698 Id. The same opinion is shared by the Consultative Committee (2021), p. 5 [emphasis added].

technologies[1699]. Indeed, the rules set out in the proposed Article 5 embed certain criteria that have been elaborated in the last few years by the European national and supranational Courts in surveillance case law. Certainly, it has been underlined that *not all* EFR applications could automatically fall within the purview of the regime of Article 5 of the Proposal, because some of these tools may not be designed to directly perform identification operations, specifically by matching the images of the people labelled as suspicious with a database of pre-stored templates. However, given the specificities of the law enforcement context, it seems pertinent to apply these criteria to EFR tools. Here, as said, public authorities always need to perform identification activities to pursue their primary objectives of preventing, and especially investigating and prosecuting criminal offences. Practically, emotional AI capabilities may be embedded in facial recognition software already designed for the identification of individuals. When such features are not available in the system, identification operations will probably be subsequently carried out by police officers themselves.

Guidelines from the European surveillance case law. Different aspects should be taken into account when assessing fair and balanced implementations of EFR technologies in law enforcement: (i) grounds for authorisation; (ii) scope-delimitation criteria; (iii) data storage requirements; (iv) *ex ante* and *ex post* supervision.

To begin with the grounds that could legitimise EFR in public places, not all the criminal offences that authorise the use of facial recognition could probably serve the same purpose in this context. For instance, Article 5(1)(d)(iii) of the Proposal refers to the crimes listed in Article 2(2) of Council Framework Decision 2002/584/JHA and "punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State". Although these criminal offences are identified within the EU framework as falling within the category of serious crime[1700], they may not always reach such a level of gravity to justify the deployment of EFR, which implies the setup of an indiscriminate surveillance system (even though in specific locations). EFR, if suitable and effective, could be used only to address the most serious forms of crime that also fall within the State needs of protecting its national security. For example, that would be the case of terrorism, a domain where the overlap between intelligence and law enforcement activities is evident[1701].

This argument finds corroboration also in the position recently adopted by the CJEU in *La Quadrature du net*. Here the Court found that only the objectives of safeguarding national security – including tackling terrorist offences – can justify more serious interference with fundamental rights[1702]. Considering that the "mental data processing"[1703] performed by EFR poses greater dangers than mere AFR identification, this kind of surveillance could be implemented only on the basis of objective evidence establishing the risk of a terrorist attack or other immediate danger for national security.

Furthermore, Article 5 refers to geographical, temporal and personal limitations to ensure a proportionate use of AFR in public places for law enforcement purposes. Clearly, these criteria are

[1699] For instance, it has emerged that controllers often give insufficient consideration to necessity and proportionality issues tied to the deployment of such systems. See ICO (2021), p. 11.

[1700] The same categories of offences are listed as constituting serious crime in Annex II of the Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.

[1701] On the issues that the growing proximity between intelligence and law enforcement has raised, see generally Vervaele (2005); De Hert (2005).

[1702] CJEU, *La Quadrature du Net*, §§135-137.

[1703] Ienca and Malgieri identify "mental data" with emotions or other thoughts that are not "related to health status, sexuality or political/religious beliefs". See Ienca et al (2021), p. 1.

drawn from the approach consistently applied by the CJEU in (mass) data retention cases since *Digital Rights Ireland*. The Court considers that the goal of fighting against serious crime does not allow indiscriminate surveillance: any monitoring measure needs to be circumscribed by objective criteria presenting an objective link with the stated aims[1704]. These criteria can limit data collection measures to particular areas or categories of people presenting – in specific timeframes – objective risks related to the commission of serious criminal offences[1705]. In absence of personal criteria of scope delimitation, temporal and geographical restrictions in EFR should be interpreted even more strictly than in AFR. However, quantifying the length and breadth of the surveillance measure remains difficult at a theoretical level. As provided for by Article 5 of the Proposal, decisions authorising practical implementations of the technology need to be guided by risk-informed criteria, such as the likelihood of the foreseen negative event and the seriousness of its consequences. Only in light of such information would it be possible to perform a balancing test to decide on the specific timeframe and location of EFR implementations. In order to avoid leaving too wide a margin of appreciation to public authorities, the relevant legislation should establish maximum delays and procedures for renewal of the measure with sufficient clarity.

According to the long-standing surveillance case law of the ECtHR and the CJEU[1706], clear and precise rules should also govern the procedures for subsequent storing of the data. In addition to data security standards, access to stored data shall be granted only to specifically trained officers, preferably less in number compared to those authorised to analyse AFR feeds. In this context, precautions to be taken before communicating data are also important. The expertise of the deployed officers has a bearing on the effective application of the right not to be fully subject to an automated decision, foreseen in the EU general data protection framework[1707]. In the preventive phase, specifically, this right should be triggered automatically, regardless of any request of the data subject, who is often unaware of the processing. This means that before taking any further action towards an individual flagged as suspicious, law enforcement agencies should *proprio motu* submit the assessment made by the AI agent to a manual review[1708].

When it comes to storage conditions, maximum periods of retention also play a significant role when assessing the proportionality of the surveillance system. To keep the intrusion within the limits of what is strictly necessary, data relating to individuals identified as potentially dangerous are to be distinguished from those that have not been determined as such[1709]. Similarly to the AFR "Locate" regime, data relating to the individuals that have not been labelled as dangerous should be immediately

---

[1704] CJEU, *Digital Rights Ireland*, §57; CJEU, *Maximilian Schrems,* §93; CJEU, *Tele 2/Watson,* §110; CJEU, *Opinion 1/15*, §191; CJEU, *La Quadrature du Net*, §133; CJEU, *Privacy International,* §78. With regard to the application of these criteria to the case of the AFR app Clearview, see Neroni Rezende (2020), 385 ff.

[1705] This approach has also made inroads outside the EU legal system with the recent decision R (Bridges) v. the Chief Constable of South Wales Police [2020] EWCA CIV 1058. Specifically, the Court of Appeal stated that two concerns arose within the legal framework of AFR Locate, namely the "who question" and the "where question". Indeed, in relation to the people that could be inserted in the watchlists and the locations where the technology could be deployed, legal rules were too generic and left an excessive margin of appreciation to public authorities.

[1706] Starting from the *Huvig* judgment, the ECtHR elaborated a set of foreseeability criteria against which surveillance laws need to be assessed. These criteria were later refined in the *Weber and Saravia* case, and have been thus called "Huvig" or "Weber" criteria since then. De Hert and Malgieri (2020, p. 32) argue these criteria have been implicitly integrated in the CJEU case law since *Digital Rights Ireland*.

[1707] See Art. 11 LED and Art. 22 GDPR.

[1708] A similar mechanism is already provided in Art. 6(5) of the PNR Directive.

[1709] The need for establishing difference in the storing regime according to the specific situation of the data subjects emerges clearly in the case law of the CJEU. See CJEU, *Opinion 1/15*, §§196-203.

erased[1710]. Also, retention periods for data relating to people flagged as suspicious should be severely restricted. Two scenarios can be discerned in this regard: if the initial positive match does not overcome the manual review, data shall be immediately erased as in the first case; conversely, if the human agent esteems that the pinpointed individual does express a suspicious attitude, the data storage should be limited to the time strictly necessary for the authorities to decide whether and how to take action, or for the notified individual to challenge the decision[1711]. Especially in real-time EFR scenarios, these decisions should be made in a very short timeframe to satisfy the preventive purposes of the surveillance initiative. In other words, EFR should only function as a tool for highlighting promising targets of intervention, assuming that one regards these systems as capable of such a task. Thus, data should be retained for a very limited amount of time. Also, immediate erasure of the data should prevent any further use or "leak" in subsequent criminal proceedings, where these could be used as evidence.

With regard to the nature and organisation of *ex ante* and *ex post* supervision of EFR processing, one first concern is the system used to authorise EFR deployments. To ensure that these are circumscribed to what is strictly necessary and that competing interests are reasonably balanced, authorisation should be given by an independent authority, in compliance with Article 8(3) of the Charter and the case law of both the CJEU and the ECtHR. Even though the ECtHR has expressed a preference for judicial control in the past, it suffices that the authority in question is capable to freely adjudicate without suffering interference from the government[1712]. In the case at stake, this requirement does not seem to pose problems, as it is already foreseen by Article 5(4) of the Proposal.

Instead, a second set of concerns regards notification obligations for surveilled individuals. To ensure a fair balancing of the interests at stake, interference with the rights to privacy and data protection should be compensated by strong safeguards, among which the right to an effective remedy. Regardless of their being checked by the police, should individuals targeted by EFR be notified that a positive match has occurred in their situation? Different answers may be given depending on how the surveillance scheme put in place by EFR-equipped cameras is qualified. For instance, expressing a difficulty in totally embracing notification requirements[1713], the ECtHR deems that bulk surveillance systems may not require a regime of bespoke individual notification, if remedies against inaccurate or unlawful processing are granted on a general basis to the population as a whole. According to the Court, in some cases this may even be the best solution to provide the highest standards of protection[1714]. Nonetheless, when the intrusiveness of the technology is this serious, nothing prevents legislators from cumulating two systems of remedies: one generalised and independent from the previous notification, and one based on notification for people having been specifically targeted by the system.

Considering the opposing interests at stake, it would indeed seem reasonable to generally exempt law enforcement EFR processing from transparency requirements, as provided by Article 52 of the Proposal. On the other hand, however, this derogation from the general regime does not appear to achieve a fair balance between security and fundamental rights requirements when it comes to people singled out as dangerous by the system. In this case, the potential negative consequences for the data

[1710] The AFR Locate program, implemented by the Welsh police and censured in the Bridges case, provided that when the facial data processing of passers-by did not lead to any positive match, such data should have been immediately erased. See R (Bridges) v Chief Constable of the South Wales Police [2019] EWHC 2341, §16.
[1711] See paragraph below.
[1712] De Hert et al (2020), p. 10. See also Malgieri et al (2017).
[1713] See De Hert et al (2020), pp. 26-29.
[1714] ECtHR, *Big Brother Watch*, §358.

subject and the seriousness of the intrusion in his or her private sphere should outweigh the exigencies of opacity normally underlying law enforcement activities. Therefore, in conclusion, a fair balancing of the needs at stake could probably be obtained only with a bespoke regime of subsequent notification for individuals labelled as dangerous by the EFR system.

2.3.2.1.3. EFR and the presumption of innocence

Presumption of innocence and preventive justice. It is widely acknowledged in literature that digital technologies are bringing about new challenges for the presumption of innocence.[1715] Foreseen in different constitutional traditions[1716], as well as at the international[1717] and EU level[1718], this principle is at the core of the notion of fair trial as enshrined in Article 6(1) of the Convention[1719]. In criminal proceedings, the presumption of innocence functions both as a rule of judgement[1720] and as a rule of treatment[1721]. While the presumption finds application only in *ongoing* criminal proceedings, it is not specifically devised for the preventive phase[1722]. Only persons "charged" with a criminal offence can benefit from this important safeguard[1723]. Despite the statutory limits of the principle, surveillance scholars have raised multiple concerns over a supposedly increasing erosion of the presumption of innocence, weakened by emerging mass surveillance programs[1724].

These positions rely on an extensive interpretation of the principle, which is reworked as a "moral entitlement" based on civic trust. People have right to be treated as trustworthy and should be presumed as acting in compliance with their main obligations in society, thus making any unfettered monitoring measure implemented by the State unjustified (e.g., mass data retention systems, ANPR, live facial recognition in public places). Where surveillance is not grounded on individual suspicion, the presumption of innocence is subverted by assuming everyone to be guilty of something.

In criminal legal scholarship, Ashworth and Zedner proposed a similar concept, i.e., the presumption of *harmlessness*. Like the presumption of innocence, this principle is underlined by the respect for each individual's status as a responsible agent in society[1725]. This implies that, aside from

---

[1715] See, e.g., Caianiello (2019); Hadjimatheou (2017), p. 40; De Hert (2005), p. 85.

[1716] In 2012, the CJEU recognised the presumption of innocence as "a feature of the constitutional traditions common to the Member States". See CJEU, *Criminal proceedings against Marcello Costa and Ugo Cifone*, judgment of 16 February 2021, Joined Cases C-72/10 and C-77/10, §86.

[1717] All EU Member States are part to the International Covenant on Civil and Political Rights, whose Art. 14(2) explicitly refers to the accused's right "right to be presumed innocent until proved guilty according to law".

[1718] In primary EU law, the presumption of innocence is enshrined in Art. 48 of the Charter, whose explanations equate to the contents of Art. 6(2) of the Convention. Even before the entry into force of the Charter, however, the CJEU had already recognised the presumption of innocence as one of the fundamental rights protected in Union law (see CJEU, *Montecatini S.p.A*, judgment of 8 July 1999, Case C-235/92, §175). At the level of secondary law, this right is explicitly recalled in Art. 2 of the Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings OJ L 65, 11.3.2016, p. 1–11.

[1719] ECtHR, *Konstas v. Greece*, judgment of 24 May 2011, Appl. No.53466/07, §29. It is no surprise that the ECtHR frequently examines complaints of violations of the presumption of innocence with joint reference to both the first and second paragraph of Art. 6.

[1720] This means that the burden of proof is placed on the prosecution, and any doubt on the criminal responsibility of the accused should profit the latter. Cf. ECtHR, *John Murray v. United Kingdom*, judgment of 8 February 1996, Appl. No.18731/91, §54; ECtHR, *Telfner v. Austria*, judgment of 20 March 2011, Appl. no. 33501/96.

[1721] This rule prohibits that the accused person is considered or treated as guilty before her responsibility is established by a court of law. Cf. ECtHR, *Shyti v. Romania*, judgment of 19 November 2013, Appl. No. 12042/05.

[1722] De Hert (2005), p. 85.

[1723] In this regard, it should also be noted that the Charter used a more neutral language compared to the Convention. Indeed, while Art. 6(2) ECHR employs the expression "charged with a criminal offence" – which should be nonetheless interpreted in light of the so-called 'Engel criteria' – the Charter only uses the term 'charged', avoiding any explicit reference to criminal offences.

[1724] Hadjimatheou (2017), pp. 41, 43 ff.

[1725] Ashworth et al (2014), p. 66.

high-risk settings (e.g., airport security), people should not be subject to universal risk assessments as they are to be "presumed free from harmful intentions"[1726]. Albeit suggestive, these attempts to broaden the interpretation of the presumption of innocence have been criticised by some other scholars who maintain that this safeguard should continue to be understood in strict legal terms, i.e., as a specific fair trial entitlement applicable only within the boundaries of ongoing criminal proceedings[1727].

It can be observed, nonetheless, that preventive criminal justice cannot avoid all considerations associated with the presumption of innocence. If that were the case, eluding individual fair trial safeguards would be extremely easy for public authorities. Indeed, these would simply have to make recourse to preventive instruments to subtly circumvent the rights that are granted to suspects in the framework of criminal proceedings.

Against this background, the need to pay a closer attention to the scope of the principle emerges in this case too, possibly "anticipating" its protective effects also to the preventive phase. In a world where individuals are increasingly singled out thanks to increasingly insidious technologies[1728], the risks for individuals to be wrongfully stigmatised are only destined to grow, dramatically. When it comes to EFR, specifically, potential issues with the presumption of innocence are twofold: (i) the lack of personal limitations in the scope of surveillance operations; (ii) the possibility of drawing adverse inferences against the suspect from inaccurate or unreliable processing carried out by the EFR system. In tackling these gaps, procedural safeguards attached to the rights to privacy and data protection seem to offer comparable standards of protection.

Absence of personal limitations. As said, the first issue with EFR implementations – contrary to remote biometric identification – is the lack of personal limitations in scope. People having no connection whatsoever with the commission of criminal offences may in fact suffer the negative consequences of EFR surveillance, and be wrongfully stigmatised because of it[1729], Interestingly, the absence of personal criteria and the resulting risks of undue criminalisation seem to generate concerns for both the presumption of innocence and the rights to privacy and data protection. On the one hand, the ECtHR assured that the presumption of innocence shields the individual from the stigmatising effect of an allegation of criminal liability, thus preserving his or her dignity[1730]. On the other, the rights to privacy and data protection are – as pointed out above – ultimately aimed at the preservation of human dignity. Their relevance to this end is only increasing with the world's digital transformation, as personal data processing can easily result in discriminatory and otherwise stigmatising practices.

The conceptual links between these safeguards could be spotted in the case law of the CJEU. While anchoring its considerations to the rights to privacy and data protection – and not specifically the presumption of innocence – the CJEU has raised concerns over the absence of personal limitations with regard to the provision of unfettered surveillance systems in the Union. In *Digital Rights*, for instance, the CJEU stated that the Data Retention Directive was susceptible for its indiscriminate scope of creating a (rather stigmatising) "feeling that their private lives are the subject of constant surveillance" in the minds of the people concerned[1731]. Since this landmark judgment, the approach

[1726] Id., p. 130 (citing Floud, Young (1982)).
[1727] Hadjimatheou (2017), p. 41.
[1728] On the preventive justice, see van Brakel, De Hert (2011); Brayne (2017); Ferguson (2017a).
[1729] Wrongful criminalisation is defined by Hadjimatheou (2017, p. 45) as "treating someone as if they have a particular propensity towards criminality or indeed are already involved in criminal activity, without proper grounds for doing so".
[1730] Balsamo (2018), p. 116.
[1731] CJEU, *Digital Rights Ireland*, §37.

taken by the Court in data retention cases has continued to be consistent. As confirmed in the recent *La Quadrature du Net* judgment, a data retention system targeting "persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with that objective of combating *serious crime*"[1732] is simply not compatible with the principle of proportionality as enshrined in EU law.

In the same line of reasoning, more invasive measures involving the *real-time* collection and analysis of communication metadata directly by law enforcement can only be justified with regard to specific individuals, thus requiring "a valid reason to suspect that they are involved in one way or another in terrorist activities".[1733] What emerges from this analysis is that particular serious forms of interference with the rights to privacy and data protection – if not justified by objectives of national security – need to be circumscribed by criteria of a personal nature, may these operate at a group or individual level. Further evidentiary elements need to substantiate a reasonable suspicion that such individuals may be involved in a criminal undertaking of a serious nature. As things stand, EFR does not seem to be fit to ensure that such subjective limitations are enforced.

Thus, the use of EFR seems to be at odds with the requirements of the CJEU, and this gap probably cannot be overcome. Overall, if legal theorists are still struggling to stretch the applicability of the presumption of innocence – understood as a component of the fair trial – the rights to privacy and data protection seem to offer an equivalent coverage for individuals in less safeguarding phases of law enforcement activities, in the broad sense (including preventive ones).

The implications of this argument go beyond the scope of the present work. What can be observed here is that the link between the presumption of innocence and the rights to privacy and data protection is probably to be found in the centrality of the value of *fairness* in the safeguards they provide. These rights share a common concern for undue stigmatisation, and more broadly for any *unfair* adverse treatment against the individual. This underpinning rationale for fairness translates into safeguards of a *procedural* nature, aimed at identifying justifications for encroachments on individuals' personal freedoms. This aspect further emerges in the guarantees that the rights to privacy and data protection can afford with regard to adverse inferences that can be leveraged against the individual based on the processing of his or her personal data.

Adverse Inferences. The use of adverse inferences by EFR surveillance against the suspect or accused is another condition that could negatively affect his or her presumption of innocence. In the case of EFR, these may be drawn from the "emotional demeanour" of the individual, caught in situations that the police find to be connected to the commission of a criminal offence. The use of presumptions can raise tensions with the presumption of innocence, as they can subtly reverse the burden of proof that should always weigh on the prosecution. Still, the ECtHR has clarified that the existence of presumptions of fact or law that may operate against the accused does not necessarily violate the presumption of innocence. This only requires such presumptions to be circumscribed within reasonable boundaries, ensuring a fair balancing of the interests at stake and defence rights[1734].

[1732] CJEU, *La Quadrature du Net*, §143 [emphasis added].

[1733] Id., §188.

[1734] ECtHR, Salabiaku v. France, judgment of 20 October 1998, Appl. No.10519/83, §28. More recently, see also ECtHR, *Iasir v. Belgium*, judgment of 26 January 2016, Appl. no. 21614/12, §30. In EU law, this approach was confirmed in the Directive on the presumption of innocence. Its Recital 22 indicates that the principle is not impinged by the use of presumptions, provided that these are "rebuttable", "used only where the rights of the defence are respected", and "confined within reasonable limits", also considering the proportionate use of means employed in relation to the aims pursued.

Looking at these requirements, could someone be fairly presumed to be "suspicious" only based on EFR processing? This point seems hard to argue. At the outset, it could be assumed that the use of such invasive technology may be proportionate in relation to the most serious criminal offences and threats to national security. However, several issues would persist with regard to the *fairness* of these operations. As argued above, the scientific unsoundness of EFR and its underlying technology makes the decisions of such software opaque and thus difficult to challenge for targeted individuals. If garnered datapoints – even those collected in preventive operations – were introduced in the proceedings, they could hardly be considered rebuttable by the defence[1735], also in light of an aura of objectiveness that often surrounds scientific evidence. Needless to say, this would irremediably impair the individual's rights of defence, his or her right to the equality of arms, to an effective remedy and the overall fairness of the proceeding.

Once again, similar procedural concerns are also supported in the data protection legislation, applicable to the preventive phase. Fairness as a basic tenet of data protection law prevents data controllers from taking any unjustified adverse or stigmatising action towards the data subject based on the processing of its personal data. The right not to be fully subject to an automated decision represents another an important entitlement in this sense, as it ensures that EFR processing is surrounded by adequate safeguards, among which the right to obtain human intervention and – as added by Recital 38 LED – the rights to express one's point of view, to obtain elucidation for the decision or to challenge it. All in all, whether presumptions based on EFR processing were introduced at trial or taken as bases for preventive and investigative measures, similar safeguards should be available to individuals to defend their presumption of innocence.

Having examined the issues of EFR in the security domain, the analysis will now shift its focus to the commercial context. General remarks will be made in the concluding section.

2.3.2.2. EFR in the targeted advertising domain

Applications of EFR in the commercial context. The use of biometric classification tools is growing in a significant variety of domains. In the commercial context, mere face detection systems seem to prevail. These do not necessarily infer outputs based on emotions displayed on the target's face, but on other physical features like gender and age. Applications of this kind have been installed in public places (e.g., squares and railway stations) for purposes of targeted advertising[1736]. In other cases, these functionalities are coupled with emotion recognition capabilities. For instance, United States' top retailer, Walmart, has patented a smart video-surveillance system that tracks customers' facial expressions as they move through the store, as well as their movements at checkout lines[1737].

In Italy, smart billboards (named "digital signage") have been placed in various railway stations, an initiative which has been validated by the national DPA[1738]. Software embedded in these billboards had the task of detecting a face within its focal range and measure different data, like the individual's age and gender, the time spent before the advert, and potentially the emotions displayed through facial expressions. At the outset, the *Garante* acknowledged the personal nature of the data collected by the billboards. However, it also emphasised that such data was immediately "erased" and not "remembered" by the system; data was used only for purposes of "anonymised analysis of the

[1735] On the issues brought about the use of AI system with regard to the defence rights, especially in adversarial systems, see Contissa et al (2020); Quattrocolo (2019).
[1736] On smart billboards, see e.g., Yalcinkaya (2017).
[1737] Graham (2017).
[1738] Garante per la protezione dei dati personali (2017).

audience" (*analisi anonimizzata dell'audience*), which could legitimise the processing based on the grounds of legitimate interest.

Personal data? The personal nature of the data processed by smart billboards has been highly debated in academia and among national DPAs, which have often expressed opposing views on the matter[1739]. Such question is strictly connected to that of the legitimacy of such systems, and will be briefly analysed by distinguishing various possible scenarios. A major factor to take into consideration is whether the advert is meant to change based on the characteristics of the viewer, in the timeframe within which the latter is present before the billboard. That being the case, it would be difficult to exclude the personal nature of the data in question, as argued before[1740]. Identifiability is not only linked to our L-identifiers (name and other attributes connected to our civil identity), but also to other individual features of a physiological nature. Where those are used to take a decision about individuals, or have an impact on them, then the processing should be considered to rely on personal data. Different might be the case – as analysed by the Italian DPA – of purely statistical uses of such data. Indeed, if facial reactions to posters are only used to provide advertisers with general feedback on the effectiveness of their communication strategy, then the impact of such systems on individuals' privacy and personal data protection would certainly be contained, and could be justified on grounds of legitimate interest.

Essence of the right. The same does not apply for systems designed to change in real-time based on the individual's cognitive reactions. As argued above, individuals have a right to not be obliged to manifest their thoughts and emotions to the outside world. This prerogative is protected both under the right to privacy, the freedom of thought and individual autonomy. Capturing (or trying to capture) such inner states without people's consent is likely to undermine the very essence of the fundamental rights at stake. Such processing would indeed entail an objectivisation and reification of individuals' cognitive states, which is something that could touch upon their personal dignity. Also from a data protection standpoint, reliance on highly contested scientific methods, with possible discriminatory impacts, could impair the fairness principle in such a way that an effective remedy would be impossible to achieve.

General interest and proportionality. Even if we deem that EFR processing does not to contradict the essence of the right criterion, it appears extremely difficult to legitimise its use in public or semi-public places for purely commercial purposes. Although a pivotal component of smart cities, economic dynamism cannot legitimise the most serious interferences with fundamental rights. Data protection authorities have been repeatedly sceptical about legitimising invasive data processing (or specifically, repurposing) only based on mere economic convenience. Legitimate interests in heightening the impact of programmatic advertising may not be strong enough to allow non-consensual reification of people's emotions. In other words, these practices may fall short of the strict necessity criterion. Lastly, in light of the value of urban public places[1741], a strict proportionality assessment of this practice may also highlight that a correct balancing of the interests at stake may not be in favour of a further privatisation of such environments.

2.3.2.3. Concluding remarks

In light of recent developments suggesting an increasing use of EFR technologies in the law enforcement and commercial contexts, it was considered appropriate to evaluate them in light of the

[1739] See above Chapter I, §2.4.2.2.
[1740] Id.
[1741] On the meaning and value of public places, see above Chapter III, §2.2.

European standards of fundamental rights protection. Specifically, EFR deployments were assessed against four fundamental rights, sharing a common rationale: the rights to privacy and data protection, the freedom of thought. To some extent, and as far as law enforcement activities were concerned, the presumption of innocence was also taken into consideration. Ostensibly, a certain degree of speculation could not be avoided in this preliminary assessment of EFR. As a matter of fact, two levels of unpredictability are involved.

On the one hand, the legal framework for regulating the use of AI in the EU is still underway and the future work of legal interpreters may further impact on its concrete application. On the other, specific instances of implementation of EFR technologies are still surrounded by several uncertainties and tailored assessments can only be supported by a substantial factual basis. These information gaps can only be tackled in future research.

All in all, the surveillance case law elaborated both by the ECtHR and the CJEU is still under development, but now provides a comprehensive framework through which new technological advancements can be assessed. While it is acknowledged that such tools may have a beneficial impact on the efficiency of law enforcement activities, their use should also be critically evaluated in democratic societies. The same goes for commercial employments of EFR, e.g., for purposes of targeted advertising in public environments. In other words, relevant actors should not only be able to determine when and how new technologies can be fairly deployed, but also which uses should simply be rejected in a democratic society. In the case of EFR, the latter seems to be the most solid conclusion.

3. Drones

Outline. This section will provide an overview of drone applications and their technical capabilities. It will also outline surveillance and fundamental rights risks of the technology. Lastly, two use cases will be examined, one related to delivery services through drones (both in commercial and emergency situations), the other to security-related scenarios.

3.1. Overview of the technology

What are drones? Uses and definition. Despite their increasing popularity, drones are not a new or emerging technology[1742]. The reason for drones' renewed traction today is that they are smaller, less expensive and more available to the public than ever before[1743]. Statistics indicate that drone market was worth approximately 27.4 billion U.S. dollars in 2021, and it is estimated to reach the value of 58.4 billion by 2026[1744].

Initially designed for military purposes, drones today serve a great variety of purposes, including delivery purposes, agriculture monitoring, wildfire control, public infrastructure surveillance, humanitarian aid, and journalism[1745]. In addition, their potential for delivering smart city services is also being explored. Drones can support urban actors in managing traffic congestion and car parking, crowd monitoring and control, weather assessments, security and emergency response. Compared to sensors embedded in fixed infrastructure, they can offer even a wider pool of useful data to city planners and municipal governments[1746].

[1742] Custers (2016), p. 9 (providing a brief history of drones and similar technologies).
[1743] Id.
[1744] Statista (2021).
[1745] Bassi (2020), p. 62. See also Wright et al (2016), p. 327.
[1746] McCulloch (2020).

In Europe, the European Union Aviation Safety Agency (EASA) expects urban air mobility (UAM) to become a reality in three to five years[1747]. The Agency also conducted a study on the social acceptability of UAM, finding that European citizens are more lenient to welcome uses of drones that have a clear social benefit, i.e., medical and emergency-related transportation and disaster management[1748]. Against this background, an EU-funded coalition of cities and regions is also focusing on the sustainable development of urban air mobility, trying to convey a citizen-centric perspective[1749].

Behind what is commonly termed as "drone", however, there is a more varied group of technologies. the most used terms in technical literature and legislation are "unmanned aerial vehicles" (UAVs) and "unmanned aerial systems" (UASs). While UAVs refer to the flying platform (and its payload, if any), the term UAS more generally describes both the flying platform and the ground station controller[1750]. Another common terminology is Remotely Piloted Aircraft Systems (RPAS), which identify unmanned aerial systems that are remotely controlled by a pilot[1751]. For instance, the International Civil Aviation Organization (ICAO) defines an RPAS as a "set of configurable elements consisting of a remotely-piloted aircraft, its associated remote pilot station(s) the required command and control links and any other system elements as may be required, at any point during flight operation"[1752].

In the following sections the term "drone" will be employed, being one most used in the media and public discourse. The military connotation of the word is indeed fading, and drones are increasingly associated with civil use, e.g., a small helicopter equipped with a camera, remotely controlled with a smartphone[1753]. Because the focus here is urban surveillance, this more general terminology seems more appropriate in this context.

Technical capabilities. Drones can differ greatly in their payload ranging and embedded IoT sensors, which can make their impact on fundamental rights quite disparate on a case-by-case basis[1754]. Among the most common drone equipment, there are (i) visual recording sensors; (ii) detection equipment; (iii) radio-frequency equipment; (iv) specific sensors for the recording of nuclear traces, biological traces, chemical material, explosive devices[1755].

Firstly, smart cameras can have fixed or variable focal length, store or transmit live images, have embedded (emotion) facial/object recognition software that allow drones to identify individuals, objects (e.g., licence plates), patterns of movement, or detect the thermal energy emitted by a target (e.g., a home), even in poor lighting conditions (e.g., at night)[1756].

Secondly, detection equipment can include infrared scanners, radars focusing on objects, vehicles and vessels collecting location information on targets bypassing walls, smoke and other barriers[1757].

Thirdly, radio-frequency sensors can be antennas harvesting the location of Wi-Fi access points and cellular stations, or IMSI catchers used by law enforcement[1758]. Of course, the number and kind of

1747 EASA (2022).
1748 European Commission (2022b).
1749 Id.
1750 Custers (2016), p. 11.
1751 Id. The same terminology is described in Završnik (2016), pp. 1-2.
1752 ICAO (2011), p. x.
1753 Custers (2016), p. 11
1754 See Finn et al (2016), pp. 48, 50; Wright et al (2016), p. 328.
1755 Article 29 WP (2015), p. 6.
1756 Id., pp. 6-7. See Brewster (2021).
1757 Article 29 WP (2015), p. 7.
1758 Id.

sensors installed in a given drone can raise quite different privacy and data protection risks, as will be shown next.

3.2. Surveillance and fundamental rights risks

A new kind of surveillance? Drones have sparked both techno-enthusiast and techno-dystopian views[1759]. On the one hand, tech corporations often propose a supporting narrative of drone technologies, which will allow us to even "place" sensors in the skies to sense the world's "heartbeat"[1760]. On the other hand, drones are seen as part of the wider development of the IoT, which has normalised pervasive surveillance[1761]. Because drones do not usually encounter traditional barriers to surveillance, these have raised worries of "fishing expeditions" aimed at collecting personal data covertly.

Early reflections on drones have focused on whether these could somehow change the nature of contemporary surveillance. While some label drones simply as "another tool in the box", others believe that these technologies have a transformative power on surveillance[1762]. Among the most cited privacy risks associated with the deployment of drones, we find the "chilling effect; dehumanisation of the surveilled subjects; transparency and visibility, accountability and voyeurism; function creep; bodily privacy; privacy of location and space; and privacy of association"[1763]. Moreover, from a strictly law enforcement perspective, the use of drones in policing also fits within the broader shift from reactive to preventive justice[1764]. With crowd management and individual identification capabilities, drones can be deployed by law enforcement in their tasks of keeping the public order and prevent the commission of crimes.

Against this backdrop, the following sections will briefly outline recurrent privacy and data protection risks associated with drones. Firstly, general privacy risks will be outlined, touching upon associational privacy and freedom of thought. Secondly, the focus will be shifted on specific data protection risks. Privacy and data protection legislation is indeed very relevant for a legitimate deployment of drone technology. Unsurprisingly, Art. 132 of the Regulation 2018/1139 on common rules in the field of civil aviation explicitly recalls the applicability of GDPR rules[1765]. After the overview on the most relevant issues, a brief legal analysis of concrete drone applications will be proposed.

3.2.1. Privacy risks

The scope of surveillance. Because drones have become increasingly affordable, multi-tasking and are not subject to usual land barriers, they could significantly extend the scope of standard surveillance practices. In these terms, a comparison with CCTV is often made. The unique vantage point for drones heightens the capabilities of on-board sensors to collect data, when compared to similar fixed sensors

[1759] Završnik (2016), p. 3.
[1760] See Evans (2012).
[1761] Id.; see also the critique of Andrejevic (2016), pp. 21 ff.
[1762] Finn et al (2015), p. 27; Research Group of the Office of the Privacy Commission of Canada (2013), p. 11; Wright et al (2016), p. 330.
[1763] Finn et al (2016), p. 50; Bassi (2020), p. 64.
[1764] Završnik (2016), p. 5.
[1765] Art. 132 of the Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.) PE/2/2018/REV/1, OJ L 212, 22.8.2018, p. 1–122.

like cameras[1766]. The fact that drones could be interconnected to other IoT systems also increases the possibility to carry out surveillance on a large scale and in real-time, allowing to link information that would otherwise have remained siloed[1767]. Applying geographical restraints to aerial surveillance also appears to be critical, as drone may collect data without the need for a direct line of sight[1768]. These concerns may even be magnified when drones incorporate visual payloads (e.g., high-resolution, thermal imaging or infrared cameras), which are in fact the most common in drones[1769].

Covert surveillance: accountability and rule of law. Sensors embedded in flying drones can also "travel" long-distance and escape the sight of individuals on the ground. This implies reduced transparency of the data collection, when compared (again) to CCTV[1770]. With respect to other IoT sensors embedded in the urban infrastructure, they are also highly mobile, which may hamper individuals from keeping track of when their data is being collected. The covert nature of drone surveillance thus poses great challenges of accountability[1771]. People may not be aware of whom has collected their data, and therefore may not be able to exercise their data protection rights and remedies. When public authorities (in particular law enforcement) are the ones carrying out aerial surveillance, the issue is magnified and may touch upon the very principle of the rule of law. Very intimate intrusions upon individuals' lives may indeed occur without a sound legal framework circumscribing the powers of the State to resort to such measures, which in itself may not guarantee a transparent and proportionate implementation of the technology.

Chilling effect: Associational privacy and freedom of thought. For their covert nature, drones are also high impacting on behavioural and associational privacy. Since individuals may not be aware of when surveillance is actually taking place, these technologies generate a chilling or panoptic effect[1772]. Under the constant fear of being watched or tracked, individuals may unconsciously restrain their behaviour in public venues. Of course, this has a bearing on fundamental rights such as freedom of thought and association. In particular, people may feel dissuaded from taking part in social movements, demonstrations, or public dissent activities, worrying that they may be monitored[1773].

3.2.2. Data protection risks

Identifiability and lawfulness. As said, drones can integrate a great variety of sensors. While the most basic type of aircraft (embedding only vital components) might not process personal data, this may not be the case of other artefacts supporting visual payloads and other IoT sensors[1774], which require a legal basis for processing under EU data protection law. Different possibilities can be envisaged. Firstly, consent (Art. 6(1)(a) GDPR) may constitute a viable legal basis only in limited scenarios, especially when the collection occurs in public spaces[1775]. Drone processing operated in quite restricted environments, where attendants are aware of the processing, may be legitimised pursuant to these grounds (e.g., a sport training session with no spectators, or wedding photos)[1776]. Monitoring activities carried out by public authorities out in the open may instead not fall so easily within this category.

1766 Article 29 Working Party (2015), pp. 5, 8; Finn et al (2015), p. 29; Bassi (2020), pp. 65-66; Wright, Finn (2016), p. 331.
1767 Id., p. 8; Finn et al (2016), p. 48.
1768 In line with the case law of the CJEU on surveillance, this is advocated by Article 29 WP (2015), pp. 8, 11.
1769 Finn et al (2015), p. 30.
1770 Article 29 WP (2015), p. 5.
1771 Finn et al (2016), p. 48.
1772 Id.; Article 29 WP (2015), p. 7; Bassi (2020), p. 65; Finn et al (2015), pp. 31 ff.
1773 Finn et al (2015), pp. 31 ff.
1774 Article 29 WP (2015), p. 6. Vital components of drones are frame, motors, battery, receiver and flight controller.
1775 On the issues of providing consent to data collection in public spaces, see Chapter I, §3.1.
1776 Article 29 WP (2015), p. 12.

When drones are employed to deliver a specific service, data processing may be based on the performance of a contract (Art. 6(1)(b) GDPR). In its 2015 Opinion on drones, the Working Party illustrated the example of someone purchasing a product that is to be delivered to his or her home via a drone. The criticism about this solution is that Art. 6(1)(b) would only cover the processing of data relating to the parties of the contract, excluding the incidental processing of non-affected third parties (individuals present in the trajectory of the delivering drone)[1777].

Drones used in emergency-related situations may instead rely on Art. 6(1)(d) GDPR, which covers processing that is necessary to protect the vital interests of the data subject or of another natural person. This might be the case of widely accepted uses of drones like disaster relief, fire scenes inspections, rescue of victims of snow and mountain incidents[1778]. In this regard, however, the Working Party has warned about the need for a restrictive interpretation of this legal basis, encouraging recourse to other legal bases such as compliance with a legal obligation (Art. 6(1)(c) GDPR), public interest (Art. 6(1)(e) GDPR), legitimate interest (Art. 6(1)(f) GDPR).

The legitimate interest of the controller (Art. 6(1)(f) GDPR) may provide grounds for data processing by drones. Here, the Working Party makes the example of operations necessary for pipe or power line inspection, critical infrastructure surveillance, aerial photogrammetry, atmosphere and meteorological research, wildlife research, energy monitoring, hurricane tracking archaeological site mapping, or sea ice monitoring[1779]. It can be noticed that many of these scenarios involve interests with a broader societal meaning, which begs the question of whether a public interest basis may sometimes be more appropriate when the societal goal is recognized by the law[1780].

Lastly, drones employed in the law enforcement domain will need to comply with the LED to lawfully process personal data. Because such measures constitute an interference upon the rights to privacy and data protection, the Working Party considered that the processing should be subject to the conditions laid down in Art. 52 CFREU[1781]. Firstly, it should be grounded on an additional legal basis under EU or Member State law. Such a legal basis should abide by foreseeability and accessibility requirements and thus clearly circumscribe the extent of the surveillance powers that can be exercised by law enforcement agencies. Interestingly, the Working Party here referred to the geographical and time limits that echo the CJEU surveillance law on the matter[1782]. The deployment of drones should thus be strictly limited to locations and time periods that feature high risks in terms of public security. Nonetheless, because of their chilling effect, caution should surround the use of drones to monitor demonstrations and similar gatherings[1783].

GDPR applicability and data controllership. Entities and stakeholders using drones are quite varied. Among these, we can find manufacturers and different types of users, ranging from drone-enthusiast individuals, to companies, public authorities and law enforcement. The issue of *who* is operating the drone has of course a bearing on the applicability of different data protection regimes. For instance, Art. 2(2)(c) GDPR exempts natural persons from complying with the Regulation when performing purely personal or household activities. While this may apply to individuals flying drones in their free time, it should be kept in mind that the CJEU tends to construe the household exception quite

1777 Id.
1778 Id.
1779 Id., p. 13.
1780 On the implications of relying on these two legal bases in smart cities, see Chapter II, §§3.2 and 3.3.
1781 Article 29 WP (2015), p. 11.
1782 Id.
1783 Id.

strictly[1784]. In this light, it appears difficult to apply such an exception to private citizens operating camera-equipped drones out in open spaces, where the aircraft is likely to record the presence of other people[1785].

Data controllers and processors should also be clearly identified for each drone operation[1786]. Taking into consideration the Working Party's Opinion on the recent developments of the Internet of Things, situations of diversified control can be envisaged[1787]. While Recital 78 GDPR seems to exclude any responsibility of IoT manufacturers with respect to data controllership, the Working Party believes that these should be qualified as controllers for the processing of data generated by the devices (including drones)[1788]. Third parties can also develop applications to access drone sensor data through APIs. If data subjects install these applications in their devices and the transferred data is not properly anonymised, such app developers should be designated as controllers for the processing consisting in the access to collected data[1789]. Users of drones (whether entities or individuals) also exercise an operational control on the data that is being collected, as they pilot where the drone flies and can turn on or off some of the sensors installed in the aircraft when needed. Different layers of control can thus be envisaged in drone-populated environments. Who the controller is and who the processor is can only be assessed on a case-by-case basis.

Transparency and right to information. The lack of clarity on who exercises control over drone data also impacts on the effectiveness of transparency obligations under data protection law. As mentioned above, transparency is also affected by the reduced visibility of drones in aerial space. For this reason, the Working Party proposed a "multi-channel approach" to make individuals aware of the ongoing data collection[1790]. Controllers may have recourse to signposts, information sheets for events (but also QR codes) when drones are operated in fixed locations. The same goes for social media, TV screens, flashing lights, buzzers and similar tools. Drone operators could make themselves and aircrafts visible from the ground by displaying a registration mark (like a license plate). The Working Party has also recommended operators to publish information in their website, or in newspapers, leaflet, posters or by mailbox[1791]. In smart cities, public authorities are already making sensor registries public, and the same could be done with real-time information on drones.

Data minimisation, privacy by design and default, data security. Because drones are not subject to traditional land barriers, they can easily fly across different locations and collect data on a large scale. Also considering the great variety of sensors that these devices can support, the principle of data minimisation is certainly put under stress. The risk that drones collect data where they are not supposed to is indeed very high.

In the law enforcement domain, it should also be considered that the data minimisation principle is translated in a lighter fashion. Art. 4(1)(c) LED merely establishes that gathered data should not be "excessive in relation to the purposes for which they are processed". The rationale for this provision is

[1784] See CJEU, *Bodil Lindqvist*, §47: "That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people".
[1785] Article 29 WP (2015), p. 9.
[1786] Id., p. 8; Bassi (2020), p. 68.
[1787] Article 29 WP (2014a), p. 12.
[1788] Article 29 WP (2014a), p. 11.
[1789] Id.
[1790] Article 29 WP (2015), p. 15.
[1791] Id., p. 16.

understandable in this domain, where it is often difficult to assess a priori how much and what kind of data is necessary to achieve law enforcement investigative and preventive objectives. Nonetheless, when applied to such far-reaching technology in the first place, its implications may be worrying[1792].

In light of these technical difficulties, the EDPS has highlighted the importance of data protection by design and default measures. With specific regard to manufacturers, it recommended to (i) diversify the categories of sensors to be installed in the aircraft depending on the operators objective; (ii) set up data retention by design measures, with the possibility of scheduling the automatic and continuous deletion of stored data; (iii) foresee the possibility to turn on and off sensors in flight (so that the recording is always proportionate); (iv) set the most privacy-friendly functionalities by default; (v) provide clear information to the user on privacy issues that may arise when using the device, possibly in a privacy notice accompanying all drones sold within the EU territory[1793]. Other measures may also include differential privacy functionalities through the design of flight maps which could help minimise drones' trajectories and thus data collection[1794]. Furthermore, privacy by design measures should be adopted to ensure the security of data processed by drones. Relevant measures include encryption tools for video-recording drones[1795].

Among organisational measures mandated by the GDPR, the DPIA is of the utmost importance. Under Art. 35(3)(b), DPIAs are mandatory when processing is carried out on a large scale, which is often the case for drones[1796]. Scholars have also stressed the importance of involving manufacturers in these assessments, as they are "the best placed to design privacy preserving technologies in a drone"[1797]. Impact assessments should assist all those involved in the production and use of drones in identifying risks to all types of privacy (including behavioural and associational privacy), to understand how to address them (also in consultation with all relevant stakeholders), and evaluate when the processing of personal data by drones is legitimate, necessary and proportionate to the pursued purpose[1798].

3.3. Illustrations

At present, drones are being experimented in varied contexts. In Castellfedels (Spain), Taranto, Grottaglie and Manduria (Italy) the SESAR project is experimenting drone delivery in different use cases, such as domestic package deliveries from an airport, small items from a warehouse direct to a customer, regular payloads from a company warehouse to field engineers or deliveries between two fixed locations, delivery of drugs and defibrillators[1799]. Advertised benefits of these solutions include (i) avoiding traffic congestions; (ii) lowering emissions; (iii) more rapid response to medical emergencies in remote locations[1800].

In Bari (Italy), the municipality concluded an agreement with the national civil aviation agency (ENAC) to create a drone living lab. Different operations are envisaged, ranging from monitoring waters, changes in soil sealing, to general surveillance of the territory (an objective that remains unspecified in public sources)[1801]. On the other side, drones are also being used by security agencies to

[1792] This provision is seen as critical by Bassi (2020), p. 66.
[1793] EDPS (2014), §61. See also Article 29 WP (2015), p. 17.
[1794] See Bassi et al (2019).
[1795] Bassi (2020), p. 67.
[1796] Id., p. 68. See also Article 29 WP (2015), p. 14.
[1797] Wright et al (2016), p. 340; See also Finn et al (2015), pp. 77-78.
[1798] Wright et al (2016), p. 332.
[1799] SESAR (2022), p. 9.
[1800] Id.
[1801] Comune di Bari (2020).

keep the public order in vastly crowded events, such as sports matches in stadiums or religious processions (in Zaragoza, Spain)[1802].

Against this backdrop, the following sections will analyse two use cases: one related to delivery services offered by drones, the other concerning the monitoring of public spaces for security reasons. Each scenario, inspired by real-world projects, will be enriched with possible variables to suggest differentiated proportionality assessments.

3.3.1. Drone delivery

Scenario description. Flying Forward 2020 is an EU-funded three-year research project aimed at integrating drones into the geospatial infrastructure of European cities[1803]. Last mile and emergency delivery was one of the use cases tested by partners in the High Tech Campus Eindhoven (HTCE)[1804]. Three drones were used for last mile delivery of food, express shipping of mail, emergency support with medical equipment.

In the case of food, the objective was to shorten the delivery time and costs of meals. Campus residents would order their food from a predesigned app; thanks to a centralised system, the order was prepared and placed in a delivery box and subsequently secured in a locker located at the drone departure tower. The drone would then take off for a drone destination tower. The customer would finally receive an app notification to pick up their meal and open the smart locker.

As for express shipping of mail, autonomous drones were used to unburden the Swiss Post employees from picking up express (urgent) mail packages. In this case as well, a customer would bring their package to a departure tower where a delivery box is placed. The drone would then carry the box to the destination tower at the Swiss Post distribution centre. The Swiss Post will finally receive a notification to pick up the package. Lastly, the emergency support case entailed drone delivery of medical equipment to unconscious people even in most rural parts of the campus. One of the goals was to reduce the delivery time of medical equipment. In case of need, the drone would take off from its nest on top of a smart lamppost and fly straight to the emergency site where the emergency toolkit is dropped with a cable to the ground and detached close to the ground. The caregiver would finally be able to pick up the equipment without the risk of touching the drone in operation.

Legal analysis: Legal basis and proportionality. In this context, the legitimate interest basis (Art. 6(1)(f) GDPR) seems the most appropriate to ground drone data processing for these research purposes. In balancing the interests of research partners (i.e., drone operators) against the interests and fundamental rights of data subjects (i.e., campus residents and those who work on the premises of the campus), different factors should be taken into consideration.

Firstly, the experiment takes places in a restricted environment, a large innovation hub hosting different offices and social services. There are extensive green areas and population density is lower than in regular cities. The official website of the HTCE provides information on drone rules, which may lower the privacy expectations of people strolling around the campus (although these may not be reduced to zero). The high concentration of high-tech companies in the area also suggests that similar privacy-impacting experiments are also possibly implemented in the area.

[1802] Flying Forward 2020 (2022), pp. 36 ff.
[1803] See the official website of the project. https://www.ff2020.eu/about/.
[1804] See the description at Flying Forward 2020 (2022), pp. 68 ff.

Because privacy expectations in the HTCE are likely to be lower, the balancing test embedded in the legitimate interest ground seems to be tipped in favour of drone operators. However, the assessment might differ if the same services were translated in a real city, especially a big one.

As indicated by the Working Party, data processing in the context of drone delivery could be based on the performance of a contract basis. Nonetheless, Art. 6(1)(c) could here cover only the processing of data belonging to the person requesting the service, leaving aside all the data collected incidentally by the drone in its path. Such data may also fall within the legitimate interest case. The balancing test here, however, may not necessarily give the same outcome. A real urban environment is indeed very different, and the data that could be potentially gathered by the aircraft are significantly higher in number. Data collected may also belong to people having different privacy expectations according to the urban environment they find themselves in.

Therefore, the balancing test should be quite stricter. Surely, privacy-by-design and by-default measures embedded in the drone could help the controller to have a positive proportionality assessment of the initiative. If the drone is meant for service delivery and not for strictly surveillance purposes, it should be equipped with low resolution cameras (i.e., obstacle avoidance sensors)[1805]. They should neither collect unnecessary GPS or RFID data[1806], nor communicate with databases providing for this information, to avoid identification of people caught in camera (although not immediately recognisable).

As in the HTCE scenario, predefined corridors for drones (in addition to no-fly zones) would be useful and could reduce the pervasiveness of drone presence across the city and generate clear expectations in citizens as to where urban aircrafts may be flying. Admittedly, however, this solution may significantly frustrate the economic advantage and customer convenience of relying on drone service delivery. In fact, different considerations should finally be dedicated to the purpose concretely pursued by the drone. For the first two cases of drone delivery (meals and urgent mail shipments), mere economic advantage for delivering companies may probably not be enough to legitimate large scale processing by drones in cities[1807].

The case of emergency response may be different, since the processing would be based on the need to protect the vital interests of the data subject or of another natural person (Art. 6(1)(d) GDPR). This purpose encounters wider social acceptance than mere commercial ones, and could also legitimise – where strictly necessary – the use of visual payloads on the drone.

From a surveillance perspective, it should also be considered that the extensive integration of drones in cities requires the setup of an Unmanned Aircraft System Traffic Management (UTM). UTMs will be the tool to control multiple drone operations conducted beyond visual line-of-sight (BVLOS), where air traffic services are not present. The data collected by these systems would normally include the real-time location of the drone, as well as its flight trajectory.

Some of these data could in fact qualify as personal. That might be the case of data emitted by privately-operated drones and used for recreational purposes: here, the data could certainly be traced back to the identity of its operators (which should be known also for liability purposes). As for flight trajectories, the assessment might be more challenging. In the context of service delivery indeed, it might seem difficult to trace back such data to identified or identifiable persons, if not in specific circumstances (e.g., delivery in very remote locations). At the time being, however, it's impossible to

[1805] See Bassi et al (2019), p. 584.

[1806] Drones equipped with standard GPS sensors would not seem to be able to sniff location data from devices in the vicinity. On the contrary, the network that drones usually use to send data to the ground seems to be very similar to Wi-Fi and thus prone to attacks. That is why more advanced solutions propose to leverage mobile networks (i.e., 4G and 5G).

[1807] See also Article 29 WP (2015).

know if these datasets will be linked to other sources, thus allowing for re-identification of people having benefitted of drone-based services.

Although any unnecessary data collection or repurposing should be avoided, UTMs of the future may constitute mass surveillance systems at urban scale, where the data generated by flying drones are systematically collected to prevent accidents and ensure a coordinated management of urban airspace. If UAM is to become an integrated part of city infrastructure, possibly providing essential services (e.g., emergency response) such systems could be legitimised even under national security reasons. Likewise, avoiding life-threatening accidents (e.g., drones or helicopters crashing upon individuals) may constitute a very strong reason to justify such extensive data collection.

3.3.2. Security-related scenarios

Scenario description. The following scenario is construed based on two separate research projects. Generally speaking, the technical community has been working on equipping drones with tracking capabilities, i.e., to identify individuals and suspicious vehicles[1808]. In Matera (Italy), a 5G network has been set up with the support of two communication companies. The computational power provided by this network allowed researchers to deploy a drone able to recognise objects and people from video-recordings in harsh flying conditions, as well as to detect jammers[1809]. In the hypothesised scenario, the drone would be equipped with a 2D camera, transmitting real time footage to a local server. Then, deep learning techniques would extract facial biometric templates and run them against a hotlist database (containing images of the members of the research centre). In a real-world situation, the researchers also theorise the possibility of alerting law enforcement in the event of a positive match (an occurrence that would raise important data protection issues).

Drones with visual payloads are also being deployed for monitoring large green areas in Zaragoza (Spain) in the framework of the Flying Forward project[1810]. The "Luis Buñuel" Water Park (120 hectares) is located in the Ranillas meander, next to the site of where the International Exposition of Zaragoza 2008 was held. Although the area is very busy at weekends, drone trials will preferably be carried out during working hours (Monday-Friday). When regulations will allow, the municipality of Zaragoza and the law enforcement department (including the fire department) will deploy two drones over the park: one will fly over the former Expo pavilions and the other over the green areas. Each drone will take off from a different location and will have a 500m radius flight zone. They will transmit images and information in real time to the advanced command post. The drone will start a prefixed flight route through the described area and will remain in stationary flight when it finds a person or vehicle, sending an audible warning and a video signal. Importantly, most activities will be carried out in-house by the municipality, with the exception of software development. Servers where data will be hosted are handled by the municipality internally as well, no cloud will be used. Data is mostly exchanged within the municipality.

Legal analysis. If we imagined that drones deployed by Zaragoza municipality were equipped with the facial recognition capabilities designed in Matera, a particularly intrusive system of surveillance would be in place. If it is difficult to justify the legitimacy of any of the previously mentioned surveillance technologies, the challenge magnifies when they are coupled with drones. Some of these tools are considerably intrusive in the first place (e.g., AFR, EFR, sensor tracking), and combining them with

[1808] Ferro et al (2020), p. 1.
[1809] Id., p. 2. Jammers are electronic devices capable of disturbing common communication technologies, GPS and radio-frequency signals.
[1810] See a detailed description of the project at Flying Forward 2020 (2022), pp. 40 ff.

flying drones would, in most cases, extend the scope of monitoring measures beyond what may be acceptable in democratic societies. It would be extremely difficult (if not impossible) to overcome proportionality issues raised by such initiatives, which could be labelled both as mass/hybrid or hybrid/targeted surveillance systems according to the kind of software embedded in the aircraft (e.g., EFR vs. AFR).

Preliminarily, it should also be observed that privacy expectations of citizens strolling in the park may impose a strict proportionality test on privacy and data protection interferences prompted by the initiative. Public spaces like parks and squares serve an important function as "privacy places" in cities, as described in chapter III. Especially in large areas like the Luis Buñuel water park, people may search for a remote place to wonder in their mental bubble, read a book, or share some affectionate moments with a friend or a partner.

Because the project is also meant to monitor massive events, it is not easy to understand why drones should be deployed during the week, and not during the weekends, which is when the park is most crowded and escalating situations may jeopardise public order. This evidently challenges the whole suitability of the initiative to reach the proposed objectives. In terms of strict necessity, information about past accidents should definitely be compiled if the project were to be implemented in real-word scenarios. Drones are prospected to detect – and attempt to identify – any individual present in their "sight range"[1811]. Imagining that this would happen even in the absence of a potentially dangerous situation, such processing could hardly meet the strict necessity requirements.

On the positive side, the little information provided seems to suggest that collected data should be subject to secure technical and organisational measures in both projects, which is something that could be taken into account in the strict proportionality test. Although nothing is said about the retention period, it can be appreciated that the data is kept in-house and not unnecessarily shared with other entities. Nonetheless, these measures alone may not be enough to reverse the balance of interests in favour of controllers/surveillants.

4. Environmental policing

Environmental data and predictive policing. Environmental data is certainly of great importance in smart cities, for instance, to track pollution levels and take informed decision on how to reduce them. Sometimes, however, data about the weather, lighting conditions, wind and alike are directly incorporated in decision-making impacting directly on individuals.

The personal nature of these data has been long debated. According to an extensive interpretation of the notion of personal data, "one could argue that "if the weather is going to be used to target and categorise me, I need protection against its potential to define me as dangerous or depressed, even if achieving this protection is difficult"[1812]. Nonetheless, applying standard data protection rules may not be straightforward when it comes to environmental data. On the one hand, one could imagine that asking information on the logic behind the use of weather data in automated decision-making would be possible. On the other, it appears to be difficult for data subjects to demand the erasure or rectification of data stemming from the environment and collected by sensors in a fixed infrastructure, and therefore not tied to any of their personal identifiers.

On a different level, maintaining public security is another important goal of smart cities, one that can be pursued also thanks to environmental data sources. Specifically, it is argued that this data can be used to make predictions about potentially dangerous situations and prevent the commission of

[1811] Id., p. 42.
[1812] Purtova (2018a), p. 75 (reporting a personal communication with Mireille Hildebrandt).

criminal offences[1813]. This trend seems to give rise to a new form of policing, i.e., *environmental (or sensor-based) policing*, as will be explained next.

Outline. Against this backdrop, this Section will analyse the novel features of predictive policing which draws on environmental data collected by IoT sensors. To this end, a general overview of predictive policing applications will first be provided[1814]. Afterwards, legal and ethical risks associated with traditional predictive policing tools will be highlighted[1815]. Lastly, the focus will shift to a particular environmental (or sensor-based) policing scenario. The example of the Stratumseind will be taken into consideration to understand in what way these initiatives bring new issues for individuals, and how data protection alone may not be enough to counter them[1816].

4.1. Overview of predictive policing applications

Artificial intelligence meets law enforcement. For many years now, AI has been faithful to the promise of revolutionising the field of law enforcement. As big data and machine learning techniques offer unprecedented insights into the patterns of criminal activities, they are leveraged not only to rationalise police departments' limited resources, but also to prevent the commission of crimes. The increased availability of data and digital technologies now allows law enforcement to undertake the greatest variety of surveillance activities, taking place either before or after the commission of a criminal offence. Undoubtedly, such data-driven initiatives fit into pre-existing trends highlighting an approximation of *preventive* and *reactive* approaches in criminal justice and security policies. Data referring to individuals with no connection whatsoever with ongoing criminal investigations are now fed into risk profiles informing the decisions of public authorities in the fight against more (and less) serious crime. Means of automated data processing – including those powered by AI – did nothing but accelerate these global changes.

Definition and iterations of predictive policing. Among the numerous applications of AI in the security domain[1817], predictive policing represents only one of the data-driven strategies tackling the manifold uncertainties of the urban environment. Predictive policing can be broadly defined as "any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention"[1818]. Different taxonomies of predictive policing have been put forward in the relevant literature. For instance, Perry et al. distinguish four different forms of predictive policing: (a) methods for predicting places and times of crimes; (b) methods for predicting offenders and identifying individuals likely to commit crimes; (c) methods for predicting perpetrators' identities; (d) methods for predicting victims of crime[1819].

Drawing on its history, Ferguson instead discerns three iterations of predictive policing[1820]. *Predictive Policing 1.0* software firstly targeted places of property crime, such as burglary, automobile theft and thefts from automobiles[1821]. The most notable example here is certainly CompStat, originally exploited by the New York Police Department (NYPD) in the 90s and later also adopted by the Los Angeles

[1813] See above Chapter I, §2.4.2.2.
[1814] See §4.1.
[1815] See §4.2.
[1816] See §4.3.
[1817] See generally González Fuster (2020).
[1818] Uchida (2009).
[1819] Perry et al (2013), p. 8.
[1820] Ferguson (2017a), pp. 1123-1142. Cf. also Hung et al (2020), p. 1.
[1821] Ferguson (2017a), p. 1126.

Police Department (LAPD)[1822]. In practice, the software entailed algorithmic processing of historical crime data – structured according to the three variables of time, place and type of offence – to predict probable areas of criminal activity (i.e., hotspots)[1823]. Interestingly, many predictive mapping applications were built following the so-called "near-repeat effect", a theory initially conceived in the field of seismology that later inspired criminologists in the analysis of burglaries' spatial patterns[1824]. Similarly to what happens with aftershocks of earthquakes, empirical research has shown how some property crimes often occur in a short time frame and close to the original crime scene[1825].

Predictive mapping was soon diverted to the fight against violent crime affecting particular urban areas. *Predictive policing 2.0* applications drew on the traditional hotspot approach but added newly studied factors to risk assessments of places around the city. Geographic vulnerabilities, lighting conditions, all sorts of deviant behaviour (i.e., drug and alcohol abuse), precursor crimes and temporal patterns were integrated in statistical analyses of the spatial incidence of crime[1826]. In this case as well, the theory behind the models echoed near repeat effect: like residential burglaries, gang violence tends to be territorial, but also retaliatory. This meant that violent crimes linked to gangs' rivalries were frequently concentrated in specific neighbourhoods and in tight times frames, which could be identified by the machine with appropriate accuracy.

Lastly, *Predictive Policing 3.0* software shifted their focus from places to individuals[1827]. These AI applications rely on vast datasets to pre-emptively identify individuals and groups that are likely to engage in serious criminal activities (e.g., connected to gun violence or terrorism). Historical crime data, including past offences and criminal associations, is used to build predictive profiles of individuals with a high propensity to offend. The models integrated in the software are often based on insights coming from the field of criminological studies, highlighting how certain environmental conditions, like poor socio-economic background or negative human connections, can play a role in the person's likelihood to commit criminal offences[1828]. Among individual-based predictive policing programs, the "Strategic Subject List" of the Chicago Police Department is probably the most prominent example[1829]. The algorithm analyses interpersonal connections in cases of gang violence to score the risk of an individual becoming a perpetrator or a victim of gun crimes. Another promising software is Beware, which provides real-time threat scores to police officers responding to 911 calls[1830]. The software searches the names of the people living at the given address and processes their publicly available data (e.g., social media) to assign a colour-coded risk level (green, yellow, red) to each resident. In this way, first emergency responders are informed of the kind of household they are going to intervene in.

Regardless of the possible classifications, predictive policing software today are varied in their uses and data sources employed. From a privacy and data protection perspective, one main distinction that seems worth keeping is the one between location-based (or crime mapping) and individual-based applications. While the former are focused on spotting high-risk areas, the latter aim to identify potential crime offenders, and should clearly be subject to data protection requirements.

As we will see next, even these categories are under stress in IoT environments, with the advent of another form of policing, i.e., "atmosphere" or "environmental" policing.

1822 On CompStat see Brayne (2017), p. 981; Ferguson (2017b), p. 195.
1823 Ferguson (2017a), p. 1126. Hardyns et al (2018), p. 205.
1824 Degeling et al (2018), p. 349.
1825 Id. See also Ferguson (2012), pp. 277-281.
1826 Ferguson (2017a), p. 1133.
1827 Ferguson (2017a), pp. 1116, 1137-1143.
1828 Id., p. 1137.
1829 On the Chicago "heat-list", see Ferguson (2017a), p. 1139; Degeling (2018), p. 350; Egbert et al (2020), p. 913.
1830 Degeling (2018), pp. 350-351; Ferguson (2017b), p. 196.

4.2. Surveillance and fundamental rights risks

Proprietary black boxes. There is a consistent body of literature focusing on the risks brought about by the increasing use of AI in society[1831]. One major issue surrounding any kind of automated decision-making regards the opacity of algorithms. Because models are often covered by trade secret and their functioning may not be clear even to specialists, it may be difficult to understand the rationale underpinning the processing and to trace back the logical steps leading up to a decision[1832]. That is why AI algorithms are commonly represented as "black boxes"[1833]. This lack of transparency may prevent parties involved from questioning the results of the algorithmic processing, in terms of both their accuracy and fairness, leading to broader accountability issues for the actors relying on AI technologies in their public or commercial activities.

Correlation and not causation. Because AI has syntactic and not semantic capabilities, algorithms can only find correlations between datapoints in large datasets[1834]. These correlations do not establish causal links between events, although the distinction may not always be straightforward to technology users. Algorithms' computational power to unravel unseen correlations may have a great potential in preventive policing, a realm that is mostly driven by intuition and experience, rather than proven facts. Some caveats are nonetheless necessary[1835]. For example, an algorithm may indicate that there is a strong correlation between speeding and drug trafficking. This may occur not because all speeders are drug dealers, but because police officers are more likely to find illegal substances in a vehicle searched after a violation of the road regulations[1836]. Besides, police officers may further reinforce the correlation if they keep limiting their searches only to speeding cars, thus contributing to the self-fulfilment of the algorithm's prophecy[1837]. That is why AI users need to be properly trained to avoid automation biases when confronted with decisions made by the machine.

Bias and non-discrimination. Another set of concerns relates to the data used as evidence basis for decisions. Data is expected to have an objective connection to the problem at stake, but this is not always true or verifiable in the big data paradigm. Data as models can be opaque to external scrutiny, which further undermines the transparency of the decision-making process. The outcome of the processing may also be questioned from the perspective of the *quality* of data that is used to draw inferences. In fact, data may not always be complete or accurate when errors are made during the collection and retention phases. These flaws are frequent in the drafting of police reports and management of criminal records, and they could be even magnified when analysis integrates commercial data[1838]. Acknowledging the limits of available data and establishing strategies to minimise errors in databases is thus crucial to achieve greater accuracy in the processing.

Issues of data quality notably have a direct bearing on fundamental rights such as privacy and data protection. The exponential growth of AI applications has been made possible not only by new computational capabilities, but also by the ever-increasing availability of data. In modern information societies, (personal) data collection is ubiquitous, thanks also to the advent of the IoT. Data-driven

1831 See generally Mittelstadt et al (2016), pp. 1-21.
1832 Kroll et al (2016), pp. 13-14, 23.
1833 The developers of XLAW argue on the software official website that their system actually works as a "white box", but this claim is not further substantiated.
1834 Mittelstadt et al (2016), p. 4.
1835 On the role of correlations in preventive justice see Caianiello (2021).
1836 Miller (2014), p. 125.
1837 Mittelstadt et al (2016), p. 9.
1838 Ferguson (2017a), pp. 1150-1153.

technologies are now leveraged in the field of criminal justice, and they are relying also on data repurposed from the commercial sector. If larger datasets fulfil the promise of delivering ever more precise predictions on future events, questions concerning the lawfulness or fairness of the data processing cannot be overlooked. Processing activities such as profiling may have a discriminatory impact on specific individuals and groups, sometimes amplifying already existing power asymmetries existing in society. In predictive policing, for instance, several studies have shown how biases embedded in inputted data or models can reinforce discriminatory stop-and-search practices of police patrols, who may disproportionally target people belonging to ethnic minorities or living in disadvantaged neighbourhoods[1839].

Beyond these general issues, the use of IoT environmental data in profiling the risk of criminality is raising new legal uncertainties. Critically, these may not be tackled by means of data protection only. In the next subsection, the most relevant problems will be highlighted through the example of the Stratumseind. Subsequently, a possible solution will be proposed at the intersection between data protection and criminal procedure safeguards.

4.3. Illustration

Scenario description. An example of environmental or sensor-based predictive policing is the *CityPulse* project in the SLL[1840]. This very busy, hectic street was filled with different sensors collecting data on sound levels, weather conditions, and combined with Wi-Fi tracking data, blurred video cameras and AI systems that perform sentiment analysis on social media posts tagging the Stratumseind. The goal of these systems is to look at anomalies in data patterns. For instance, they may single out individuals walking suspiciously down the street, but also profile the actual *atmosphere* in the street. Specifically, when the data point to a potentially dangerous situation, the regional police control room is alerted, and police officers receive notifications in a designed app, signalling four possible situations "nothing wrong", "everything alright", "backup needed", "high-risk situation". Where necessary, police patrols arrive on the pinpointed scene to de-escalate dangerous situations, prevent the commissions of crimes, or take necessary actions where a situation of flagrancy is encountered.

What type of surveillance? From a surveillance standpoint, data processing is clearly delimited to the area of the Stratumseind. Therefore, on the urban scale it resembles a mass/hybrid surveillance scheme, which is geographically and temporally circumscribed, but not subjectively so. It impacts on anyone coming into the focus range of the system. As previously shown, the use of such data would be permissible only in light of very strong public security reasons, which would include tackling serious crime, or preventing high risks to human integrity[1841].

It seems, however, that the *CityPulse* project (and the *De-escalate* one, as we will see next) was mainly directed at the prevention and repression of petty crime and mild disturbances to public order. From a proportionality standpoint, it would not be permissible for law enforcement to have direct access to footage and assessments made using emotion detection cameras installed in the street, nor to the data acquired through indiscriminate Wi-Fi tracking. This would allow them to directly identify and locate not only (allegedly) suspicious individuals in the streets, but also anyone in the street area with a Wi-Fi function active on their smartphones.

Against such intense interference on individuals' rights to privacy and data protection, the only way to justify these practices is arguably to have recourse to anonymisation and pseudonymisation

[1839] Brayne (2017), p. 1000. See also Browning et al (2020).
[1840] A detailed description of the project is provided by Galič et al (2021), pp. 4-5.
[1841] See Chapter IV, §3.4.2.

measures. Biometric and non-biometric data is not immediately examined by law enforcement, which only sees data at the aggregate level. De-anonymisation (e.g., in the form of de-blurring images or re-identifying individuals in Wi-fi tracking datasets) would be permissible only in very limited cases.

Of course, assessing the level of risk of specific situations leading to the commission of a criminal offence or other threats to public security is extremely difficult in the preventive context, when the negative event has not taken place yet. Accessing data thus seems a very delicate passage, one that is prone to risks of abuse. Therefore, while anonymisation and pseudonymisation is likely to tip the balance in favour of law enforcement objectives, the significant chances for (undue) re-identification cast a doubt on the compliance of such initiatives with EU fundamental rights.

Does data protection apply and how? Despite its non-binding nature, Recital 12 LED is clear in establishing the applicability of the Directive to data processing in preventive operations. This includes several situations where there is no investigation on a committed criminal offence, but the police is tasked with maintaining public order (e.g., demonstrations, major sporting events and riots). Nonetheless, the applicability of data protection law also depends on whether the employed systems actually process personal data. Here, different situations should be distinguished.

In traditional crime mapping software, the LED may not apply. Indeed, these systems process historic crime data, and their goal is not that of identifying specific individuals, but to spot *areas* where criminal activity is likely to take place[1842]. The case of individual-based predictive policing is also clear cut, where identification and profiling of a given individual is certainly intended; the LED should thus apply.

Things may get slightly more problematic in cases of environmental policing like the Stratumseind, where identification *may* (but not always) be intended. As argued by Galič and Gellert, the main goal of the whole project is not, in most cases, that of tracking specific individuals. Rather, it is that of managing them as a multiplicity, which makes identification often unnecessary. *City Pulse* is mainly aimed at profiling *atmospheres, situations* in the street, and environmental data certainly plays a role in building these profiles[1843]. For instance, patrols might be sent to a specific corner of the street where poor lighting conditions and high sound levels (caused, e.g., by yelling) may suggest that a riot is about to take place.

At the same time, however, there are cases where the individual will be directly profiled. For instance, somebody roaming alone in the street in bad weather conditions may be targeted as suspicious (e.g., he or she may be a drug dealer). In such cases, the attention of law enforcement will be already focused on one particular individual and efforts to re-identify him or her (with de-blurring or through Wi-Fi tracking) will likely be made. Here, data protection would arguably apply.

The hybrid nature of environmental policing. Therefore, environmental policing shares features with both location-based and individual-based predictive policing software. Certainly, the main goal of these software is to profile places and situations. At the same time, however, they also leave the door open to individual (re-)identification in specific instances, also thanks to the collection of non-environmental data like Wi-Fi data and (de-blurred) camera footage. The hybrid nature of environmental policing further stems from the fact that non-personal data is not simply used to "profile" spaces (e.g., crime hotspots like in *Predictive policing 2.0* software[1844]), but may also have an impact on individuals. If

[1842] See the analysis of Linskey (2019).
[1843] See Chapter I, §2.4.2.2.
[1844] See above §4.1.

environmental data can represent an incentive for law enforcement to re-identify certain individuals and thus interfere with their rights to privacy and data protection, these may have a right to know what role or weight that data play in assessing their dangerousness.

Indeed, there are situations where profiling the atmosphere could easily translate into profiling of the individuals involved themselves. As things stand, profiling about atmospheres and their dangerousness does not fall within the purview of data protection, as the processing does not immediately target individuals. However, taking into account the risk-level of the atmosphere that was profiled by the algorithm may challenge this assumption.

It can be argued that the more we move towards high-risk situations, the more identification may become the primary objective of law enforcement. As police patrols are asked to immediately intervene in such escalating scenarios, people involved will certainly be affected in the exercise of their rights to privacy and data protection. For example, they may be subject to questioning or stop and search.

Likewise, if the software intervenes with its assessment right before the commission of a criminal offence, the profiling arguably becomes more about individuals and their likelihood of passing over into actuality. In these cases, the link between the processing and the involved individuals could be too tight to exclude the applicability of certain data protection safeguards.

From atmosphere profiling to individualised suspicion. However, even if we admitted that certain data protection guarantees should be provided for, how could the people involved be protected against atmosphere profiling? Let us imagine that a police officer is notified of a high-risk situation (e.g., potential escalating fight) and intervenes immediately, for example by stopping and searching the people involved. The rights to privacy and liberty of these individuals would have been restrained *only based on how the atmosphere was profiled*. Of course, such interference may have been based on an erroneous assessment of the algorithm. What kind of data protection safeguards could therefore be applied here?

For instance, Art. 11(1) LED provides an important safeguard in this sense, enshrining the right not to be subjected to a fully automated decision:

> Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, *at least the right to obtain human intervention on the part of the controller* [emphasis added].

Applying it to this context, this safeguard could bar police officers from making any intervention impacting on individuals based uniquely on the output of the machine assessment. The problem here, however, seems that of applying an *individual safeguard* to a situation of *atmosphere profiling*.

Where data protection faces an impasse, criminal procedure safeguards may help understand what kind of protection could be provided for individuals in this case. We should remember that every kind of probabilistic evidence, such as the assessment made by the predictive machine bears some degree of generalisation[1845]. The same goes for the decisions made by police officers at the street level, like that of stopping and searching individuals involved in suspicious or escalating situations[1846].

Nonetheless, a difference between these two assessments should be highlighted. Compared with decisions made by the algorithms, those made by police officers should be more case-specific and tailored to the targeted individual, thus meeting a standard of *reasonable suspicion*[1847]. This safeguard

[1845] Berman (2020), p. 474.
[1846] Id.
[1847] Id., pp. 492-493.

would thus require a police officer to make an individualised assessment of the person's position, before proceeding to any invasive measure.

Nonetheless, criminal procedure safeguards may go even further. First of all, the acting police officer should identify the existence of facts and information that would satisfy the objective observer that a person may have committed, or is about to commit, an offence. As required by the ECtHR jurisprudence, however, this review may comprise an assessment of different elements. Indeed, the adjective "reasonable" also calls for a review of the *circumstances* (and therefore of the *situation,* or the *atmosphere*) in which the individual is positioned[1848]. These may have been labelled as dangerous by the machine but may not be so for the police officer according to different standards (even subjective ones).

Therefore, any action of police patrols triggered by the input of the *CityPulse* system would arguably demand a prior review of both the *overall situation* and the *individual position* of the people involved, as required by both data protection and criminal procedure safeguards.

Concluding remarks. The integration of environmental data in preventive operations is giving rise to a new and hybrid form of predictive policing, i.e., *environmental policing.* As in other smart environment initiatives, the applicability of EU data protection law is extremely volatile and contentious. Systems in the Stratumseind mainly focus on profiling atmosphere and situations, rather than individuals. Applying traditional data protection rights may not be entirely straightforward when it comes to data stemming from the environment. Nonetheless, people may still be in need of getting some form of protection against this new method of atmosphere profiling. Where this protection may not fully come from data protection, criminal procedure safeguards may come to the rescue. Echoing the right not to be fully subject to automated decision-making, the concept of reasonable suspicion may indeed be leveraged to argue for the need for a human review of the machine assessments with regard to both the escalating atmosphere and the individuals involved.

5. Smart nudging

Human rationality is not perfect. It is a given in behavioural science nowadays that humans make imperfect decisions. Already in the 1950s', Herbert Simon's concept of "bounded rationality" challenged the neoclassical idea of the *homo economicus* as a fully rational agent. In the 1970s, Daniel Kahneman and Amos Tversky further challenged this assumption in their seminal research on how people form judgements under uncertainty. They highlighted indeed how (i) humans tend to rely on heuristics and cognitive biases to minimise cognitive efforts, and (ii) such mental shortcuts tend to lead to suboptimal outcomes[1849]. Further on, the publication of Thaler's and Sunstein's book *Nudge* opened a rich and still ongoing debate on how policies and choice architectures should be designed to steer individuals to make smarter decisions[1850].

This novel knowledge about human behaviour is now widely leveraged by private and public actors alike. In particular, regulators and public administrations are increasingly relying on behavioural insights to formulate policies that are tailored to how people actually behave, not how they are assumed to behave[1851]. Indeed, nudging is often seen as a cheaper and more effective way of addressing social problems. Smart technologies have only incentivised the recourse to such techniques. As is widely

[1848] ECtHR, *Fox, Campbell and Hartley v. The United Kingdom*, judgment of 30 August 1990, App. nos. 12244/86, 12245/86 and 12383/86, §32. See also Vogler et al (2016), p. 193.
[1849] See e.g., Tversky et al (1981).
[1850] Ranchordás (2020).
[1851] Alemanno et al (2014).

known, large corporations today tend to leverage predictions about consumers' likely behaviour. They rely on big data and algorithms to extract meaningful patterns from data collected by diverse IoT sensors (e.g., smart fridges, movement patterns)[1852]. Likewise, smart city governments may exploit IoT solutions to improve how they make decisions and nudge citizens to overcome common biases.

Against this background, the following Section will investigate the role of nudging techniques in smart cities. While an analysis on overall nudging techniques in public regulation and economics goes well beyond the scope of this work, existing literature on the topic will be leveraged to provide a brief overview of the technology and key concepts, i.e., choice architectures and types of nudges[1853]. Some examples of how smart cities are using nudging to (allegedly) improve citizens' lives will then be given[1854]. Common legal and ethical concerns raised by nudging will be described[1855], but surveillance will be the primary focus of the analysis.

Lastly, the impact of nudging should always be assessed against practical examples/scenarios[1856]. On the one hand, the issues raised by the reuse of IoT data for nudging purposes will be examined[1857]. On the other, a notorious smart city project, *De-escalate*, will be outlined to highlight the manipulative side of nudging[1858].

5.1. Overview of the technology

5.1.1. Choice architectures and nudges

What are nudges? Cass Sunstein indicates that "[n]udges are interventions that steer people in particular directions but allow them to go their own way"[1859]. Examples of nudging are reminders, information campaigns, warnings, indications provided by a GPS, or default rules. A primary feature of a nudge is that it does not impose considerable material incentives or disincentives to make a particular decision[1860]. This excludes from the category of nudging binding measures like taxes, fines or jail sentences which are expressions of traditional command and control regulation. A particular striking example of nudging are default rules, i.e., what happens if you do nothing. For instance, the law of contracts is infused with default rules (e.g., automatic renewals of contracts), and so are many electronic devices that come with default settings. Many would consider default rules as disturbing, as they affect individuals' chances to organise their lives as they want. And yet, they often seem beneficial or even inevitable for human beings. Attention indeed is a scarce resource for humans. If applications for loans, educational opportunities, and refinancing mortgages were solely dependent of individuals' initiatives, a lot of money would probably be lost as a result of their inertia or procrastination.

What are choice architectures? The concept of nudging should also be considered in combination with that of "choice architectures". The design of places like cafeterias, supermarkets or websites impacts on how people choose[1861]. These architectures are unavoidable, whether we like it or not. Even if a

[1852] According to Kuang (2012) Google used behavioural economics techniques to encourage its employees to healthier choices in corporate offices. By rearranging the fridge with bottled water at eye level and soda at the bottom, the company achieved a water intake increase of 47% and soft drink consumption decrease of 7%.
[1853] See §5.1.
[1854] See §5.2.
[1855] See §5.3.
[1856] This methodological assumption is often stressed in Sunstein's work. See Sunstein (2015), p. 416. Of the same opinion are Cassese (2017), p. 244; Alemanno et al (2014), pp. 253-254.
[1857] Below, Sect. 5.3.1.
[1858] Below, Sect. 5.3.2.
[1859] Sunstein (2015), p. 417. See also McCrudden et al (2017), pp. 75-139.
[1860] Sunstein (2015), p. 417.
[1861] Id.

department store is not designed according to any logic, this will inevitably impact on whether shoppers will end up buying something or not[1862]. Nature itself nudges us. What the weather is like on any given day influences people's decisions, and we cannot certainly imagine our lives without some kind of weather[1863]. The State itself cannot avoid nudging. No system or goods (e.g., private property) could be protected if the public authorities refrained from doing anything to preserve them[1864]. For that reason, any country needs an "intelligently designed and continuously adjusted legal framework"[1865]. Since choice architectures appear inevitable in human life, Sunstein argues that it is pointless to reject them based on ethical grounds[1866].

5.1.2. Smart cities and nudges

Behavioural science and public regulation. Public law is not new to integrate behavioural models into its decision-making processes[1867]. Nonetheless, regulatory attempts drawing on behavioural studies have recently gained new and stronger traction. The basic assumption of this trend is that effective and efficient regulation should always consider how targeted people could respond[1868]. Cognitive sciences have changed our understanding of human behaviour, and this should also impact on how policies are defined and implemented. The reliance on behavioural techniques by private actors globally has only incentivised public administrations to exploit behaviourally informed regulatory strategies[1869]. These present themselves as low-cost and smarter alternatives to traditional binding measures, such as fines and bans[1870]. Compared to old methods of regulation, they also appear as choice-preserving, for they enable the addressee to opt-out of the preferred policy option[1871]. In this sense, nudging techniques have been labelled as "libertarian paternalism": while the State redesigns choice architectures in a paternalistic way to encourage citizens to make the most sensible choice, it also leaves them the ultimate decision on the matter[1872].

Some of the most widespread nudging methodologies in the field are (i) disclosure requirements, (ii) simplification, (iii) default rules (which have been already referred to). Disclosure requirements are not new to administrative law. What is new here is that behavioural insights now inspire regulators to understand how citizens process and use information to maximise the impact of a given regulatory tool[1873]. Also, simplification may facilitate participation and provide clearer messages to targeted groups about what they are expected to do[1874]. Indeed, some nudges are not meant to correct behavioural biases, but simply to offer additional information. This might be the case of communication nudges (e.g., reminders) and information-framing nudges (e.g., putting favoured options in bold letters).

Smart cities and nudging. Local authorities are experimenting with nudging to design places that encourage citizens to make more environmentally friendly decisions[1875]. Nudges here work as non-regulatory measures that influence individuals' behaviour through subtle and cheap manipulation of the

---

1862 Id., pp. 417-418.
1863 Id., p. 421.
1864 Id.
1865 Id. (citing Hayek FA (1943) Road to Freedom).
1866 Id., p. 422.
1867 Alemanno et al (2014), pp. 435-436.
1868 Id., p. 436.
1869 Id.
1870 Id.; Ranchordás (2020), p. 259.
1871 Alemanno et al (2014), p. 436.
1872 Id., p. 438; Ranchordás (2020), pp. 257, 260; Gandy et al (2019), p. 2113.
1873 Alemanno et al (2014), p. 438.
1874 Id.
1875 See Gandy et al (2019); Glowacki (2016); Ranchordás (2020), p. 255.

environment[1876]. They encourage individuals to defeat their cognitive biases that could lead them to make irrational choices, like walking through an unsafe neighbourhood or being reckless in energy consumption. Relevant examples may include efforts to inform consumers about how their energy use compares to their neighbours'[1877], setting green energy programmes as a default rule[1878], or nudging individuals' behaviour in public streets through lighting adjustments[1879]. The city of Boston, for instance, has introduced the "Boston safest diver" smartphone app, which gives feedback on driving based on speed, acceleration, braking, cornering, and phone distraction[1880].

Some argue that the use of nudging techniques clearly fits into the paternalistic mission of smart cities[1881]. Regulators are relying on top-down approaches, trying to steer inert or deviant citizens towards healthier and more sustainable decisions. In a sense, nudging is also coherent to more experimental approaches to the smart city, which sees citizens as informed-decision makers who are involved in the management of urban goods. While promoting collective welfare, however, these processes do not seem to adequately commit to democratic participation, fairness, justice and transparency[1882].

5.2. Legal and ethical risks

Democratic legitimacy, rule of law, accountability. Because nudging impacts on the human decision-making process, it engages different fundamental rights and calls into question the rule of law itself. Ranchordás explains that nudging is underpinned by an asymmetrical kind of power that, differently from traditional state interventions, is not counterbalanced by democratic checks and balances. These techniques may indeed be designed by public officials, behavioural teams or private companies, with little or no participation of the citizenship.

Given the lack of coerciveness of nudging, it is also difficult to frame these interventions within the typical instruments of administrative law. This poses problems with respect to the principle of legality and accountability[1883]. While the scope of any act by public administration needs to find a basis in the law, behavioural informed strategies are not formed through strictly predefined and circumscribed processes[1884]. Identifying public bodies (e.g., the parliament, regulatory oversight authorities) that should authorise nudging by the government *ex ante* may be equally difficult[1885]. On the *ex-post* side, the informal nature of nudging hampers the quest for effective remedies[1886], starting with the identification of competent judges on the matter.

Privacy and data protection. While most data collected in smart cities is considered non-personal, the risks of re-identification of individuals are always around the corner. Drawing on data collected by IoT sensors, data-driven nudges may become as intrusive as other forms of regulation, especially if they rely

[1876] Ranchordás (2020), p. 257.
[1877] Rasul et al (2012). Notable examples include the cities of Sacramento, Sheffield and Johannesburg, see Ranchordás (2020), p. 264.
[1878] Sunstein (2015), p. 427.
[1879] See §5.3.2.
[1880] Ranchordás (2020), p. 264.
[1881] Id., p. 255.
[1882] Iaione et al (2019).
[1883] Alemanno et al (2014), pp. 449 ff.
[1884] Id.
[1885] Cassese (2017), pp. 244-245.
[1886] Id. See also Alemanno et al (2014), p. 452.

on discriminatory profiling[1887]. Of course, these practices pose varied issues from a privacy and data protection perspective. A first concern regards the legitimacy of the data collection: is it necessary and proportionate to the nudging goal? The same goes for data reuse: if the data was collected for a different objective, is the repurposing of such data proportionate? Also, are recommendations based on data fair and non-discriminatory? If most nudges are most effective when hidden[1888], how can the principle of transparency of the processing be upheld?

Autonomy and manipulation. The question of autonomy is also strictly connected to privacy [1889]. With respect to this issue, the impact of nudging may be ambivalent. Sunstein believes that only some kinds of nudging intrude on autonomy[1890]. In some cases, indeed, nudges may even promote autonomy[1891]. If agents need to be informed to make autonomous choices, informative interventions may provide people with a better understanding of the facts and correct their biases[1892]. It can also be argued that autonomy does not require active choosing *anytime*. People have intellectual and time constraints, and they should prioritise their attention to the most deserving matters. That is why they should be put in a position where they can focus on the most pressing issues. For instance, this might be topical where daily life is often hectic and citizens do not always dispose of the time and resources to make fully reasoned decisions, e.g., about which path or means of transportation to take.

The case of nudges that exploit people's behavioural biases and resort to manipulation is different. When nudging perverts the way people reach their decisions, and form their preferences, then their autonomy is most likely intruded upon[1893]. Manipulation indeed occurs when individuals' rational decision processes are subverted, primarily in the following ways: (i) pressure to acquiesce, (ii) playing up emotions, (iii) emotional needs or weakness, (iv) deception[1894].

For instance, in behavioural science it is now standard practice to discern between two categories of cognitive operations: on the one hand, there is "*system 1*", which is fast, automatic and intuitive, and often associated with cognitive failures; on the other, "*system 2*" which is slow, calculative and deliberative. Nudges providing information disclosure try to strengthen *system 2*, while countering more impulsive actions stemming from *system 1*. On the contrary, interventions that are usually labelled as manipulative appeal directly to *system 1* and operate at a sub-conscious and non-rational level, which arguably makes them more insidious than more overt forms of coercive regulation[1895]. Specifically, nudges that play with emotions are particularly dangerous when appeal to our irrational selves (e.g., subliminal messages) is not recognised by our rational part[1896].

Freedom of thought and expression. The way in which nudging leverages our cognitive failures also engages our freedom of thought and mental privacy. As explained with respect to emotion recognition technologies, emotions have cognitive features that make them very similar to thoughts themselves[1897]. Therefore, any nudge that exploits our instinctive and emotional behaviour can be said to intrude upon the freedom of thought, extensively interpreted as inclusive of the right to form, express and keep our

[1887] Ranchordás (2020), p. 266.
[1888] Id., p. 268.
[1889] On the relationship between the right to privacy and autonomy, see Chapter III, §2.1.1.
[1890] Sunstein (2015), p. 438.
[1891] Id., p. 237. See also McCrudden et al (2017), p. 113.
[1892] Sunstein (2015), pp. 437-438.
[1893] McCrudden et al (2017), p. 112.
[1894] Id., p. 113.
[1895] Id., p. 114.
[1896] Id., p. 116.
[1897] Above, Sect. 2.3.2.1.

emotions to ourselves. Likewise, government's attempts to use information tools to affect citizens' behaviour (i.e., anti-smoking campaigns) have been considered to interfere upon the freedom of expression because they shape the cognitive environment in which individuals are provided information[1898]. When such campaigns concern socially and politically divisive matters (e.g., abortion, nuclear energy), the line between information campaigns and government propaganda may also become quite blurred[1899].

Having considered the basic features of nudging and its fundamental rights risks, the following sections will attempt to apply these insights to two specific case scenarios of "smart nudging", that is nudging techniques relying on data generated by IoT devices.

5.3. Illustrations

Defining the terms of the analysis. As outlined above, nudging poses a great variety of issues. In this investigation, nudging strategies will be assessed mainly from a surveillance perspective. Therefore, the issue of the legitimacy of nudging itself will not be handled here[1900]. In performing a legal analysis, the rights to privacy and data protection, as well as the freedom of thought, will be considered as relevant benchmarks. Two different scenarios will be analysed: on the one hand, a case where data collected for specific purposes (e.g., commercial, public service) is repurposed to nudge citizens; on the other, a specific nudging project in the Stratumseind, *De-escalate*.

Does nudging interfere in fundamental rights? At the outset, both scenarios involve an interference with the fundamental rights at stake. Indeed, any government action should sustain a burden of justification[1901]. The informal and non-coercive nature of nudging, however, has often led interpreters to exclude that such techniques actually intrude on the right to privacy, data protection and the right to expression. Yet, others have argued that the influence and persuasion exercised by nudging are "no less restrictive" than coercive regulation. These interventions do intrude upon citizens' choices, occasionally manipulating their freedom[1902]. Therefore, nudging represents a new form of regulation, although it may come across as "gentler"[1903].

Despite this acknowledgement, it is difficult to frame the *intrusiveness* of different nudges. Indeed, with respect to the means, the non-binding nature of these measures may exclude that the interference at stake is serious, and that it should be subject to a strict proportionality test. A different interpretation may be put forward if one looks at the "privacy zone"[1904] that is affected by nudging. Because these strategies tend to impact on our most private zone, touching upon our mental and decisional privacy, nudging may also be regarded as very intrusive. Other criteria that should be taken under consideration may include the *place* in which the nudging is taking place (e.g., a public venue). But ultimately, this assessment should be made by the interpreter on a case-by-case basis, as we will see further on in the analysis.

5.4.1. Repurposing for nudging

Scenario illustration. Smart nudging can draw on a plethora of sources. Static, dynamic data (predictions, real-time data) stemming from infrastructural sensors, crowdsourcing initiatives, and third

[1898] Alemanno et al (2014), p. 446.
[1899] Id.
[1900] On this, see the opposing views referred to in Sunstein (2015) and McCrudden et al (2017).
[1901] Sunstein (2015), p. 415.
[1902] Cassese (2017), p. 243.
[1903] Id., p. 244.
[1904] See Chapter III, §2.2.2.

parties can all be integrated in an IoT architecture for nudging purposes[1905]. Often, these data may not have been collected with the ultimate goal of steering citizens toward sensible choices, e.g., environmental-friendly behaviour. On the contrary, different actors can reuse data belonging to pre-existing datasets (like data about the traffic or the user) that are formed and continuously updated by private actors. The reuse of these sources in the public context for environmental nudging can thus put a strain on the principle of purpose limitation. Citizens that have consented to specific data processing operations through their smartphone apps or are aware of data collection within public service delivery, may not anticipate that the same data can be used by public authorities to influence their behaviour in different situations. Therefore, their privacy expectations may be high with regard to this processing.

Issues of data repurposing are potentially raised in a smart nudging architecture implemented in Norway (i.e., NUDGE project) to incentivise green transportation choices (hereinafter: "green nudging")[1906]. The project will be taken as a relevant scenario to assess the legitimacy of data repurposing for green nudging purposes. Further variables will also be introduced to understand how the assessment could be attuned according to different circumstances.

Legal basis. Any data repurposing entailing an interference with the rights to privacy and data protection needs to find a basis in the law, if not based on consent, or on a case-by-case assessment by the controller. The Regulation indicates that data reuse should be authorised by a national or EU law that constitutes a necessary measure in a democratic society for any of the objectives pursuant to Art. 23 GDPR. Among these, we find "important objectives of general public interest of the Union or of a Member State" (Art. 23(1)(e) GDPR), a formula that recalls the requirement of a general interest under Art. 52 CFREU.

Although the requirement of the legal basis is often straightforward for the interpreter, this is not the case for smart nudging involving data reuse. In this case indeed, nudging is not only the output of the data processing, but can also assume significance as an act of the public administration. Within the purview of administrative law, arguments have been made to enhance the legal significance of the *single* nudge[1907]. Even if the nudge does not have a coercive nature, it can nonetheless be a harbinger of worrisome consequences for individuals. Surely, context is crucial in this regard. Nudges that go beyond the provision of additional information and may involve reputational damage for citizens, could be equated to actual administrative acts that should be accompanied by the relevant safeguards[1908]. At the same time, the data processing underlying the smart nudge should also be supported by a legal basis, as mentioned above.

Against this background, the requirement of the legal basis should comply with both data protection and administrative law requirements, although this poses different questions. For instance, should the nudge be grounded in two separate legal bases, one framing the processing, and the other the action of the public administration? Or should the legal basis for the processing also serve as an *ex-ante* authorisation to nudge for public authorities?

The answer likely lies in the legislative technique chosen to introduce the smart nudge. A unique legal basis may favour accessibility and foreseeability for citizens, but different solutions cannot be excluded. From a data protection perspective, moreover, we should also consider that the GDPR does not always require an explicit legal basis for data reuse. In fact, it also foresees the possibility of

[1905] Andersen et al (2018), pp. 338-339.
[1906] See Andersen et al (2018).
[1907] Alemanno et al (2014), p. 454.
[1908] Id., p. 453.

repurposing data based on a multi-factor assessment. For public authorities, this possibility may be open only for repurposing according to a legitimate interest (e.g., pilot projects), while it may be barred where data reuse should be based on a legal obligation or public interest. In these cases, Art. 6(3) should indeed apply and an additional legal basis should ground the repurposing.

General interest. In the case at stake, smart nudging is essentially aimed at ensuring the preservation of the environment, by means of incentivising green choices in terms of transportation. Generally speaking, the EU is committed to ensure a "high level of protection and improvement of the quality of the environment" (Art. 3 TEU). Thus, the preservation of the environment certainly qualifies as an objective of general interest which may legitimise an intrusion upon fundamental rights, as long recognised by the CJEU[1909].

The goals of environmental protection might assume several forms in the smart city. In the scenario at stake, there would not be any situation of emergency threatening the very integrity of the environment, something that would likely legitimise a more serious interference with the rights to privacy and data protection (i.e., under the heading of national security)[1910]. Here, indeed, non-coercive measures like nudging would not even comply with a suitability requirement under a proportionality test. The non-binding nature of nudging would not probably be suitable to overcome the emergency situations brought by such environmental threats. Instead, what is arguably at issue in the case of green nudging is an objective of (mere) *optimisation* of resources, and thus of improvement of the quality of the environment. Such a "lighter" purpose may thus legitimise non-binding measures such as nudging, which leave the ultimate choice to the individual targeted.

Essence of the rights at stake. This leads us to another issue to be assessed with respect to the legitimacy of nudging. Is the core essence of the rights to privacy, data protection or freedom of thought irremediably compromised by green nudges such as the ones from the app under examination? If nudges were designed as simple informative ones providing additional data on the greenest choice to make, it could be characterised as an intervention on the so-called "*system 2*" of our cognitive skills. That would be the case especially if the app at the same time displayed alternative paths, thus presenting different alternatives.

Therefore, it may be argued that such kind of non-manipulative nudging may not compromise the essence of the rights at stake (especially our decisional privacy and freedom of thought), understood as our capacity to reach cognitive conclusions autonomously. Nudges that preserve the core of our autonomy (seen as the second-order capacity to critically reflect on our first-order preferences and desires) can arguably be respectful of our individual dignity.

A different conclusion may be argued for if, however, nudge were built with deceptive information-framing techniques, which would trigger unreasoned and impulse decisions as to which means of transportation to take. This would probably undermine individual dignity, understood as the essence of fundamental rights in the Charter.

Admittedly, this analysis takes into account a "narrow" conception of "dignity-as-autonomy", entailing the respect of people as rational human agents[1911]. This outlook "saves" the legitimacy of nudging under the assumption that nudging is not coercive and leave the ultimate choice to the targeted persons. Although this is certainly a simplistic perspective to assess the legitimacy of nudges altogether,

[1909] See inter alia CJEU, *Procureur de la République v Association de défense des brûleurs d'huiles usagées (ADBHU)*, judgment of 7 February 1985, Case C-240/83, §§13, 15; CJEU, *Commission v Belgium*, judgment of 9 July 1992, Case C-2/90, §32.
[1910] See Chapter IV, §3.4.2.3.
[1911] McCrudden et al (2017), p. 109.

it may serve as appropriate standard to evaluate whether the *essence* of fundamental rights is touched upon.

Proportionality. Data repurposing should also satisfy a proportionality test (Arts. 6(4) GDPR and 52 CFREU). This principle should be assessed against the objective of environmental protection that is pursued. As mentioned above, achievable degrees of environmental goals are possible[1912]. The higher the level of protection sought, the stricter the measures allowed will be[1913]. Historically, the CJEU has treated the objectives of environmental protection favourably, accepting collaterals on trading in the internal market[1914]. Thus, the control has often been "limited to assessing whether the measures adopted [were] *manifestly inappropriate* for achieving the objective pursued"[1915].

In the case at stake, green nudging in a transportation scenario may not pose great challenges from a proportionality perspective. The objective pursued by the measure is indeed one of resource optimisation and *improvement*, and is not immediately linked to natural disasters or other emergency situations undermining the very survival of the environment itself. First of all, non-binding measures like green nudges may in themselves be suitable to achieve this "subtler" kind of goals. To be truthful, however, this requirement may raise some issues when looking at the factual efficacy of nudging. Indeed, research has shown that nudging may often be more impacting with individuals or households that share the ideas the nudges want to steer them toward in the first place (as in the case of environment-friendly behaviour)[1916]. The efficacy, and thus suitability, of the nudging initiative should likely be assessed in a testing environment (e.g., regulatory sandboxes) that can give indications as to whether the measure is suitable to the objective pursued.

Secondly, strict necessity should be evaluated. As indicated by the EDPS, this should be a fact-based assessment: the controller needs to present objective evidence showing that there is no less invasive way to achieve the objective pursued. In the case at stake, this would include *inter alia* the failure of other traditional informative campaigns on the importance of public transportation and green choices. With specific respect to the data to be repurposed, the controller would need to demonstrate the importance of the datasets to be fed to the system to achieve personalised and effective green nudges[1917].

Lastly, proportionality *stricto sensu* should be checked. The provision of data protection safeguards (e.g., pseudonymisation, data security) is certainly one of the factors to be taken into account in the balancing test. The nature of the data (whether sensitive or not) is also relevant, although this is an increasingly difficult element in assessing big data environments. Furthermore, the context in which the data has been collected and the one in which data should be repurposed are also to be taken into account.

It has often been mentioned in the course of this work that data reuse (even of those collected within the private sector) in the public domain is generally viewed favourably by data protection authorities, that tend to apply a lighter approach in such cases[1918]. Arguably, this may play out favourably in the situation at issue, where the repurposing is operated by public authorities for a public interest objective. Lastly, the possible consequences for data subjects are also important. Different

[1912] Cf. also Jacobs (2006), p. 194.
[1913] Id., p. 195.
[1914] Id., p. 196.
[1915] Id., p. 197.
[1916] Rasul et al (2012); Ranchordás (2020), p. 258.
[1917] On the importance of personalisation in smart nudging, see Andersen et al (2018), pp. 335 ff.
[1918] See Chapter IV, §3.4.2.3.

scenarios might be taken into consideration here. If, as in the initial illustration, the nudge retains its non-coercive nature, it might be considered proportionate to an objective of resource optimisation. However, we may not reach the same conclusion if binding or reputational consequences were attached to an individual's decision not to follow the suggested path. We can imagine instances where following the nudge may be reconnected to positive points in a credit scoring system designed for the citizen. Even worse, non-compliance may also be leveraged by public authorities that exclude non-virtuous citizens from subsidies or other public services. Such negative consequences may tip the balance against the overall legitimacy of the depicted green nudging initiative.

5.4.2. Manipulative nudging: *De-escalate*

Scenario illustration. De-escalate was a sub-project of the SLL. Researchers at the technical University of Einhoven and Philips developed smart lighting system with the aim of affecting and diffusing escalated moods and behaviour in Stratumseind street. The system ran from 2014 to 2018, in partnership with the Eindhoven municipality, the police, and smaller local technology companies.

De-escalate was presented as an intelligent lighting system that could control emotions[1919]. The technology was based on psychological research postulating that escalating behaviour can be neutralised with exposure to dynamic lighting. For instance, psychology literature indicates that dim and warmer colours can be linked to lower arousal and pulsating orange lights can relax breathing rhythms in humans[1920]. Bright light environments can strengthen people's self-awareness and steer them toward better self-regulation, while darkness can trigger feelings of anonymity and deviate behaviour[1921].

In the Stratumseind environment, people were profiled to find out what prompts aggressive and escalating behaviour. Data from past incidents were analysed, as well as open data and social media data. Data mining techniques were used to find correlations between potential stress factors and escalated behaviour (e.g., weather or football matches)[1922]. These predictive insights were then integrated into the dynamic lighting system, with the purpose of managing public lighting in such a way as to keep stress levels at acceptable levels (although this standard was not further defined)[1923]. As things stood, the *De-escalate* project was labelled as a true nudging tool, aimed at influencing people's behaviour[1924].

Legitimacy. It is not a straightforward matter to assess whether the projects connected to the SLL (including both *CityPulse* and *De-escalate*) were "in accordance with the law". At the outset, the requirement of a grounding legal basis seemed to pose even greater challenges than in the previous scenario. From a data protection perspective, the personal nature of the data collected in the Stratumseind has been long debated[1925]. Although the personal nature of environmental data gathered in the street can be easily excluded, the same does not apply to location data acquired through Wi-Fi tracking and blurred video footage. Despite the applied aggregation and video-blurring measures, such data can arguably be exposed to re-identification and their initial processing should comply with EU data protection requirements.

[1919] Galič et al (2021), p. 5 (citing de Kort Y (2014) Spotlight on Aggression. ILI, p. 10).
[1920] Id.
[1921] Id.
[1922] Id., p. 6.
[1923] Id.
[1924] Id.
[1925] See Galič et al (2021) for a more restrictive approach and Purtova (2018) for a more extensive one.

Specifically, different legal bases could ground the processing operations, depending on whether we consider them to fall within the scope of the GDPR or the LED. Law enforcement objectives seem to be the dominating ones in the project, but research purposes should also be considered given the experimental nature of the initiative. In addition, some Member States (such as the Netherlands) seem to apply the GDPR to processing referring to general tasks of maintaining public order, which arguably includes preventive operations such as in *De-escalate* and *CityPulse*.

If the LED applies, data processing in the Stratumseind should be grounded on an additional legal basis pursuant to Art. 8 of the Directive. The same would be required if the processing was based on a public interest under Art. 6(1)(e) GDPR. Within the national system, it is however not clear whether data processing operations in the Stratumseind were adequately grounded on a foreseeable and accessible law. The living lab was set up by the municipality of Eindhoven, and the De-escalate project was implemented based on a call published by the Dutch Research Council (NWO)[1926]. The legal bases grounding these projects could have embedded an authorisation for data processing for public purposes, and thus integrate the requirement of the additional legal basis under Arts. 6(3) GDPR and 8 LED. Indeed, both the Regulation and the Directive allow for a wide range of legal instruments to serve as a basis for the processing (and not only acts of the parliament)[1927]. Nonetheless, if law enforcement goals are considered as underpinning the project, such legal bases should specifically include "the objectives of processing, the personal data to be processed and the purposes of the processing"[1928].

Secondly, the processing entailed within the pilot project could be based on a legitimate interest (Art. 6(1)(e) GDPR). This option encounters some difficulties, however. Indeed, the processing in the Stratumseind is actually meant to heavily impact on fundamental rights, as data subjects may be limited in enjoying the public space and could potentially be targeted by law enforcement. The Working Party indicates that broader emotional consequences and the chilling effects of pervasive surveillance should be evaluated in the balancing test between data subjects' rights and controllers' legitimate interests[1929]. In light of the seriousness of these risks, it is difficult to argue that the balance should tip in favour of the controller both in the contexts of *De-escalate* and *CityPulse*. Also, the diminished foreseeability of Art. 6(1)(f) GDPR may suggest that such interferences should preferably be based on public interests or law enforcement processing legal bases, which may be stronger in terms of foreseeability.

Essence of the rights at stake. Another issue to determine is whether the nudging interferes with the essence of the rights at stake. Differently from the previous case, the technology put in place in *De-escalate seems* to be designed to trigger our most immediate impulses. With dynamic lighting scenarios, it aims at generating non-rational responses, e.g., pushing people to abandon certain zones or angles of the street. In other words, it is arguably built to appeal to "*system 1*" of our cognitive system, in a way that seems to intolerably restrain people's ability to reach reasoned conclusions as to how to behave and move within the public space. For this reason alone, it can be argued that a system like that of *De-escalate* may touch the very essence of the rights to privacy and freedom of thought and should thus be rejected under EU human rights law.

Proportionality. With such an assessment on the essence of the right criterion, we should not even attempt to perform a proportionality test. In this case, nevertheless, different issues that may arise

[1926] See https://www.nwo.nl/en/projects/314-99-112-0. Accessed 16 June 2022.
[1927] Recitals 41 GDPR and 33 LED.
[1928] Art. 8(2) LED.
[1929] Article 29 WP (2014b), p. 37.

under this perspective will be presented as well, in order to reinforce previous arguments on the illegitimacy of systems like *De-Escalate*.

Such an initiative is undoubtedly put in place to pursue security-related objectives, which are considered objectives of general interest under EU law and the ECHR. What kind of interference may however be justified in light of such goals? At the outset, it should be considered that smart policing initiatives in the Statumseind were explicitly introduced to tackle petty crime (e.g., fights, thefts, dealing of small drug quantities) and deviant behaviour in general (e.g., drunkenness). Pursuant to the strict necessity principle, it seems difficult to justify such a serious intrusion upon fundamental rights and individual autonomy based solely on purposes of petty crime reduction.

Furthermore, it appears arduous to calibrate interferences in the De-escalate scenario. As highlighted, the guidelines of the project do not seem to define what should be understood as "acceptable behaviour". Thus, what kinds of deviant behaviour require an intervention by the system? Who is in charge of determining how people should behave in the public space, when individuals' actions may be considered "deviant" or "dangerous" but are not criminally or administratively sanctioned? These questions show a clear problem of foreseeability in the operationalisation of the system, which does not even allow a decision to be made beforehand about when it could be proportionate to nudge people according to the situation at stake.

Lastly, it can be argued that a proportionality *stricto sensu* assessment should also take into account the context in which the nudge occurs. Specifically, it should be examined whether the nudge/output of the processing ought to be "broadcast" in the public environment, or whether this is directed only to specific people that have subscribed to a pre-designed app. In the former scenario, a stricter approach would probably be required, as the nudge is likely to have a broader reach and impact on the fundamental rights of a multiplicity of people. Indeed, the fact that a "public nudge" could introduce a constraint on the use of public places and services should also be regarded as critical, considering the high expectations of privacy surrounding smart public environments[1930]. In the case of *De-Escalate*, the nudging system is potentially aimed at an indeterminate variety of subjects in the public space, which puts an additional strain on the proportionality of this initiative with respect to fundamental rights.

Concluding remarks. Two illustrations of smart city nudging based on real scenarios were presented. The legal analysis revealed different possible outcomes in terms of the legitimacy of such initiatives in the urban environment. A common issue appears to be the difficult applicability of the requirement of the prior legal basis for nudging by the public administration. Secondly, the distinction between non-manipulative, and thus permissible, kinds of nudges may not always be clear-cut. This makes assessment of the respect of the essence of the right criterion under Art. 52 CFREU difficult to evaluate. In this respect, varied scenarios were illustrated in order to show how contingent variables may affect the proposed solution.

Even the outcome of the proportionality test is affected by multiple factors. Firstly, we can observe that environmental objectives are treated quite favourably by jurisprudence and may justify a broad range of interferences with fundamental rights. The same cannot be said for law enforcement objectives. As seen in Chapter IV, both the CJEU and the ECtHR have introduced a more granular distinctions between security-related goals and attributed a minor weight to the fight against (serious) crime. Because nudging techniques often introduce serious interference with the rights to privacy, individual autonomy and freedom of thought, it appears difficult to justify such intrusions for the mere detection of petty crime, as in the case of the Stratumseind.

[1930] On the value and expectations of privacy in public environments, see Chapter III.

6. Interim conclusions

In this chapter, different instances of surveillance applications in smart cities were analysed. Traditional proportionality assessments have been enriched with additional evaluations on privacy expectations and types of surveillance systems put in place by such initiatives. These factors, stemming from the research carried out in Chapter III and IV, are meant to achieve more granular and fine-attuned legitimacy assessments of surveillance technologies, according to a more precise methodology that is arguably lacking at the moment.

Specific conclusions as to the legitimacy of the examined applications can be found in the dedicated sections. Nonetheless, some general considerations can also be made at this point. The development of smart cities is underpinned by a broad variety of objectives, among which law enforcement, commercial and environmental ones.

Different weights can be attached to such goals. Generally speaking, the jurisprudence looks favourably at environmental aims, which could justify extensive data collection regimes, provided that these do not simply pursue resource optimisation purposes. Security objectives also play an important role, but surveillance regimes in this domain should be more strictly assessed in light of their sensitive implications for data subjects. Commercial monitoring activities in public places, on the other hand, do not seem to bear the same weight and may not justify very serious interferences with fundamental rights.

These applications may however ground data processing when the goals pursued reach a "collective" dimension and are connected with strong data security measures (e.g., use of EFR-equipped billboards in public squares or railway stations, data collection linked to the protection of critical services). Of course, such different interests can legitimise different types of surveillance in terms of scope. Therefore, a prior assessment of the kind of monitoring system at stake (according to the taxonomy proposed in Chapter IV) could help achieve more fine-attuned evaluation.

Overall, the proportionality assessments here proposed are meant to overcome dystopian narratives arguing for a blanket rejection of any kind of surveillance in urban environments. This does not mean, however, that all iterations of surveillance can be acceptable in democratic societies. For instance, covert or non–consensual instruments that manipulate and objectify cognitive states can be seen as touching upon the very essence of different fundamental rights, and thus be rejected within the European system of human rights.

VI. Data Governance and Surveillance in Smart Cities

1. Introduction

Smart cities, governance and surveillance. So far, what has emerged from the analysis is that handling data in smart cities always comes down to a question of balancing. Indeed, there are now diverse actors that participate nowadays in running cities and just as many objectives underpinning their strategies. Private companies follow their corporate agenda and see the city mainly as investment opportunity. Individuals look to preserve their fundamental rights with regard to invasive data practices. Public entities are bound by law to pursue public interest goals, possibly improving life standards in the city. Overall, smart cities can be seen as a unique stage for regulating competing interests in the digital era.

Arguably, any way we choose to balance and govern such interests is likely to impact differently on people and society as a whole. Different ways of governing data also have a bearing on surveillance. Indeed, governance of collective issues requires collecting knowledge on such relevant phenomena, and different ways of governing can also entail different models of surveillance. On its side, surveillance also embeds the balancing of opposing interests, i.e., those of the surveillants (public authorities, corporate agents) and those of the surveillees.

Two main outlooks of governance (and surveillance) currently compete in the data domain. The dominant market-led model of data governance is often associated with reckless data practices (e.g., targeted advertising, discriminatory profiling), which roughly go under the umbrella term of "surveillance capitalism"[1931]. On the other side, a set of pilot projects and alternative visions are trying to challenge the assumptions of the prevailing ideal, by proposing schemes centred on control over data by communities and the value of common good. These models seem to envision mitigated frameworks of surveillance, as they aim to circumscribe the number of entities that can have access to data, and thus curb uncontrolled data repurposing. Importantly, these outlooks have also inspired different visions of smart city governance.

EU data governance: Which way to go? EU institutions are now standing at the crossroads of these two possible data governance models. In the 2020 European Data Strategy, the Commission outlined ways in which the European society could make better decisions and improve its welfare through digital data resources[1932]. Is also launched a series of legislation that will shape future EU data governance. Among these, the Data Governance Act, the Artificial Intelligence Act and the Data Act are certainly the most relevant to the purposes of this analysis. While the project is ambitious, it certainly betrays contradictory views of how data governance should be implemented in the EU, mixing both common good narratives and elements of the dominant data economy model. As a result, there emerges a set of fragmented mechanisms through which public and private interests should be balanced in the governance of data. Against this backdrop, this chapter will investigate the following sub-research question: *Which data governance frameworks can most mitigate the impacts of surveillance in smart cities, ensuring a fair balancing of public and private interests in the urban sphere?*

[1931] See Chapter IV, §2.2.

[1932] European Commission (2020) Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A European Strategy for Data. COM (2020) 66 final.

Outline. To answer this question, an overall picture of what data governance is and what it entails will firstly be outlined. This account will also briefly touch upon the (social) nature of data, which has been differently characterised according to the objectives pursued by competing data governance models. While the topic of data governance is in itself extremely broad and embeds several legal, ethical and societal questions, the analysis will mainly take a surveillance perspective. Therefore, it will cover how data is conceived in governance, and which norms regulate who can access data and for what purposes. With this focus, the two main models of data governance and their specific implications in the smart city context will be presented. Subsequently, the inquiry will shift to the current EU proposal on data governance. The underlying logic in balancing mechanisms and the overall vision of data surveillance they propose will be disclosed. Following this critical analysis, some policy recommendations will be put forward.

2. What is data governance?

Governance and data: The data economy. As explained in the introductory chapter, governance here refers to collective decision-making, people working together to solve and manage issues of common interest[1933]. At the outset, governance involves questions of power. Who has the power to shape the way we go about societal problems? Which policies and procedures balance competing interests and solve conflicts? How do different governance models impact on individuals and ensure values like legitimacy, transparency and inclusion?

With reference to data, governance identifies the set of mechanisms through which different actors manage data-related systems, and the power relations between them. Currently, the dominant model is that of the data economy, which features profound power asymmetries and aims for a worldwide free market of data. Data is conceived as a commodity and mostly handled by a handful of big tech corporations and telecommunication companies that have established *de facto* monopolies[1934]. The underlying assumption of this model is that if individuals are properly compensated with rights over data, these can be freely traded as private property. From a data governance perspective, this framework has functioned mainly through self-regulation by tech corporations and other actors handling data. In this sense, narratives about "data ethics" and "responsible AI" have often been cited by corporations to argue that they could be left alone in governing their use of data[1935]. Arguably, these claims are strongly inspired by a capitalist ethos, whereby corporate actors behave as key engines of growth and innovation in economy. As we will see next, this data governance model has also heavily impacted the dominant conceptualisation of smart cities and of the role of private actors therein[1936].

What is the nature of data for the purposes of data governance? An initial matter to be explored when dealing with data governance is the nature of data from a social and legal perspective[1937]. As said, the dominant model handles data as a proprietary asset that can be traded as any other commodity[1938]. Importantly, this idea is upheld not only in top business environments, but also by international organisations including the EU[1939]. Other assumptions, however, underlie the strategies of the data economy and are

[1933] See Introductory Chapter, §3.2.1.
[1934] Micheli et al (2020), p. 1.
[1935] However, in 2021 one of the chief proponents of this approach declared that "the time has come to acknowledge that, much as it might have been worth trying, self-regulation did not work". Floridi (2021), p. 622.
[1936] See below §3.1.
[1937] Madison (2020), p. 30.
[1938] Cf. e.g., Janeček (2018), p. 1040; Singh et al (2019), p. 54.
[1939] Solano et al (2022), pp. 21-24; Janeček (2018), p. 1045; Catanzariti, Curtin (2023b), p. 159.

embedded in current data protection legislation[1940]. For instance, different impacts and legal rules are usually established for the processing of personal and non-personal data, as well as sensitive and non-sensitive data. The market-led model relies on the fact that non-personal (and thus non-sensitive) data is tradable and reusable with no particular restrictions. These assumptions, however, have recently been challenged by advancements in profiling technologies. The distinction between personal and non-personal data is becoming increasingly blurred, and data-related harms no longer affect individuals only, but also groups[1941]. Sensitive information about individuals can be inferred not only through traditionally protected data (e.g., ethnicity, religion, sexual orientation), but also through the combined processing of seemingly innocuous datapoints. This means that the current legal regime is not necessarily up to date when it comes to ensuring fair data governance, which needs to go beyond legally protected categories of data.

In contrast with the data-asset perspective, data has also been characterised as no one's property (i.e., a *res nullius*)[1942]. The supporters of this position describe data as *non-rival* (meaning that their consumption cannot deplete them) and *non-excludable* (meaning that no one can be prevented from using them)[1943]. Because it can be easily copied, data is highly distributed in time and space (i.e., data "multiplicity"). For all these reasons, some have argued that data could be conceived as public goods[1944] and could be handled through open access regimes.

Controllability for data governance. To be true, both the "data-asset" and the "data as no one's property" appear radical in describing the nature of data and do not fully account for the specificities of big data contexts.

On the one hand, considering data as a commodity mainly serves the interests of a handful of actors in the data economy. Potentially, this could curb the distribution of value generated through its processing to the society at large. On the other, some have pointed out that the features of big data environments make data both excludable and rivalrous from a functional standpoint[1945], which questions the possibility of considering these resources as public goods to be available for anyone.

Firstly, data is clearly made excludable in the data economy. Tech corporations control big datasets and can impose legal or economic restrictions on access, like taxes and patents[1946]. Also, users usually lack the tools to make sense of big data and can be easily excluded from the benefits stemming from its processing[1947].

Secondly, scholars have shown changes in data flows (how it is shared and who has access to it) can impact on the value of these assets, demonstrating their rivalrous nature[1948]. This indicates that preserving the value of data implies some kind of stewardship (i.e., control). Therefore, it is arguably more coherent to adopt a non-formalistic position over the issue of data ownership, which avoids fully qualifying data as a commodity but also acknowledges its rivalrous nature. Data governance is not a

1940 Solano et al (2022), p. 25.
1941 On group privacy, see generally Taylor et al (2017a); Taylor (2016a); Mantelero (2016).
1942 As explained by Purtova (2015), p. 4. Prainsack (2019), pp. 2-3.
1943 Taddeo (2016), p. 6. Importantly, also Recital 6 of the draft Data Act qualifies data as a "non-rival good".
1944 Taddeo (2016), p. 4; Hummel et al (2020), par. 2; Froomkin (2015), pp. 1721, 1732; Beckwith et al (2019), p. 209. *Contra* Purtova (2015), pp. 2, 4.
1945 On the description of data "multiplicity" see Prainsack (2019), p. 7.
1946 Taylor (2016b), p. 2.
1947 Johnson (2014), p. 268: "(…) big data is not, in practice, open to citizens".
1948 Beckwith (2019), p. 209.

question of full ownership over data, but rather of "data controllability", in the sense of obtaining and keeping control over certain datasets, or setting specific conditions for data sharing[1949].

3. Governance models in smart cities

Techno-driven vs. human-driven smart cities. Generally, two models have been opposed in conceptualising the development and governance of smart cities. On the one hand, techno-driven (or technocratic) approaches stem from the initiatives of big US tech corporations in the field and rely on the assumption that technology alone can overcome any urban hurdle (i.e., technological solutionism). On the other, human-driven visions of smart cities tend to focus on bottom-up strategies and aim to combine technology potential with "soft infrastructure", like human and social capital (e.g., knowledge and education)[1950].

Both models have clear consequences for how data is collected and managed within smart cities. Technocratic models are underpinned by neo-liberal aspirations and fully fit the logics of the data economy, thus favouring intensive data surveillance practices. Inversely, human-driven outlooks aim to maximise the value of data for the public good of the city. In the following sections, the characteristics of both governance models will be examined and their implications from a surveillance perspective will be explored.

3.1. The Techno-driven approach

Overview. As previously illustrated, big tech corporations have been involved in defining the core traits of the smart city paradigm from the 1990s to this day[1951]. They have long advocated for the implementation of digital technologies in the urban environment and have often conceived cities merely as a promising market for their products. That is why companies like IBM and Cisco have frequently been regarded as the main proponents of the techno-driven governance model for the smart city[1952]. The essential features of this framework can be summarised as follows. Firstly, cities are seen as privileged settings not only for selling technology solutions, but also for implementing intensive data collection practices. These initiatives are underpinned by a strong logic of data accumulation. Therefore, data is not only used to run and improve public services, but also to build individuals' profiles to serve vendors' corporate interests. Digital solutions, developed by large multinationals, are integrated into diverse urban environments with a blind top-down approach. Local specificities and citizens' real needs are not a primary concern in this process. Consequently, scholars point out that cities are now turning into post-political constructs[1953]. Once seen as complex political, cultural and social entities, they now depend on easy, allegedly neutral and efficiency-driven solutions that completely disregard their specific connotations.

Against this background, this section will delve into the aspects of the techno-driven governance model for smart cities. Firstly, the conceptual link between cities and (surveillance) capitalism will be explained, also by referencing two concrete examples. Secondly, how the advent of the IoT and extensive datafication processes might change the urban landscape will be considered. Specifically, the neo-liberal model of the city "as a platform" will be illustrated.

[1949] Hummel et al (2020), par. 3.1. *Compare*, in a similar vein, Catanzariti, Curtin (2023b), pp. 164 ff.
[1950] Ziosi et al (2022).
[1951] See Introductory Chapter, §3.2.3.
[1952] See the reconstruction made by Sadowski et al (2019).
[1953] Ziosi et al (2022), p. 12.

Cities and (surveillance) capitalism. Cities have often attracted the attention of the market for their significant social and economic impact. There has always been a strong connection between urban planning processes and capitalism. Indeed, urban geographer David Harvey observes that cities have always played a role in the absorption of capital surpluses: "[…] since urbanisation depends on the mobilisation of a surplus product, an intimate connection emerges between the development of capitalism and urbanisation"[1954]. Hollands reminds us that there is a world-wide recognition of the fact that urban spaces in Western cities are primarily governed by neoliberal strategies[1955]. In the digital era, this has not changed. Cities continue to attract investments and capital surpluses, but also of a different kind. Drawing on Zuboff's framework of surveillance capitalism[1956], it can be contended that smart cities today constitute a selected environment for the production and re-investment of behavioural (data) surpluses. Specifically, corporations design and market their technologies not only to optimise the efficiency and sustainability of urban services, but also to grasp considerable amounts of behavioural data generated by citizens in their daily activities.

Examples: Google's Street View and Flow. Cases like Google's applications *Street View* and *Flow* can help illustrate this point. As we know, *Street View* is Google's notorious application providing a 3D representation of the world through satellite and aerial images[1957]. Starting from 2009, *Street View* was hit by serious privacy concerns. In 2010, an independent analysis by German security experts demonstrated that Street view's cars were gathering unencrypted personal data from homes. Experts in Canada, France and the Netherlands also discovered that garnered data included names, telephone numbers, credit information, passwords, messages, emails, chat transcripts, medical information, location data, photos, videos and audios files, as well as records of users' activities on online dating, pornography websites and other online search engines[1958]. Worryingly, these data were used to reconstruct detailed profiles of citizens' private lives and were later exploited in offline contexts "for use *in other initiatives*"[1959].

On the other side, *Flow* is a traffic management system managed by Google's affiliate Sidewalk Labs. In 2016, the company entered into partnership with the US Department of Transportation to provide city officials with its own transit data. Importantly, *Flow* was fuelled with data captured in other initiatives of Google's, such as *Maps* and *Street View*. Collected data would allow public and private actors to infer peoples' movement patterns and improve traffic flows in the city. Nonetheless, the data was exploited for aims beyond the mere optimisation of a public service. Indeed, *Flow* data was also used in real time to fuel virtual markets that extracted maximum fees from people in the city, e.g., for targeted pricing of parking spots[1960]. *Flow* would even divert citizens overcrowding public transportation systems to private ride-sharing companies like Uber[1961]. Of course, these systems were integrated in smart cities with a sheer top-down approach. Municipalities could not negotiate any condition with technology vendors, for instance by refusing certain data processing operations. They were placed in a weaker bargaining position and had to adopt the package as a whole, with no possibility of adapting it to their particular needs and urban specificities[1962].

[1954] Harvey (2008, original work of 1973), p. 316.
[1955] Hollands (2008), p. 308.
[1956] See Chapter IV, §2.2.
[1957] https://www.google.com/streetview/.
[1958] Zuboff (2019), p. 143.
[1959] Federal Commission Communication (2013), p. 11.
[1960] Zuboff (2019), pp. 229-230.
[1961] Taylor (2019), p. 5.
[1962] Id.

The role of the IoT: City datafication. If the development of (smart) cities has always been underpinned by capitalist ambitions, the advent of the IoT is now turbocharging these dynamics, allowing in-depth data exploitation. Transforming the city into a system of interconnected environments where data flows across multiple devices is indeed affecting the way in which public authorities manage cities. While data collection has always been a necessity in urban planning and policies, smart technologies can now offer a much wider and granular pool of data resources[1963]. Data are not sampled and garnered on an occasional basis as in the past, but are generated in real-time and are exhaustive in scope, as well as fine-grained in resolution[1964].

This shift in the production and analysis of urban data clearly exemplifies the phenomenon of "datafication" applied to cities. Datafication has indeed been described as "the transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis"[1965]. Daily activities such as commuting to work or strolling around city parks are sensed, translated into data, and used to adjust urban services to public demands[1966]. Urban life is therefore datafied and ultimately, commodified. In the data economy, platforms transform online and offline objects, activities, emotions, and ideas into tradable commodities[1967]. In the same way, in the city, every space and social interaction is thus reduced to an object, i.e., a set of data, to be shared or traded.

The city as a platform. This datafication process has a bearing in how cities are administrated. According to Kitchin, the integration of smart technologies in cities has produced a shift from mere *data-informed* urbanism to new forms of *data-driven* urbanism[1968]. If the former once relied on partial data collected on an occasional basis, the latter exploits big urban datasets to acquire an overall picture of the city. Through data, in fact, the city is represented to urban authorities as a *holistic* and *unique* reality, like a platform. It is regarded not just as a *place*, but as a network of systems which emulates the likes of Amazon or Uber[1969]. Just as digital platforms systematically gather and process user data, so sensors are meant to operate in an urban environment. In this way, they can provide for a real-time representation of places and social activities through actionable data, to be used not only to improve the city but also to pursue corporate interests[1970].

Post-political issues in techno-driven, platform-like smart cities: The case of Quayside Toronto. This was evident, for instance, in Sidewalk Lab's project for Quayside Toronto. The whole project was inspired by the concept of the "city as a platform"[1971]. In the company's vision, everything in Quayside had to be connected by a ubiquitous sensor infrastructure, becoming "the world's first neighbourhood built from

---

1963 Kitchin (2016a), p. 1. This is acknowledged also by Van Dijck et al (2018), p. 33.
1964 Kitchin (2016a), p. 2.
1965 van Dijck (2014), p. 198 (citing Mayer-Schoenberger, V. and K. Cukier. 2013. Big Data. A Revolution that will transform how we live, work, and think. London: John Murray Publishers, 73-97).
1966 According to Schaklett (2019), more than 3000 park benches in Paris are now equipped with sensors measuring citizens' satisfaction with park facilities.
1967 Van Dijck et al (2018), p. 37. See also Zuboff (2019), p. 140; Shaw et al (2017), p. 909.
1968 Kitchin (2016a), p. 2.
1969 To imagine how cities would be like if administered through Amazon's business model, some authors have edited an engaging collection of speculative short stories. See Graham et al (2019).
1970 Goodman et al (2019), p. 477.
1971 Goodman et al (2019), p. 474, note 138. On the "platformisation" of the urban transportation system, see Van Dijck et al (2018), pp. 75-96. See also De Waal (2017); Bollier (2016). For a critical perspective of the concept of the city as a platform, see Sadowski et al (2015).

the internet up"[1972]. A single network of neighbourhoods was to be established, functioning "at a system scale, like the internet, generating advantages that increase with each new node"[1973].

Representing the city not as a place (or better, as a collection of *different* places) but as a system or network comes with some problems. For instance, practical and social distinctions between environments and neighbourhoods in the city may not be properly represented in collected datasets: differences at the urban scale that have always been taken into account by city authorities when they analysed urban data. However, such specificities may not represent a competitive advantage for companies aiming to sell their technologies to municipalities. For example, this emerged in Sidewalk Lab's vision of the "network of neighbourhoods" for the Quayside:

> "Whereas a neighbourhood of a few thousand people will produce a modest market opportunity to attract third parties to the platform, a district of networked neighbourhoods will be powerful enough to draw companies and entrepreneurs from all over to take part in Toronto's new ecosystem"[1974].

Furthermore, proponents of post-political visions of smart cities argue that digital infrastructure in these settings is *neutral*[1975]. They reimagine the city as a bound system that can be statistically measured, modelled and assessed, and argue that collected data is a value-free and objective representation of the reality[1976].

Faced with these technocratic visions of the urban environment, however, scholars have tried to reclaim the nature of cities as normative constructs. Specifically, these should not be treated as mere technical systems or networks: they are social, cultural, political systems that must be evaluated *normatively*[1977]. The city thus not considered as an entirely knowable and manageable system, but as an *open*, *fluid* and *relational* reality living off culture, competing interests and politics[1978]. In other words, the city is first of all a human construct which cannot be understood and evaluated exclusively through urban data.

In addition, the technical systems in charge of generating or gathering urban data (sensors, for instance) are not neutral either. The way in which data about the city is collected, processed, and presented is always the result of a technical configuration and implementation. To quote Kitchin once again: "data is never raw, but always already cooked"[1979]. In the case of IoT technologies deployed across the city, urban authorities cannot make sense of collected data without considering where the sensors are placed, their field of view, their sampling rate, setting and calibration[1980].

These insights have prompted the development of a different approach for smart city governance, with the aim of enhancing their unique social features. This "human-driven approach" will be outlined in the following sections.

1972 Badger (2017).
1973 Sidewalk Labs (2017), p. 21.
1974 Sidewalk Labs (2017), p. 21.
1975 The same assumption is held with regard to the claimed neutrality of social media platforms, see Van Dijck et al (2018), p. 32. More recently, see Becker (2019), p. 310.
1976 Kitchin (2016a), p. 4.
1977 De Waal (2017), p. 18.
1978 Id., p. 11. See also de Waal et al (2017), p. 26: "Cityness then, lies in the spatial organisation of density and diversity, and the somewhat chaotic interaction that results from it, as well as in the social goods that this may produce: solidarity, creativity, innovation, trust, community. What's important in this line of thinking is that it's best understood as a normative assumption: a city works best when it functions as an open and somewhat disorderly system with ample public spaces as catalysts for chance encounters".
1979 Kitchin (2016a), p. 11.
1980 Kitchin (2017b), p. 50.

3.2. The Human-driven approach

3.2.1. The human-driven approach of Barcelona

A change in approach. One notable example in the human-driven approach to smart cities is Barcelona[1981]. Different scholars have pointed out how the city has moved forward from a purely technocratic approach, heavily involving tech giants such as Cisco, to a more democratic implementation of urban smart technologies[1982]. Under the impulse of a newly established Digital Innovation Office, a series of initiatives aiming at empowering citizens in their relationship with urban technologies was launched. Firstly, in September 2017 the Barcelona City Digital Plan was published[1983]. The 2017 Barcelona City Digital Plan enshrines the guiding principle of digital sovereignty:

> We believe in digital sovereignty for cities, full control and autonomy of their Information and Communication Technologies (ICTs), including service infrastructure, websites, applications and data, in compliance with and with the support of laws that protect the interests of municipalities and their citizens.
>
> Technological sovereignty helps cities protect citizens' rights through greater accessibility, transparency, accountability required for open government[1984].

The peculiarity of Barcelona's concept of technological sovereignty is that citizens shall exercise full control not only over their personal data, but also over the overall digital *infrastructure* (comprising services, websites, applications)[1985]. That is why the city promotes a policy of public digital infrastructure based on free and open-source software.

Furthermore, citizens are seen not only as the beneficiaries or recipients of smart city services, but also as active participants of urban digitisation processes. To provide them with effective control over their data and its exploitation, the City Council has launched a New Social Pact on Data, aiming to develop a new approach to urban data ownership: the *city data commons*. As will be explained next, this data governance approach attempts to strike a balance between the needs to maximise the exploitation of urban data and citizens' rights to privacy and data protection.

Importantly, this model inspired an important EU-funded pilot project, *Decode*, of which Barcelona assumed leadership in 2017[1986]. The *Decode* project aimed to build a decentralised data infrastructure providing individual citizens with the tools to decide whether to share their personal data for the public

---

[1981] Ziosi et al (2022), p. 4.

[1982] The techno-driven approach in Barcelona's evolution towards the smart city paradigm was initially mirrored in the vision of the city chief architect, Vincent Guallart (appointed in 2011). In his book *La ciudad autosuficiente* [The Self-Sufficient City], Guallart developed a narrative presenting the city as a "system of systems", where the urban space emerges out of the combination and interaction between different nodes (i.e., the home, the neighborhood, the district…) and network flows. As previously explained, this vision of the city as a "system of systems" has been highly criticised by scholars that argue that the urban environment should be seen as a complex human construct, with all its political, social and cultural dimensions. On this topic, see March et al (2016), pp. 818-819.

[1983] https://ajuntament.barcelona.cat/digital/sites/default/files/LE_MesuradeGovern_EN_9en.pdf. Accessed 1 August 2022.

[1984] Ajuntament de Barcelona (2017). The notion of "sovereignty" is also referred to in the Declaration of Cities Coalition for Digital Rights, endorsed by the City of Barcelona. https://citiesfordigitalrights.org/#declaration. Accessed: 27 August 2020. The value of sovereignty, however, seems here to be stricter in scope, being associated only with the control of personal data. The concept of technological sovereignty is also mentioned in Francesca Bria's work, who takes a "holistic" approach to the concept, see Morozov (2018), pp. 30 ff. *Compare* also Calzada et al (2020).

[1985] One example is CityOs, a horizontal platform called CityOs, using open standards and processing data with common ontologies. CityOs is also integrated with Sentilo, the city's main sensor and actuator platform. Sentilo receives real-time data from all IoT sensors deployed across the city. Through Sentilo, the City Council provides a map showing where different kinds of sensors are deployed across the city, see: https://connecta.bcn.cat/connecta-catalog-web/component/map. Accessed 27 August 2020. On collaborative platforms developed in Barcelona, see Fuster Morel et al (2018).

[1986] https://www.decodeproject.eu/. To understand Decode's vision of data as a common asset for the city, see one of the project's reports, Bass et al (2018).

good of the city. Another EU-funded project piloted by the City Council, *Decidim*, also played a role in fostering active participation of citizens to solve common urban issues[1987]. Through an open-source digital platform[1988], Barcelona experimented new methods of participatory democracy. With more than 31,000 registered users, the *Decidim* platform has until now collected and adopted over 9,000 citizens' proposals[1989]. In addition, citizens are also enabled to decide whether the data they generate can be used as an evidence base for new policy proposals[1990].

3.2.2. The communitarian critique to neoliberal smart cities

Communitarianism: A brief overview. In philosophical literature, scholars are turning to communitarian outlooks to reconvert technocratic and neoliberal trends in smart cities[1991]. At the outset, the prominent scholar Amitai Etzioni defines communitarianism as "social and political philosophy that *emphasises the importance of community* in the functioning of political life, in the analysis and evaluation of political institutions, and in understanding human identity and well-being"[1992]. The core traits of this moral approach can be briefly summarised as follows. Communitarianism offers a practice-based account of morality, which arises from social conventions and traditions in specific communities. That is why communitarians reject the universalist pretentions of (neo)liberal and Kantian thinkers, who see morality as a set of universally binding principles that can apply in any given social and cultural context (as for individual fundamental rights). They also dismiss the excessive individualism purported by neoliberalism and place great importance on the value of common good, which is often disregarded in light of allegedly universal individual rights[1993]. For their tendency to accept pluralism in morals, communitarians have faced challenges of "cultural relativism", which bears the risk of legitimising unacceptable practices such as torture, discrimination and other violations of basic fundamental rights[1994]. They have also been criticised for their scarce consideration of individual autonomy.

The communitarian critique to neoliberal smart cities. Communitarian thinking has provided alternative visions for techno-driven smart cities. In *The Spirit of Cities*, for instance, Daniel Bell and Avner de-Shalit argued that every city has its own ethos and upholds a particular way of life, in contrast with neoliberal universalist perspectives. To overcome issues of cultural relativism, moreover, they also proposed a slight variation of classic communitarianism, i.e., "cosmopolitan communitarism". While they still place the roots of morality in local practices, they admit that for an urban ethos to be granted moral recognition, this has to guarantee a minimum threshold of basic human rights[1995]. For the importance they give to the concept of common good, communitarians also challenge the individualistic drifts that underpin the functioning of neoliberal smart cities. Indeed, when smart cities

---

1987 https://www.decidim.barcelona/?locale=ca.

1988 Decidim digital platform was built by using the results of another important EU-funded project, D-Cent (Decentralized Citizens Engagement Technologies), see: https://dcentproject.eu/. Accessed: 27 August 2020.

1989 See Glasco (2019), p. 5.

1990 Iaione et al (2019).

1991 See, e.g., Cardullo et al (2019a).

1992 Etzioni (2013). See also Bell (Fall 2020). Generally speaking, modern communitarianism finds its roots in the work of the empiricist philosopher David Hume, who gave his "conventional" account of morals in the 1750 *A Moral Philosophy of Traditions and Communal Convention*, see Beauchamp (1991), pp. 266-271.

1993 Communitarians are also criticised for devaluing individual autonomy. Because they find the basis of morality on collective agreements between the members of a given community, individual freedom and personal determinations are not given large space. See Beauchamp (1991), p. 270. However, this original and more radical position has been later mitigated by Etzioni's concept of responsive communitarianism. See Etzioni (1996).

1994 Notorious is the case of Micheal Walzer, who in its famous *Spheres of Justice* defended the moral legitimacy of the caste system in India – a system that may be regarded as discriminatory from a Western viewpoint – as the latter was coherent with the local perspectives on societal order. See Beauchamp (1991), p. 276.

1995 Bell et al (2012), pp. 4-8.

are conceived as a mere economic project, citizens are primarily regarded as market actors, users and consumers of digital services[1996]. Public service delivery is not arranged to optimise values of distributive justice and sharing of common resources, but to accommodate the preferences and the socio-economic status of the individual consumer. In other words, neoliberal urbanism "shifts citizenship away from inalienable rights and the common good towards a conception rooted in individual autonomy and freedom of 'choice'"[1997]. Against this backdrop, a communitarian-oriented perspective on smart cities may inspire a better balance between shared values of "commoning" and excessive individualism and consumerism.

The Right to the City. In the field of urban sciences, the concept of the right to the city is also regaining strength in the critique towards the techno-driven approach to the smart city. The idea was first made popular by the French philosopher Henri Lefebvre, who defined it as follows: "[t]he right to information, the rights to use of multiple services, the right of users to make known their ideas on the space and time of their activities in urban areas; it would also cover the right to the use of the centre"[1998]. Lefebvre conceptualised the right to the city as a tool to challenge power relations that permeate decision-making processes about the development and management of city spaces. Its objective was to transfer control from corporate actors and the State towards urban inhabitants (*les citadins*), regardless of their nationality. Importantly, it might be argued that Lefebvre also expressed communitarian or collectivist views on the city[1999]. Indeed, he valued the *community of place* (i.e., communities based on geographical location) as a normative ideal, meaning that the right to the city could only be exercised by the urban community as a whole, whose members had earned it by experiencing daily life in the city.

The idea of the right to the city has been very successful in the field of urban studies and was later reworked by several scholars[2000]. More recently, Shaw and Graham have also offered an up-to-date analysis of the right to the city in light of cities' current digital transformation[2001]. They focus on one specific component of the right to the city, the right to information, highlighting its renewed complexity in smart cities[2002]. They contend that flows of information now create a new kind of abstract environment, the city digital layer[2003]. This means that digital information about urban space is as important as the physical space, made of concrete buildings, roads and squares. As a result, the

---

1996 Cardullo (2019), p. 814. The radical difference in the concepts of citizen and consumer is also highlighted by Ranchordás (2018), p. 159: "Another difference in the traditional foundations of the concepts of a citizen and a consumer refers to the fact that citizenship conveys the idea of universal equality, solidarity between citizens, and community-based values. Citizenship tends to be presented in normative terms as a counterpoint of marketisation and commercialism. Access to public services reinforces equality of status among citizens and their identity, allowing citizens to participate actively in public life, regard- less of their educational background or economic power. On the contrary, the position of citizens tends to be more market oriented. Consumerism links consumption to individual social status, well-being and upward mobility".

1997 Cardullo (2019), p. 817.

1998 See Marcuse (2009), p. 189 (citing Lefebvre, H. (1991) Les illusions de la modernité. In: Ramoney I, Decornoy J, Brie CH (eds) La ville partout et partout en crise, Manière de voir, p. 34. Paris: Le Monde diplomatique).

1999 It should be remembered that Lefebvre has often been labelled as a Marxist philosopher. In this respect, Amitai Etzioni stressed how the works of Marx – and of other philosophers and sociologists – had focused on the role of "authentic communities" as a force against alienation and despotism, as well as a pillar of a good society. See Etzioni (1996), pp. 3-4.

2000 See, *inter alia*, Harvey (2008, original work of 1973) pp. 315, 328-329. Marcuse (2009); Purcell (2016); See also Purcell (2002). With specific reference to smart cities, see Cardullo et al (2019a).

2001 See Shaw et al (2017). On applying the Right to the City idea to the contemporary of context of the smart city, see Keymolen et al (2019), pp. 3-4.

2002 Shaw et al (2017), p. 908: "[…] we contend that the right to information is now a more complex aspect of political struggle than Lefebvre could realise (at the time). And, that a right to the city now depends upon a better reading of today's critical phase in urbanisation as a period where the city is increasingly reproduced through digital information".

2003 Id.

"urbanisation of information" – i.e., the power relations surrounding the production of digital urban information – needs to be addressed as a pressing issue. In this respect, the case of Google Maps is offered to show how Google itself profits from its privileged position to mould social and economic experiences in cities, influencing where people go, how they get there, which parts or activities of the urban sphere are visible or not[2004].

3.2.3. Alternative data governance for smart cities

Alternative models to the data economy. Smart cities adhering to human-driven outlooks are trying to implement data governance models that are occasionally inspired by communitarian thinking[2005]. Among these, data commons, public data trusts, and data cooperatives can be mentioned. Today, these frameworks are mainly proof of concepts or pilots, but they are gaining increasing attention among scholars as alternatives to the dominant data economy[2006]. While they all are distinguished at the theoretical level, it is important to note that they could (partially) overlap in practice.

3.2.3.1. Data commons

Overview: Traditional and digital commons. This governance model is inspired by Elinor Ostrom's work on commons theory. It originally focused on natural physical resources, like fisheries and water basins that are to be used jointly by the members of a specific group (the appropriators). The commons framework aims to identify rules under which common-pool resources can sustainably be shared within appropriators in the long term, without diminishing their quality and quantity[2007].

In relation to the digital realm, the commons model enshrines a scheme that grants access to data through a shared infrastructure in ways which make it less excludable by corporate interests[2008]. At the normative level, the data commons aim to mitigate the power asymmetries with regard to private sector actors who exercise *de facto* monopolies in modern platform societies[2009]. Data commons have been extensively advocated in the health and scientific research domains, but they are yet to be realised[2010]. This can be explained by the fact that the governance of digital data poses different challenges compared to the management of traditional common pool resources. Specifically, data needs both material and digital infrastructure to be managed and shared as common-pool resources[2011]. As a solution to these issues, a scheme of data semi-commons was also put forward. In this framework, individuals, public and private entities, and data intermediaries could all have different access rights to commons data, within the boundaries of privacy rights[2012]. Translated at the EU level, this could entail that specific categories of data could be governed as common property of Member States and their residents, and control over these resources could be ensured centrally with varying degrees of access[2013].

Data commons in smart cities. In smart cities, data commons could be established to make sure that these resources are operationalised to respond to real social issues and needs of urban communities[2014].

[2004] Id., p. 911.
[2005] Solano et al (2022), p. 18.
[2006] Id., p. 25.
[2007] Prainsack (2019), p. 4. See also Madison (2020).
[2008] Solano et al (2022), p. 27.
[2009] Prainsack (2019), pp. 3, 6. See also Singh et al (2019), p. 55. Taylor et al (2019), p. 1.
[2010] Solano et al (2022), p. 27.
[2011] Id., pp. 27-28.
[2012] Id., p. 27.
[2013] Id.
[2014] For an overview of the "city data commons" policy scheme in Barcelona, see Calzada et al (2019). On the topic of urban commons, see Foster et al (2019); De Lange (2019).

If data is placed under the stewardship of relevant communities, urban authorities could maximise data benefits for the local population, while downsizing the influence of big tech corporations in the city.

Of course, the commons model presupposes that data should be characterised as a rivalrous good. As shifts in data flows can lead to variations in their value[2015], urban communities need to exercise control over such data and maximise the benefits of its processing. That is why cities (and higher scale authorities) should have a decisive role in implementing data governance rules (as well as legal arrangements) that ensure that data is controlled by local communities[2016].

Importantly, the urban data commons model seems to uphold the value of *positionality*, a concept developed by geographers and that was translated in the data ethics field too[2017]. This principle mandates to take into account the spatial and social contexts where the data is generated in order to make sense of the acquired information in a fair manner. Carrying out contextualised analysis of city data therefore means to refute the assumption that data and technologies are neutral in themselves, a perspective that is purported by tech corporations investing in smart cities.

Implications from a surveillance perspective. Central in the concept of commons is the prerogative of controlling communities to exclude third parties from access to their resources. When it comes to data, this can be important from a surveillance standpoint. The more entities have access to data, the more information can potentially be inferred from such data. The more individuals and groups fit into different profiles and classes of interests, the more they can become targets of surveillance. Therefore, governing the data commons may require creating adequate frictions in the flow of information, excluding entities that cannot ensure a fair processing or have discriminatory interests over data from access. This could be an important strategy to curb unwarranted surveillance, the multiplication of targets and inferences from data. In smart cities, this could imply restraining unlimited repurposing of urban data to corporations that pursue commercial ends only and do not contribute to the common good of the city.

The commons and open data. Importantly, different conceptualisations of data commons can be found in literature[2018]. In some cases, commons are conflated with open data schemes (i.e., open access commons), where data is free for everyone to use and there is no control over the flow of information[2019]. In others, access to the data commons is restricted[2020].

From a smart city perspective, however, the commons and open data schemes should arguably be conceived as two distinct data governance models with different implications for urban communities. As opposed to the commons, open data is an umbrella term that defines different initiatives involving a "commitment to make data publicly available in a non-proprietary, machine-readable format at the lowest granularity possible"[2021]. Because in open data the information belongs to everyone, communities cannot exercise any form (or very limited) of stewardship over data. While some see open data as a means to achieve greater transparency for urban authorities' decisions, others claim that this

[2015] Beckwith et al (2019), p. 209 (the Authors build upon the considerations of Aragon LV (2011) Where Commons Meet Commerce: Circulation and Sequestration Strategies in Indonesian Arts Economies. Anthropology of Work Review 32 (2): 63–76).
[2016] Id., p. 218.
[2017] Taylor (2019), p. 3. On the value of spatial analysis of data see further Dalton et al (2016).
[2018] Solano et al (2022), p. 28.
[2019] See, e.g., Calzada et al (2020).
[2020] Solano et al (2022), p. 28; Madison (2020), p. 35. An argument for restricted data commons in smart cities is made by Beckwith et al (2019).
[2021] Johnson (2014), p. 264.

model actually expresses the "libertarian ethos" of the information technology sector, dominated by the values of technological neutrality, radical individualism, and naïve technological determinism[2022].

Indeed, open data frameworks are often seen as problematic because it is often difficult to ascertain who actually profits from its processing. Because data is made available to everyone, it can also be exploited by entities that do not have the necessary knowledge to contextualise it, thus leading to unjust and erroneous inferences. This kind of blind approach to data is said to ignore the constructed nature of data[2023]. Making data publicly available may not be morally good in itself: one should always pay attention to *which* data is being made open. The process of data production is always informed by the values and assumptions that reflect the preferences and interests of the actors involved. When these values or assumptions are unjust, injustice becomes an embedded and magnified feature of the open data as well (i.e., data ethics principle "garbage in, garbage out)[2024]. Importantly, scholars have warned against these risks in the smart city context as well[2025].

3.2.3.2. Data cooperatives

Brief overview. As a governance model, data cooperatives (DCs) are characterised by a high level of reciprocity that puts all relevant stakeholders (including citizens) on an equal position with regard to how data governance rules and procedures are determined. Data subjects share data on a voluntary basis and are the main actors when deciding how data should be used and shared. To this end, they establish a trust relationship with an intermediary (a cooperative) that manages data on their behalf. This association is made through "bottom-up data trusts", i.e., agreements and contracts that provide the means for the citizens to be informed, express their preferences and concretely decide how to share their data and for which purpose[2026]. Many DCs are commons-based, with restricted access to data. Others draw on the "open cooperativism" movement and allow for the dissemination of data in open licence[2027].

From the normative perspective, DCs also stand in contrast with the dominant data economy framework. They reject the narrative of data as a commodity and define it as commons that should be managed by and for the community[2028]. They also challenge prevailing big data practices by relying on decentralised and bottom-up solutions for data management, strengthening transparency and openness over the value that is generated by data[2029]. Relevant pilot examples include FairBNB, where hosts and local communities share the profits of the house-renting services, platform cooperatives for gig workers of delivery and ones like Co-Op Ride and TURPI. Importantly, the role of data cooperatives is also mentioned in Recital 24 of the Proposed Data Governance Act.

2022 Id.

2023 Id., p. 265.

2024 Id.

2025 Noorman et al (2020): "Principles such as open, transparent, legitimate, and inclusive are 'yay' words: they evoke positive emotions, but at the same time they could mean everything and nothing at all. Since the principles are very abstract, they can be applied in many different contexts. But it also comes with the risk of treating this list of principles as a gratuitous checklist, allowing you to interpret each criterion in your own way. Because what does transparency mean exactly? Transparency for whom? Who needs to understand it and be able to do something with it? And is open always a good thing under any and all circumstances? Or does it also have problematic aspects? Open access to data can lead to increasing the power of large market parties – who have the manpower and money to do something with that data – compared to smaller organisations. It's worth asking whether that is always advisable". The opinion concerned the Tada Manifesto, a document endorsed by the city of Amsterdam to foster an ethical and responsible use of data in digitised cities.

2026 Micheli et al (2020), p. 8.

2027 Id., pp. 7-8.

2028 Solano et al (2022), p. 29.

2029 Id.

3.2.3.3. Public data trusts

Brief overview. Public data trusts (PDTs) also feature a high level of reciprocity, but in this case the public sector is in charge of managing the data. In PDTs a public institution accesses, aggregates and uses data about citizens, leveraging on both private and public data sources[2030]. Because data is conceived as a public infrastructure, it is possible that private actors may also be authorised to access it under strict accountability conditions[2031]. In this model, the public sector acts as a trustee that vouches for the ethical and secure processing of citizens' data. A trust relationship is established between trustors (the citizens) and the trustees (public institutions), and is maintained through public consultations, living labs, strong accountability mechanisms and collective benefits[2032]. Involving external independent organisations as intermediaries may also be possible[2033]. As mentioned above, relevant initiatives in this sense include the EU projects *Decode* and *Decidim* in Barcelona.

3.2.3.4. Data collaboratives

Brief overview. Data collaboratives are partnerships where privately held data is pooled with public data through an independent third party[2034]. This entity manages the data access, sharing and use of common resources is limited to the members of the agreement (usually a PPP). The data pool is mainly used for public policy objectives and members are empowered by using data that was previously not accessible. From a normative standpoint, data collaboratives rely on some of the basic principles of the dominant market-led model, especially for the centrality of data controllers in data governance. In this sense, they represent a "mitigation" of data economy drifts, rather than a real alternative to it. A relevant example is the NYU GovLab, which has created a database with more than 200 data collaboratives, mainly from the health, transportation and humanitarian domains.

3.2.3.5. Personal data sovereignty

Brief overview. Another governance setting that subtly reproduces the logic of the data economy is that of personal data sovereignty. Personal data sovereignty (PDS) is a governance model where data subjects are conceived as free market agents managing access to, use and sharing of their data[2035]. It provides individuals with greater control over their personal data and spaces for self-determination and aims to create better services allowing for user control over data. New intermediaries seeking trust from individuals to share and transfer personal data within the data economy are central to this model.

From the normative perspective, PDS stands very close to the logic of a market-led governance of data. Individuals are seen as fully rational actors with the possibility to challenge power asymmetries with big corporations. Likewise, personal data is treated as a commodity used by data subjects in exchange for better services. In practice, however, studies show that most people would not have the time or the skills to fully profit from the services of such data intermediaries[2036]. At the same time, however, PDS is characterised by privacy management and data portability compared to the current dominant model. This is made possible by a set of different technologies that provide greater control over one's data, including cryptography and Blockchain.

[2030] Micheli et al (2020), pp. 8-9; Solano et al (2022), p. 26.
[2031] Solano et al (2022), p. 26.
[2032] Micheli et al (2020), p. 8.
[2033] Id.
[2034] Reconstruction based on Solano et al (2022), pp. 26-27.
[2035] Reconstruction based on Solano et al (2022), p. 31; Micheli et al (2020), p. 9.
[2036] Micheli et al (2020), p. 10.

3.2.3.6. How do these models fit into broader governance models?

Market-led models. Even if they are presented as alternatives to the data economy, these models actually have disparate normative implications and evoke different governance structures. Firstly, individual-based initiatives like personal data sovereignty fundamentally fit the underlying logic of the data economy. They treat data as a commodity and do not offer collective mechanisms to rebalance power asymmetries in the data market. Counterintuitively, individual rights function as implicit factors that legitimise the system. Rights to data access, transfer and portability are merely a counterpart to handling data as an asset and serve as warning signs for unacceptable data uses that may lead to disrupting the efficient functioning of the market[2037]. In a sense, personal data sovereignty conveys a model of self-regulation of the individual, which conveniently matches that of corporations in the data economy.

Co-existence of the private and the public. When public and private actors cooperate, data is handled in a co-governance model. In these frameworks, intervention of the State may be more or less incisive and so the space left to companies' self-regulation may vary. Therefore, private actors can exert more or less influence on the market depending on how their interests are concretely balanced with public ones. For example, data collaboratives are an instance of potentially market-led co-governance structure. Data is managed through a PPP and relies on the idea that data is a private property that companies can own and share with public authorities through an independent body[2038]. Because private parties often exercise significant control over the decisions of these bodies, this model may reproduce the power relationships existing in the data economy within the collaborative.

Another governance model that implicitly avails of the data economy is the risk-based approach. Present in the GDPR and in the draft AI Act, this framework relies on the self-government of those tasked with handling data and advanced technologies (i.e., accountability principle). It further builds upon standardisation, codes of conduct and voluntary certification mechanisms. Because these instruments are foreseen within a regulatory framework, they cannot qualify as self-regulation *tout court* (i.e., enforced self-regulation). However, the lack of safeguards around such regulatory mechanisms may betray a pro-market stance on data governance.

Public-led governance. In public data trusts, public bodies play a leading role in the governance of data. This model stands closest to traditional State-based regulation. It manages data through the public policy mechanisms of accountability and broader governance mechanisms of public participation. However, it also faces financial sustainability challenges due to the investments required to maintain such infrastructures[2039].

Community-led governance. Frameworks like the data commons and cooperatives are inspired by a communitarian ethos and embody a model of bottom-up self-governance by communities. Especially in data cooperatives, groups are diverse and fluid, and put forward with disparate interests. Participation is voluntary because it is acknowledged that communities and their interests may change over time[2040]. Despite the collective effort in achieving control over data, data cooperatives' potential to challenge the logic of the data economy may be mitigated under the current regulatory framework. Indeed, Recital 24 of the draft DGA recognises the role of these mechanisms, but also recalls the importance of individual-based rights under the GDPR.

[2037] Solano et al (2022), p. 34.
[2038] Id., p. 33.
[2039] Id.
[2040] Id., p. 34.

After uncovering the logic and structure of most discussed governance models, the discussion will shift to the prospective EU data governance model. Relevant legislative initiatives will be reviewed to understand which governance frameworks are mirrored in the proposals. Hence, their implications for the data economy and surveillance in the smart cities will be scrutinised.

4. Data governance in the EU

A European strategy for data. In February 2020, the European strategy for data was published[2041]. In the document, the Commission depicts the EU as a potential role model for a society empowered by data to make better decisions in the public and private sector[2042]. In a society where individuals will generate ever-increasing amounts of data, the EU acknowledges the transformative value of this resource for the economy and society, while also finding ways to exploit it according to European values (fundamental rights, safety and cybersecurity)[2043]. Importantly, the Commission grounds its vision on a conceptualisation of data as a "public good"[2044]. Conceived as a non-rival good, data should be used to tackle environmental emergencies and climate change, improve people's welfare and public services, as well as fight crime more efficiently.

More legal certainty is thus needed to boost government-to-business (G2B), business-to-business (B2B), business-to-government (B2G) and government-to-government (G2G) data sharing[2045]. Legislation at the EU level should lay down harmonised rules to foster data transfers within the internal market, creating so-called "data spaces"[2046]. The objectives of such data governance framework should include fighting against power imbalances in the data economy, improving data interoperability and quality, empowering individuals' rights skills and data literacy[2047]. These legislative interventions should also be coupled with important investments in Europe's edge and cloud infrastructures[2048].

To realise these goals, the European data strategy envisioned different legislative instruments. Among these, the Data Governance Act, the Data Act and the Artificial Intelligence Act will be at the centre of this analysis[2049].

Undoubtedly, AI is scaling up the challenge of data and technology governance, from individual claims and issues to collective ones. These legislative proposals are trying to address these problems, especially in relation to the underlying conception of data as a public (or common) good. Therefore, in the following subsections a brief overview of each draft legislation will be provided. Their critical analysis, with possible implications for the smart city context, will be presented at a later stage[2050].

4.1. The Data Governance Act

Brief overview. The draft Data Governance Act (DGA) aims to foster data sharing in the internal market. Therefore, it provides for a harmonised framework for (1) the reuse of certain public sector data, (2) data sharing services, (3) data altruism.

Firstly, the DGA foresees conditions for the reuse within the EU of certain categories of public sector data that are protected on the grounds of commercial and statistical confidentiality, intellectual

[2041] European Commission (2020).
[2042] Id., p. 1.
[2043] Id.
[2044] Id., p. 6.
[2045] Id., pp. 7-8.
[2046] Id., p. 8.
[2047] Id., pp. 9-10.
[2048] Id., pp. 15-16.
[2049] For an overview, see also Poullet (2021).
[2050] See below §5.

property rights of third parties, data protection legislation (Art. 3). Importantly, it does not only refer to personal data, and thus revives the debate about the impact of both personal and non-personal data processing in digital governance[2051]. To foster data circulation the DGA generally prohibits agreements and other practices that may grant exclusive access to such data to certain entities (Art. 4). Article 5 of the Proposal lays down the conditions for reuse, which should be non-discriminatory, proportionate, objectively justified with regard to the category of data at stake and should ensure data integrity and security. Fees may be imposed by the public sector to access the data (Art. 6). Clearly, this framework follows a long-standing policy of the EU, according to which data generated at the expense of public budgets should benefit society at large (Rec. 5).

Secondly, the legislation outlines the activities of data sharing services (or data intermediaries, including "data cooperatives"). In the data economy, these providers are meant to facilitate the aggregation and exchange of data (Rec. 22). Specifically, their services consist of putting in relation data subjects and data holders (i.e., anyone who is in control of a given set of data) with data users, through legal and technical arrangements. Under the DGA, the activities of these entities in the EU will be subject to a notification mechanism involving competent authorities (Arts. 10 ff.).

Thirdly, the DGA introduces the concept of "data altruism", i.e., the voluntary sharing by data subjects of personal and non-personal data for purposes of general interest, without seeking a reward (Art. 2(10)). Scientific research and the improvement of public services are explicitly mentioned as general interest goals justifying such kind of data sharing. The legislation provides for a framework of voluntary registration of data altruism services (Arts. 15-17). The registered entities will be subject to transparency requirements (Art. 18), specific safeguards to protect the interests of data subjects (including purpose limitation, Art. 19), and conditions to transfer data to third countries (Art. 30).

4.2. The Data Act

Brief overview. The Data Act (DA) promotes fairness in the allocation of value from data among actors in the data economy and aims to foster access and use of data[2052]. Specifically, the instrument ensures that users can access the data generated by the products they own or lease, as well as share them with third parties (Arts. 4-5). For this reason, it also requires manufacturers to design IoT products in such a way that the data is easily accessible (i.e., data portability, Art. 3).

The proposed legislation further promotes the sharing of data with the public sector and EU institutions that demonstrate an exceptional need in the performance of a task in the public interest (Arts. 14 ff.). This business-to-government sharing scheme is a novelty in the EU (so-called "reverse PSI"), but limited to emergency situations only and excludes such transfers on a general basis. Art. 2(10) defines public emergency situations as exceptional situations that negatively affect the population of the Union, a Member State or part of it, with a risk of serious and lasting repercussions on the living conditions and economic stability, or the substantial degradation of economic assets in the Union or relevant Member State.

Lastly, the DA aims to develop interoperability standards for data to be reused across sectors, in order to remove barriers to data sharing among specific common "European data spaces". This concept is not further defined in the proposal[2053]. Nonetheless, the explanatory memorandum to the proposal refers to them as "governance frameworks and infrastructure[s]" that contribute to efficient

[2051] De Hert (2023), p. 110.
[2052] Proposal, p.2.
[2053] Cf. Recc. 86-87, Art. 28 ff.

and trustworthy data sharing and use across strategic sectors of the economy and domains of public interest[2054].

4.3. The Artificial Intelligence Act

Brief overview. The Artificial Intelligence Act is meant to lay down harmonised rules for the development, placement on the market and use of AI systems which present varied levels of risk[2055]. Based on such a risk-based approach, the draft legislation distinguishes four categories of AI technologies: (i) unacceptable risk; (ii) high-risk; (iii) limited risk; (iv) minimal risk (for which voluntary codes of conduct are encouraged and facilitated, Art. 69).

Title II of the proposal foresees four kinds of AI technologies presenting unacceptable risks. Art. 5(1)(a-b) bans manipulative systems that deploy subliminal techniques or exploit vulnerabilities of a specific group due to their age, physical or mental disability, distorting human behaviour or likely causing physical and psychological harm. Art. 5(1)(c) targets systems used by (or on behalf of) public authorities to evaluate or classify the trustworthiness of natural persons in time based on their social behaviour or personality traits, when the social scoring is unjustified or disproportionate, or leads to detrimental treatment in social contexts unrelated to those where the data was originally collected. Lastly, Art. 5(1)(d) refers to real-time biometric systems used in public spaces for law enforcement purposes. While the first three categories are banned *tout court*, remote biometric systems are prohibited only partially, with several exceptions[2056].

Title III regulates AI systems that entail high risks for health, safety and fundamental rights (Art. 7(2)). Only two sub-categories of AI technologies are discerned in this area: systems that are products or safety components of products covered by EU legislation on health and safety (e.g., toys, machinery, lifts, medical devices); and "standalone" systems employed in specific domains as listed in Annex III[2057]. These technologies will be subject to extensive requirements to be placed in the market, including safety controls, a risk management system (Art. 9), data quality criteria (Art. 10), record keeping (Arts. 11-12), transparency (Art. 14), human oversight (Art. 14), accuracy, robustness and cybersecurity (Art. 15).

Lastly, Title IV applies to limited-risk AI technologies, namely systems intended to interact with natural persons (i.e., "bots", Art. 52(1)), emotion recognition and biometric categorisation applications (Art. 52(2)), deep fakes (Art. 52(3)). The draft legislation merely foresees transparency and disclosure obligations for these systems, except for when these are used by law enforcement agencies.

5. Critical analysis: Governance and surveillance in European smart cities

A difficult balance. Clearly, the prospective EU data governance framework is underpinned by varied principles, which need to be adjusted in a coherent and balanced fashion. On the one hand, all the proposals are based on Art. 114 TFUE, which indicates that their primary objective is strengthening the internal market (and arguably innovation). In this respect, it is not clear why the DGA and DA have

[2054] Id., p. 3.

[2055] From its publication the Proposal presented a complex and intricate set of rules, difficult to summarise. This brief overview aims to give a comprehensive picture of the proposal, but it is important to notice that at the time of writing, the draft AI is under legislative process and affected by thousands of amendments. See Bertuzzi (2022).

[2056] For an analysis of this provision see also Chapter IV, §2.3.2.1.1.

[2057] These are: biometric identification and categorisation (beyond the scope of Art. 5); management and operation of critical infrastructure; educational and vocational training; employment, worker management and access to self-employment; access to and enjoyment of essential services and benefits; law enforcement; migration, asylum and border management; administration of justice and democracy.

not also been grounded on Art. 16 TFUE, which refers to the processing of personal data. On the other, EU institutions are also trying to distance themselves from a purely market-oriented model and stress the importance of EU values and fundamental rights in this new framework.

Outline. Despite the good intentions, the proposals have already been hit by stark criticism upon their release. To some, they feature a fragmented and market-led approach to data governance and lack a serious fundamental rights perspective[2058]. In smart cities, such deficiencies may strengthen a neo-liberal vision of urban data governance and a capitalistic take on surveillance. That is why it is important to uncover the gaps in the prospective framework and highlight their implications for smart city governance. In the following subsections, the ambiguous terminology and inconsistent conceptualisation of data *for* the public good (and *as* a public good) in the proposals will firstly be scrutinised. Secondly, it will be shown how the proposals actually struggle to put forward an alternative model to the data economy. Thirdly, some gaps in the fundamental rights protection will be highlighted. Lastly, the implications for surveillance in smart cities will be examined.

5.1. An inconsistent conceptualisation of data for the "Public Good"

Poor conceptualisation. Even if the EU governance proposals highly build upon the concept of data for the public good, its conceptualisation turns out to be fragmented[2059]. At the outset, inconsistencies stem from the terminology employed in the proposals. On the one hand, data is characterised as a "non-rival good" both in the *European strategy for Data* and the Draft DA (Rec. 6). The concept of "public good" is also mentioned in Rec. 67 of the same draft, where it identifies the need to "respond to public emergencies".

The proposal employs the term "public interest" to refer to legitimacy grounds that authorise data sharing in situations of public health and environments emergencies, major natural disasters and cybersecurity incidents (Rec. 57)[2060].

On the other hand, the expression "general interest" prevails in the draft DGA (e.g., Rec. 35), where it is mentioned in the legal definition of "data altruism" (Art. 2(10)). To define the same concept, however, the Explanatory memorandum to the proposal refers to the "common good"[2061]. The same notion is used interchangeably with that of "public good" in the *European strategy for Data*[2062].

Detangling incoherent terminology. A systematic interpretation is thus needed to navigate through these related concepts. Indeed, the EDPS notes that expressions like "public good" and "public interest" in the *European strategy for Data* are to be understood as synonyms[2063]. The same could be said for the term "general interest", which is used in Art. 52(1) CFREU to identify legitimacy grounds to interfere upon fundamental rights. In all these cases, these expressions point out to collective needs of society which justify limitations of individuals' rights. Sometimes, the issue may be just a poor choice of terminology. The legislators uses the term "good" not to qualify *objects*, but *goals* such as "responding to public emergencies". For these latter cases indeed, the term "interest" would arguably be more appropriate. In other cases, data itself is conceptualized as a "public good", as in the *European Strategy for Data*[2064].

[2058] Solano et al (2022), pp. 48 ff. See also Veale et al (2021); Papakonstantinou et al (2022).
[2059] Solano et al (2022), p. III.
[2060] However, municipalities complain that the notion of public interest is not clearly defined in the draft DA, see Dragonetti (2021).
[2061] European Commission (2020) Data Governance act, p. 8.
[2062] European Commission (2020), p. 6.
[2063] EDPS (2020) Opinion 3/2020 on the European Strategy for Data, par. 21.
[2064] European Commission (2020), p. 7: "Data from the private sector can also make a significant contribution *as* public goods" [emphasis added].

Sometimes, however, selecting one term over the other may have deeper legal consequences. For example, that is the case when data is defined either as a "public" or "common" good. A brief digression about how these concepts are conceived in philosophy and economics may explain why.

Public and common good in philosophy and economics The concepts of common and public good have been highly discussed in political philosophy. As a model of moral reasoning, the *common* good generally refers to material and non-material facilities that individuals provide to other members of their community to pursue certain common interests[2065]. On the contrary, the concept *public* good draws from insights of economic theory[2066]. It refers to goods that communities would not possess if each member was motivated by their self-interest[2067]. Public goods are both non-rival and non-excludable, and should be open and available for everyone's benefit.

Should data be a public or common good? From a governance and surveillance perspective, it is important to clarify which kind of good data should stand for in the EU. It may be perfectly acceptable to use different labels interchangeably in public and policy discourse, as long as the actual conceptualisation and its legal consequences are clear. In technical terms, defining data as a public good may imply that it should be handled through open access regimes, or at least that its circulation should be boosted with very little restrictions. This appears to be the vision of the Commission, which identified data as a non-rival resource in two instances.

Nonetheless, this option is highly problematic because it does very little to restrain the flow of data where needed and could actually serve the interests of the most powerful actors in the data economy. On the contrary, treating data as for common good entails acknowledging that data is both rivalrous and excludable, and that barriers to data flows should be set to ensure stewardship by relevant communities. Arguably, this should be the vision underlying the EU governance framework, but does not seem to be adequately implemented at this stage, as will be shown below.

5.2. The balance is tipped in favour of corporate interests

Making the interests of the data economy? The EU data governance framework was also criticised for balancing private and public interests in an unclear manner[2068]. Specifically, the stakes of corporate actors seem to be prioritised across legislative instruments, as will be shown next.

5.2.1. The Data Governance Act

G2B data sharing. This imbalance emerges clearly in the approved DGA draft. Firstly, the proposal provides a framework only for G2B data sharing, and not the other way around. Therefore, the Act arguably lacks incentives for data transfers from the private sector towards public entities acting on general interests. Such a framework is only foreseen in the DA, but under very exceptional circumstances and burdensome administrative requirements.

The role of data intermediation services. Secondly, provisions on data intermediation services do not seem to challenge the overall structure of the data economy. On the contrary, these entities are designed to play a "key role" in this context (Rec. 22). Through the proliferation of these independent data intermediaries, the Commission wished to downsize Europe's dependence on big data platforms. However, these services reproduce themselves a "platformised business model" and may lead to a new

[2065] Hussain (Spring 2018 Edition), par. 1.
[2066] Id., par 2.
[2067] Id.
[2068] Solano et al (2022), p. III.

centralisation of power in the data economy in the future [2069]. Data sharing services are meant to act for-profit (Rec. 22) and thus rely on the traditional idea of data as a commodity. Therefore, they are expected to make money by pooling and selling data. Furthermore, this governance model is inspired by PDS, which bears a highly individualistic focus[2070]. The lack of collective data management mechanisms is thus unlikely to rebalance power differentials in the data economy. To be truthful, Rec. 26 indicates that data sharing services should "bear fiduciary duty towards the individuals, to ensure that they act in the best interest of data holders". Nonetheless, a similar provision is not reiterated in the operative body of the Act. Art. 11 certainly provides some safeguards regarding the independence of these entities, but the centrality of individuals' interests in data transactions cannot be ensured.

Under-incentivised data altruism. Thirdly, the role of data altruism organisations is heavily downsized with regard to data intermediaries. Indeed, altruistic entities are meant to act independently and not for profit (Art. 16), and will also be overburdened by intricate administrative requirements. In addition, enlisting on the dedicated registry will be voluntary, thus the incentives to handle data on altruistic grounds are not clear in the proposal[2071]. Because the altruistic processing was not exempted from the scope of the GDPR, charitable entities will also have to comply with it and data subjects will be entitled to withdraw their consent at any time (Art. 22(3)). Overall, processing for the common good/general interest appears severely curtailed in the DGA, to the advantage of corporate logic in the data economy.

5.2.2. The Data Act

B2G data sharing. The draft DA is possibly the piece of legislation where the imbalance between private and public interests is the most striking. The Act provides for a B2G data sharing framework with a very limited scope. Transfers of data from the private to the public sector can occur only in situations of exceptional need, i.e., to tackle public emergencies and major disasters. Hence, B2G schemes will probably struggle to reach the same traction of G2B sharing, which instead represents a long-standing policy of the Union.

Art. 14(1) of the proposal places an obligation on public authorities to demonstrate an exceptional need to use the data requested. Remarkably, a similar burden of proof is not foreseen for private entities in the DGA, although data transfers remain non-mandatory for public authorities. Art. 15 details the circumstances under which data should be made available. It foresees different balancing exercises that become increasingly demanding for public bodies as long as the intensity of public interest goals lowers.

Firstly, data should be disclosed when it is "necessary to respond to a public emergency" (Art. 15(a)). Secondly, when there no ongoing public emergency, data can be transferred only to prevent or recover from one. However, sharing will be in this case "limited in time and scope" (Art. 15(b)). Thirdly, when the lack of data can prevent the public body from fulfilling a specific public task, data can be made available under two additional alternative conditions.

On the one hand, the institutions should not be able to get access to data by alternative means, including by "purchasing the data on the market at market rates", or by adopting a new legal basis for the transfer (Art. 15(c)(1)). On the other, accessing the data under the DA would "substantively reduce the administrative burden for data holders or other enterprises" (Art. 15(c)(2)). When data is

[2069] Vogelezang (2022).
[2070] See Rec. 23. Some of these services are indeed meant to create "personal data spaces".
[2071] Veil (2021).

transferred pursuant to Art. 15(b) or (c), public bodies may also be requested to compensate private companies (Art. 20(2)).

Public bodies should comply with administrative procedures to access data. Art. 17 lists several requirements that institutions must abide by when requesting data. These include specifying the data and exceptional need at stake, the intended use of the data, the legal basis for the transfer. The request is to be expressed in a clear, plain and concise language and should be proportionate to the exceptional need invoked. If these conditions are not met, access to data may be denied (Art. 18(2)(b)). Importantly, private companies are the ones tasked with assessing compliance with these requirements. This means that sensitive decisions like proportionality assessments in public urgency situations are placed in their hands. Private entities may also refuse access due to more subtle requirements like linguistic clarity of the request, or when data has already been transferred to another institution (i.e., once-only principle, Art. 18(3)). Once again, it should be noted that similar procedural conditions are not foreseen for G2B data sharing in the DGA.

Impact on smart cities. The DA can have a significant impact on smart cities that should rely on privately held data to develop. In fact, data collected by public entities is not always sufficient to build a detailed picture of the city. Local authorities may often need to access other datasets about urban mobility (e.g., ridesharing), tourism and finance, which go beyond their administrative capabilities[2072]. Therefore, it is now common for municipalities to ask private companies for access to their datasets, under conditions that are not always profitable or ethically responsible for cities[2073]. At present, B2G data sharing occurs under different strategies, including data donorship, public data procurement, data partnerships (data collaboratives), data sharing obligations for renewal of contracts, and other contractual/voluntary arrangements[2074]. These practices are highly fragmented and often fail to evolve in more stable and sustainable initiatives[2075]. Regrettably, DA provisions on B2G sharing may be a missed opportunity to build a consistent legal framework and boost data sharing for public interest goals.

Indeed, conditions for data access by the public sector are too limited. These are only restricted to emergency situations, while cities require data for day-to-day management and development. Also, the proposal does not address power imbalances that small and medium-sized cities face with regard to corporate actors. For instance, bigger and well-known cities are often better placed in the data market. They easily cooperate with private firms that donate their data in exchange for a setting where they can develop their technologies. These are then sold to smaller cities, which not only lag behind in terms of innovation, but also need to pay to enjoy services that other municipalities got for free[2076]. Arguably, the DA may have the potential of establishing a level-playing field for cities of any size in Europe[2077], but could fail to do so. In fact, cities may even be required to turn to the market first to purchase data to pursue their public interest tasks. The proposal potentially subjects them to financially detrimental strategies: the value of data, as an "experience good", is unknown until it has been used for a particular

[2072] Bass et al (2018), p. 12.
[2073] Id. For example, the company Strava charges $0.80 for local authorities to have access to the mobility data of each user. The map application Waze, instead, exchanges its own mobility data for real-time data about local construction across the city. See also examples provided by Dragonetti (2021).
[2074] See Micheli (2022).
[2075] High-Level Expert Group on Business-to-Government Data Sharing (2020), p. 32.
[2076] Micheli (2022).
[2077] Christofi et al (2022).

purpose[2078]. Before being able to access data under the DA, therefore, they may be forced to buy data blindly, without being certain of their quality or aptitude to solve their issues. Moreover, the condition foreseen in Art.15(c)(2) is problematic having regard to "quality of law" requirement. Indeed, EDPS and EDPB have stated that the mere reduction of the administrative burden will unlikely outweigh the impact on the fundamental rights and freedoms of the persons concerned[2079]. Hence, the prospective framework seems only to foster a neo-liberal governance model for smart cities. By setting such high thresholds for B2G sharing, it ultimately strengthens corporate interests by making municipalities more and more dependent on private datasets.

5.2.3. The Artificial Intelligence Act

5.2.3.1. Self-regulatory aspects

The NLF in the draft AIA. As stated, the draft AI is underpinned by a risk-based approach which bears the risk of prioritising corporate interests in co-governance frameworks. The primary role that private AI manufacturers are given in the AIA is exemplified by the adoption of the so-called "New legislative framework" (NLF). Under these regimes, manufacturers make pre-marketing controls to certify their products' safety and performance. Approved items are marked with the CE label and can move freely within the internal market. Echoing the principle of accountability in data protection, the NLF builds on the assumption that manufacturers are the best placed to assess the safety features of their products.

Under the operativity of the AI Act, these conformity self-assessments will be mainly performed through harmonised standards. By complying with these, manufacturers enjoy a presumption of conformity with the essential requirements foreseen for high-risk systems (Art. 40). However, the formulation of these standards is delegated by the EU legislators to two private bodies (i.e., European Committee for Standardization and the European Committee for Electrotechnical Standardization). Critically, this has been described as a potential "constitutional bomb" within the NLF framework[2080]. Indeed, technical standards entail important value-laden choices (e.g., thresholds of acceptable risks) that are being outsourced to the private sector[2081]. Unsurprisingly, the social and ethical implications of standards is being recognised by the CJEU, which is starting to subject them to judicial scrutiny[2082].

Private bodies' self-assessments acquire even greater importance as notified bodies are attributed a very limited role in the governance framework. These are typically private sector companies that are accredited to national notifying authorities[2083]. In the draft AI Act, only high-risk systems within the area of biometric identification and categorisation of natural persons will be subject to the oversight of notified bodies. Outside this domain, only self-assessments based on harmonised standards will suffice. Many high-risk AI systems may be placed in the smart city market only based on the assessments of their manufacturers', which are left with large spaces for self-regulation. Additionally, strong public accountability mechanisms are not foreseen, and the lack of individual redress mechanisms could make matters worse, as will be shown below.

2078 High-Level Expert Group on Business-to-Government Data Sharing (2020), p. 17.
2079 EDPB-EDPS (2022), §79 ff.
2080 Veale et al (2021), p. 105.
2081 Id.
2082 See CJEU, *Fra.bo SpA v Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) — Technisch-Wissenschaftlicher Verein*, judgment of 12 July 2012, Case C-171/11.
2083 Id., p. 106.

5.2.3.2. The missing human rights perspective

Missing mechanisms of public contestation. The draft AI Act has been criticised for lacking a comprehensive fundamental rights perspective[2084]. The legislation is mainly built around EU product safety law and does not address harm to either individual or collective human rights prompted by AI use. The lack of human oversight and individual redress are likely the most striking features in this sense. On the one hand, no obligation in the AI Act directly targets the users, which are merely required to follow instruction manuals prepared by manufacturers. This may raise accountability problems, as AI users may argue to exclude their responsibility for harm if such instructions were diligently followed. With general purpose AI, the lack of human oversight may raise further issues because users can reconfigure the technology for specific uses and raise unforeseen human rights concerns. In these situations, a more granular human rights assessment should be carried out by the user directly, but a similar requirement is not foreseen in the proposal[2085]. Yet, the Council's general approach in December 2022 tries to downsize the risks associated to general purpose AI, by extending the requirements of high-risk systems also to these technologies, although not automatically. Specifically, an implementing act should establish how they should be applied in relation to general purpose AI systems, based on a consultation and detailed impact assessment and taking into account specific characteristics of these systems and related value chain, technical feasibility and market and technological developments[2086].

On the other hand, individuals interacting with or being targeted by AI are not foreseen as "subjects" in the legislation. Only manufacturers and users are mentioned, alongside importers and distributors of AI products (see Art. 3). Absent figures in the legislation, individuals are not provided with rights to redress, like in data protection law. Therefore, victims of erroneous identification by facial recognition, social scoring and manipulation, or malfunctioning of drone software do not avail of a right to effective remedy under this specific framework. Certainly, a right to effective remedy under the GDPR or the LED may be available if the system was processing personal data. However, this state-of-play conveys a fragmented and obsolete conceptualisation of technology harm in EU governance[2087]. Because harm is seen either through the lens of data protection, competition or consumer protection, a unitary conceptualisation thereof is missing and gaps between legislative instruments may sometimes leave individuals unprotected. For instance, systems that do not process personal data are left uncovered[2088].

Persistent categories in data governance. The above-mentioned issues result, among other things, from the persistent distinction between personal and non-personal data in governance. Indeed, only systems that process personal data are subject to redress mechanisms under data protection law. Nonetheless, the risks associated with AI technologies go well beyond individual rights and freedoms and may involve groups and society as a whole[2089]. In this sense, the AI Act is a missed chance to address the impact of AI on communities for the first time and give fundamental rights a more collectivist focus[2090]. This might have been crucial also for a more human-driven development of smart city governance. Indeed, the application of EU data protection law remains a highly debated issue for several urban technologies,

[2084] Solano et al (2022), p. 51; Veale et al (2021).
[2085] With reference to AI leveraging personal data processing, see EDPB-EDPS (2021b).
[2086] Council of the European Union (2022), p. 6.
[2087] See Solano et al (2021), p. IV.
[2088] This was criticised by EDPB-EDPS (2021b), §18.
[2089] Id., §5.
[2090] An exception may be found in the notion of social scoring that takes into account unfavourable AI uses affecting "certain natural persons or whole groups thereof" (Art. 5(1)(c) (i-ii)).

which could include crime mapping software, biometric classification systems or other nudging systems[2091]. Companies marketing these technologies often argue for the non-applicability of data protection to implement questionable data-driven initiatives. If AI is meant to create public value, however, its governance should adopt a broader societal perspective and incentivise good behaviour by users and providers, regardless of whether individual data protection rights apply[2092].

Limited scope of prohibited practices. The scope of prohibited practices under Art. 5 is very limited despite the numerous human rights implications of AI systems. Manipulative applications foreseen in Art. 5(1)(a-b) rely on a common sense notion of manipulation, without engaging in a detailed legal definition[2093]. Art. 5(1)(a) refers to "subliminal techniques beyond a person's consciousness" that individuals "cannot perceive" (Rec. 16), although these should not necessarily be covert[2094]. This means that not all nudging systems may be considered "manipulative" under the AIA: individuals may be aware of their interaction but unconscious of the techniques employed to distort their behaviour. In behavioural science, manipulative systems are those that leverage the most automatic and intuitive cognitive operations of the mind (the so-called *system 1*)[2095]. However, the exact definition of manipulation remains unclear in the proposal. For instance, it is not straightforward whether this prohibition would extend to nudging systems of which the individual is aware, but whose manipulative techniques cannot really be grasped by the target. Additionally, it is unpredictable how this definition will be interpreted by market actors.

Moreover, AI use may not be unacceptable only because the individual's behaviour is distorted and re-directed towards the ends of the nudging agent[2096]. Physical or psychological harm to that or another person is also required. This additional condition is likely meant to open the door to "well-intentioned" uses of nudging (e.g., for environmental purposes) and may foster smart cities' paternalistic agendas in the future[2097].

Nonetheless, the harm requirement could be highly problematic and difficult to prove. In fact, harm may not originate from a single serious event but accumulate over time[2098]. Also, Rec. 16 explicitly excludes harm that arises from user-behaviour in conjuncture with AI software, overlooking significant areas like discriminatory ratings, dating apps and online markets[2099]. Similar applications are not unknown to neo-liberal smart cities, which integrate in their environment technologies that are marketed by big corporations. For instance, this might be the case of data collected by traffic management systems (e.g., Google's *Flow*) that may be used to fuel unrelated online markets, e.g., private parking.

On a different note, Art. 5(1)(b) envisages manipulative systems that exploit people's vulnerabilities. Nonetheless, the provision incorporates a very limited range of vulnerabilities. This list not only excludes some traditional proxies for discrimination (e.g., gender, sexual and political orientation), but also fails to acknowledge the dynamics of contemporary profiling which relies on hundreds of dynamic variables relating to behaviour.

2091 See the analysis in Chapter I, §2.4.2.2. and the technologies examined in Chapter IV.
2092 Solano et al (2022), p. III.
2093 Veale et al (2021), p. 99.
2094 *Contra* Veale et al (2021), p. 99. It is true, however, that nudging systems are considered to work better if individuals are not aware of them.
2095 See Chapter IV, §5.2.
2096 Veale et al (2021), p. 99.
2097 See Chapter IV, §5.1.2.
2098 Veale et al (2021), p. 99.
2099 Id.

Social scoring can have salient implications for smart cities and poses serious fundamental rights concerns. Yet, Art. 5(1)(c) bans these practices only when several cumulative conditions are satisfied. Firstly, social scoring is prohibited solely when it occurs "over a certain period of time", which makes one-time assessments acceptable (although high-risk).

Secondly, the ban only concerns the use made by public authorities (and entities acting on their behalf). The reason for this limitation is not clear in the proposal and leaves a great margin of appreciation to private actors in crucial fields for smart cities, e.g., telecommunications and transport[2100]. Importantly, the Council's general approach on the proposal in December 2022 extended the prohibition of AI social scoring to private actors as well, thus showing greater sensitivity to the matter[2101]. However, it remains to be seen whether this provision will stay in the final version of the text.

Thirdly, the draft forbids social scoring only if it leads to certain outcomes, which are narrowly defined. Art. 5(1)(c)(i) provides that AI systems should not build unfavourable assessments on data collected in an unrelated context. This provision could address citizen scoring that usually relies on corporate datasets, although the dividing line between private and public data may not be clear-cut in all contexts[2102]. The rationale for this limitation is also not clear, considering that social scoring based on public data only may be no less problematic.

Under Art. 5(1)(c)(ii) instead, social scoring becomes unacceptable when it leads to unjustified or disproportionate effects in relation to the assessed social behaviour. Regrettably, the operativity of this prohibition may also be limited. Indeed, individuals may struggle to prove the causal link between the scoring and the targeted behaviour. Likewise, the "unjustified or disproportionate" effect of the scoring should in principle be assessed by private manufacturers, with no accountability mechanisms.

Lastly, remote biometric identification in public spaces by law enforcement has sparked an intense debate in Europe. While its use is in principle forbidden by the Act, Art. 5(1)(d) provides for many exceptions which could eventually overturn the ban. The EDPB and EDPB have also censured these requirements for being vague and occasionally unjustified. For instance, the Act only addresses real-time facial recognition, even if the intrusiveness of the processing does not necessarily depend on whether the identification is contextual or *ex post*[2103]. Neither does it depend on its purpose. Law enforcement authorities may be left with wide margins of appreciation in deciding whether to deploy facial recognition. The EDPB and EDPB warned that the potential number of suspects and offenders will almost always be "high enough" to justify the continuous use of AI systems in public places. Therefore, they called for a total ban of the technology[2104].

It should be highlighted, however, that the considerations of the two data protection bodies do not seem to reject the theoretical applicability of AFR by law enforcement altogether. Rather, they arguably show mistrust with regard to the strict application by police forces of the proportionality requirements laid down in the proposal. This may suggest that – at least at the theoretical level – facial recognition technologies may not be in stark contradiction with the European human rights framework when it comes to identifying warranted people and suspects of serious criminal offences. This is coherent with

[2100] Id., p. 100. Notably, the EDPB and EDPS have called for a ban of *any* kind of social scoring, see by EDPB-EDPS (2021b), §29.
[2101] Council of the European Union (2022), p. 4.
[2102] Veale et al (2021), p. 100. The Commission made the example of a system identifying children in need of social care, leveraging data about the parents' irrelevant misbehaviour (e.g., missing a doctor's appointment or divorce).
[2103] EDPB-EDPS (2021b), §31.
[2104] Id., §32.

the taxonomy proposed in Chapter IV, which assimilates AFR with "hybrid-targeted" systems of surveillance. These certainly entail major interferences with fundamental rights, but their use may be proportionate with regard to strong public security issues mainly linked to the fight against serious crime. Importantly, this restricted instance of application should be kept distinct from other case scenarios analysed in this work: respectively, cases where matching databases are enlarged beyond what is strictly necessary (i.e., Clearview), and those where affective states are indiscriminately inferred from anyone passing through the range of the smart camera (i.e., EFR).

In December 2022, the Council's general approach tried to address some of these issues by further clarifying the objectives where the use of remote biometric identification could be considered strictly necessary. Specifically, AFR could be used not only to prevent terrorist attacks and serious threats to individuals' life and physical safety but also to avert similar menaces to critical infrastructure. Also, the new wording of the provision seems to restrict the preventive uses of the technology. Specifically, Art. 5(d)(iii) now leaves out the term "detection" and allows to leverage AFR only for the identification and localisation of people suspected or accused of serious criminal offences. The categories of crime legitimising these uses have also been further clarified. Alongside those listed in Art. 2(2) of the EAW Framework Decision, the provision now includes also criminal offences punishable in the concerned Member State by a custodial sentence or a detention order for a maximum period of at least five years. This restriction should be welcomed, although it does not exclude any preventive use of the technology. Such employment is still foreseen for serious threats to individuals' life and physical safety, which arguably includes behaviours qualifying as criminal offences.

Flawed conceptualisation of risk. Lastly, the proposal determines AI risk levels according to different factors, including the (i) the type of AI system; (ii) its domain of application and (iii) its human target[2105]. Therefore, the same kind of AI application may be assessed differently based on its concrete use. One example is represented by biometric classification systems. These are generally classified as limited-risk AI but may occasionally fall within other categories like high-risk (in the law enforcement domain) or unacceptable uses (manipulation). If this classification system has been criticised for being arbitrary[2106], it may also fail to grasp the real human rights implications of some surveillance technologies. As shown in the analysis of EFR, systems labelled as low or high-risk may actually be incompatible with the Charter since they violate the essence of the right criterion[2107]. Indeed, legitimising AI founded on pseudoscience may be one of the "original sins" of the AI Act. Lastly, it should be noted that the AI overlooks the environmental challenges posed by AI. Mandatory requirements for AI high-risk systems do not comprise any commitment against environmental impacts and this may undermine the sustainability of such systems in the future[2108].

The Council's general approach in December 2022 seems to take into account some of this criticism. Indeed, it introduced an additional criterion in the qualification of high-risk systems, which precisely focuses on the potential fundamental rights risks that given AI tools could cause[2109]. Hence, it would be desirable if such provision stays in the final version of the Regulation.

[2105] Malgieri et al (2021).
[2106] Solano et al (2022), p. 52.
[2107] See Chapter IV, §2.3.2.1.
[2108] Pagallo et al (2022).
[2109] Council of the European Union (2022), p. 5.

5.3. Surveillance implications

5.3.1. Management of data flows

Purpose limitation-inspired provisions. While advancing data circulation in the internal market, the DGA and the DA also include barriers to data flows in certain situations. There are several provisions inspired by the principle of purpose limitation, which applies in data protection law but does not extend to the processing of non-personal data. Indeed, the issue of reckless data repurposing affects EU data governance on a broader scale, but both the DGA and the DA seek to find some balance between data sharing and the risks of unwarranted surveillance and profiling.

In the DGA, the concept of "re-use" identifies the repurposing of data held by the public sector for both commercial and non-commercial purposes, excluding G2G sharing (Art. 2(2)). The conditions set by the public institution should be objectively justified in relation to the purpose for which the data should be reused (Art. 5(2)). Therefore, public authorities might potentially lay down stricter conditions (and fees) for data repurposing that poses higher fundamental rights risks. Indeed, Art. 6(4) incentivises public authorities to impose lower fees when disclosing data to small and medium-sized enterprises (including civil society organisations) for non-commercial purposes (see also Rec. 25). Data reuse can be authorised by the public sector only if data is anonymised, pseudonymised or devoid of commercially confidential information (Art. 5(3)). When complying with these conditions is not possible under the GDPR, public bodies should help re-users to obtain the consent of data subjects, or the permission of the legal entities affected by the reuse to further process the data (Art. 5(5)).

When data is to be transferred from the public to the business domain, more stringent conditions should apply. For instance, Rec. 19 advises public bodies to not allow the repurposing of data stored in e-health applications to insurance undertakings and other services providers with the aim of setting discriminatory prices.

Within the commercial sector, data intermediation services are also subject to high requirements of neutrality with regard to the data they exchange. Art. 11(1) foresees that such providers should not use data for other purposes other than making them available to data users (see also Rec. 33). Likewise, data altruism organisations are mandated not to use the data for purposes other than those of general interest that originally justified the collection (Art. 19(2)). With regard to data reuse for research purposes, Rec. 50 recalls Arts. 5(1)(b) and 89(1) GDPR, the so-called research exemption. For non-personal data instead, the conditions for reuse should be set in the permission given by the data holder to the altruistic organisation.

In the DA, purpose limitation applies to data sharing between the user of an IoT device and the third-party recipient of his or her data. The third-party can process the data only for the purposes and under the conditions agreed with the user and should apply data protection requirements where necessary (Art 6(1)). Rec. 33 clarifies the rationale of this provision, which is avoiding "the exploitation of users". Also, the third-party cannot use the data to develop a product that competes with that of the data holder (i.e., the manufacturer of the user's IoT device), nor can it share such data with another third-party for the same purpose (Art. 6(2)(e)).

In B2G sharing, Art. 19(1)(a) provides that public authorities having received data for an exceptional need should not use the data in a manner that is incompatible with the purpose for which they had been requested. Nonetheless, Art. 21(1) foresees a research exemption, and provides that public authorities having received data under the DA can further transmit it to individuals or organisations for scientific research or analytics purposes, or to national and EU bodies compiling official statistics. Rec. 68 indicates that public authorities are entitled to share the data only if they cannot perform the

processing themselves, but this provision is not reiterated in the operative body of the Act. Further, public authorities having received data under exceptional circumstances cannot make it open under the Open Data Directive.

Inconsistent barriers of data flows across sectors. These rules mirror a highly fragmented picture of the EU data governance framework. Even a systematic reading of the Acts provides a scattered vision of how data flows are regulated across the commercial and public sectors, as well as civic society.

While the system arguably pushes data circulation in the business domain more intensively, the legislator also shows concerns over the possible exploitation of data against individuals. However, the provided safeguards do not always set a high threshold of protection. Repurposing of health data from the public sector to businesses is advised against only in the recitals, rather than in the operative body of the DGA. Also, barriers to data flows in consumer-business transactions are mainly left to the determinations of contracting parties. Given the power imbalances in the data economy, individuals may not be able to negotiate strict conditions on the reuse of their data, and for-profit data intermediaries may not play a salient role in this matter. Furthermore, requirements of purpose limitation equally apply when the processing occurs in the public interest.

Compared to the commercial sector, this state of play may raise higher barriers to data flows involving altruistic organisations, even when data processing aims to serve common good purposes. This is also shown in the incoherent approach that underlines data repurposing for research in this field. For instance, the GDPR may easily allow altruistic organisations to repurpose collected data under Arts. 5 and 89, while permissions given by individuals to use their non-personal data may exclude such reuse. Therefore, repurposing of non-personal data in research may occasionally be set to a higher standard for altruistic organisations.

Overall, data flow barriers seem lower in business sector. Once data enters this domain (e.g., from the public sector), purpose limitation continues to apply to personal data (Art. 5(5) DGA), but not to non-personal data. On the contrary, public interests pursued by the public sector or non-profit entities are occasionally siloed and subject to inconsistent thresholds for data reuse (e.g., in research). Arguably, this may again suggest a more business-oriented vision of EU data governance, while surveillance for common good purposes appears to lie in the background.

What governance for common European data spaces? Things become even more complicated when the concept of European data spaces is introduced into the picture. The *European Strategy for data* aims to build a "single European data space", that is a market to exchange both personal and non-personal data (including business-sensitive ones) in a secure way and in compliance with EU law and values[2110]. "Common European data spaces" should also be established in strategic fields within the single market. These are defined as "governance structures" comprising both legal rules on data sharing and technical interoperability standards across sectors[2111]. The Commission envisions nine sectoral data spaces in health, mobility, manufacturing, financial services, public administration (including law enforcement), education and training, Green Deal and manufacturing[2112].

The concept of European data spaces is recalled both in the DGA and the DA, although not in a comprehensive fashion. Rec. 2 of the DGA refers to them as "concrete arrangements in which data

[2110] European Commission (2020), pp. 4-5. Fostering interoperable information sharing, however, mainly originated in the AFSJ and thus is not a new policy objective in the EU, see Curtin, Brito Bastos (2020).
[2111] Id., p. 12.
[2112] Id., pp. 21-22.

sharing and data pooling can happen". Importantly, relevant stakeholders in these data spaces should be represented and able to participate in the governance of these resources (Rec. 3). In the DA, common European data spaces are also evoked, but the concept is left underdefined[2113]. The Act implements the vision only in relation to technical standards of interoperability and does not give details on rules for cross-sectoral sharing[2114]. It remains unclear whether these two pieces of legislation are meant to provide a comprehensive data governance framework for data spaces already. Rec. 86 suggests that additional laws will be required to regulate data sharing within and across sectors[2115]. At the moment of writing, no specific governance structure defines stakeholders' rights to representation and participation within data spaces, except for the European Health Data Space (EHDS) proposal[2116]. Such rules should echo more community-inspired data governance models (e.g., the commons, data cooperatives), which are currently underrepresented in the prospective EU framework.

Cross-sectoral data sharing towards law enforcement. Likewise, no specific rules for cross-sectoral data sharing seem to have been published yet (except for the EHDS). Therefore, any discussion thereof would be highly speculative at this point. Nonetheless, an inconsistency may be highlighted. The *European Strategy for Data* designs the "public administration data space" not only to address e-government needs, but also law enforcement ones.

Certainly, law enforcement authorities may benefit substantially from being included in data spaces governance. Financial or mobility data coming from both the private and public sector may be of use to law enforcement to identify promising targets of investigation/crime prevention, and thus manage their resources more efficiently. However, these sharing operations are also fraught with surveillance implications that should be addressed in future legislation[2117].

For instance, mixing e-government and law enforcement objectives in the same data space may not be the most appropriate solution, due to the specificities of the latter. It would be highly problematic if data within the public administration space could be accessed by law enforcement with no or very little restrictions. In this regard, the *Strategy* pointed out that "B2G data sharing should not include the use of data for law enforcement purposes. Any action in this area should comply with data protection and privacy legislation"[2118]. While this specification is welcomed, it begs the question of how flows of non-personal data towards law enforcement authorities (including at the local level) will be regulated in the future data space proposals.

Concerning data already in the possession of the public sector, for instance, Art. 16(2) of the DA forbids public institutions to reuse for law enforcement purposes both personal and non-personal data obtained under exceptional needs. Nonetheless, this adds further confusion to how EU institutions will regulate data flows within the future public administration data space. Data spaces are designed to pool

[2113] Solano et al (2022), p. 56.

[2114] Catanzariti and Curtin (2023b, pp. 135, 150) criticise this approach.

[2115] Indeed, in May 2022 the Commission published the first proposal to regulate such common data spaces, i.e., the European health data space. See European Commission (2022) Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. COM/2022/197 final.

[2116] However, Art. 64(4) of the European health data space proposal provides that "Stakeholders and relevant third parties, including patients' representatives, shall be invited to attend meetings of the EHDS [*ed* European Health Data Space] Board and to participate in its work, depending on the topics discussed and their degree of sensitivity". Similar provisions would be welcomed in further proposals. Cities (or associations thereof) could indeed act as relevant stakeholders in several data spaces, e.g., mobility, energy, public administration, Green Deal.

[2117] On the constitutional implications of interoperable data sharing in the security domain in the EU, see Curtin, Brito Bastos (2020). Catanzariti and Curtin (2023b) highlight implications of the interoperability between databases in the law enforcement and migration domains.

[2118] European Commission (2020) European Strategy for data, p. 7, note 22. Both the DA (Art. 1(4)) and the DGA (Rec. 3) do not affect the application of sectoral legislation for data access for law enforcement purposes.

data together, and yet data circulation may be curbed by the DA or data protection legislation. Personal data coming from the private sector will still be subject to proportionality requirements under the GDPR and public institutions may not always transmit their data to law enforcement authorities. Arguably, these inconsistencies show the segmented approach currently followed in EU data governance and call for a careful rethinking of the design of the public administration data space, possibly excluding LEAs. A more comprehensive picture will likely emerge when the interplay between the DA, DGA and upcoming sectoral data space legislation is uncovered in the future.

5.3.1. A divorce between knowledge and control

Big data and AI challenges. The new EU data governance pushes for wider and stronger data circulation in the internal market. It aims at fostering innovation through an increased availability of data, which is a crucial resource to develop AI. Nonetheless, data alone is not enough to harness the potential of AI solutions. Making sense of big data is not always an easy task. Training data may be messy, unstructured, lacking timeliness and dynamism, given that it may have been generated with no specific question in mind, as a by-product of another activity[2119]. On the other side, AI needs suitable and accurate data to learn from in order to solve a particular problem. The inclusion of unnecessary variables or datapoints in the model, may result in redundancy and inefficiency in the system[2120]. Likewise, when overly complex variables are introduced, the model ends up overfitting the training data and predictions may not be generalised beyond the data generated in a given context. That is why, data science and machine learning require expertise and thoughtful reflection about which data can be used and for which purpose[2121].

Data suitability in smart cities. Greater availability and circulation of data could bring significant value to smart cities relying on technologies to solve varied hurdles. Knowledge about cities has so far been built on "small data" studies (e.g., surveys and questionnaires), and the big data revolution promises to bring more sophistication to how cities are administrated[2122]. Predictive analytics are used, for example, to classify citizen travel patterns, categorise mobility and environmental behaviour of collective groups, predict household energy consumption and GHG emissions, or areas of congestion or dense traffic in the near future[2123]. Nonetheless, AI solutions raise their own challenges as well. Predictive models may be developed with unsuitable training datasets, where data is representative of a specific urban reality, or is analysed without taking the social environment it stems from into account. Analytics techniques may not be equally appropriate to make sense of a given urban issue[2124].

Neo-liberal smart cities and data positionality. The abovementioned issues may affect technologies marketed as one-fits-all solution in diverse urban contexts. If training data is not suitable to build the model, or if predictive techniques are not apt to solve the problem in a given city, AI solutions may lead to inaccurate predictions and ultimately biased policies. Arguably, this risk is exacerbated in smart cities under the influence of big corporations purporting neo-liberal agendas, which often offer technology solutions that disregard data as a resource generated in specific socio-technical contexts. The objective, neutral and universal value of data is often taken for granted, and correlations extracted by datasets are equally accepted at face value. Yet, urban geographers and data ethicists have stressed

[2119] Kitchin (2014), p. 100.
[2120] Id., p. 101.
[2121] Id., p. 104; Bibri (2018), p. 195.
[2122] Bibri (2018), p. 208.
[2123] Bibri (2018), p. 199.
[2124] Id., pp. 209-210.

the importance of considering the *positionality* of data[2125]. Data always speaks from a particular position because it is the product of a given social, political, technical assemblage that shapes its constitution[2126]. Correlations, if not subject to further contextual analysis, may lead to failures in decision-making.

A new paradigm of governmentality. This lack of correlation between data and decision-making in the digital era exemplifies a radical change in how governance and surveillance have been intertwined so far. When Foucault first theorised the concept of governmentality, he argued that knowledge (i.e., statistics) about the population were needed to correctly manage individuals, families and the State[2127]. That is why, between the fifteenth and sixteenth century, the process of "governmentalisation" of the administrative State had also relied on the design of techniques to surveil and control the population[2128]. After the digital revolution, this paradigm is being severely undermined. Governing a population no longer depends on acquiring knowledge about that specific entity. Data comes from a much wider variety of sources. This emerges explicitly in the new EU data governance framework. For instance, Rec. 24 of the draft DGA refers to a "novel, 'European' way of data governance, [which] provid[es] a separation in the data economy between data provision, intermediation and use". In other words, surveillance is still necessary for governance, but a divorce between knowledge and control is occurring.

EU data governance issues for smart cities. This segmented circulation of data in EU data governance may exacerbate the problem of data positionality in smart cities if due precautions are not taken. Technologies developed with unsuitable data (e.g., generated in big cities) may be applied in very different environments (e.g., small cities), potentially giving way to biased decisions.

However, the draft AI Act does not completely overlook the problem of data suitability and accuracy. Among the requirements of high-risk systems, Art. 10(2) requires that training, validation and testing data sets shall be subject to appropriate data governance and management practices, including: (a) the relevant design choices; (b) data collection; (c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation; (d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; (e) a prior assessment of the availability, quantity and suitability of the data sets that are needed; (f) examination in view of possible biases; (g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed. Training data must also be relevant, representative, free of errors and complete. They must have the appropriate statistical properties in relation to the individuals, groups and geographical settings in which the AI system should be used (Art. 10(3-4)). Therefore, data positionality should be a relevant factor when selecting datasets to train AI models.

Will this be sufficient to ensure data suitability in different smart city environments? The answer is not always clear-cut, and some examples may help identify potential gaps. Data governance requirements only apply to high-risk systems, and not all smart city applications will fall within this category. In the law enforcement domain, for instance, Art. 10 seems to offer adequate safeguards to develop accurate surveillance technologies such as predictive policing software (specifically, crime mapping)[2129]. Indeed, point 6(e) of Annex III of the draft AI Act appears to include these applications

[2125] Taylor (2019), p. 3; Kitchin (2014), p. 135.
[2126] Kitchin (2014), p. 135.
[2127] Foucault (1991), pp. 92-96. For a deeper analysis of governmentality, see Chapter IV, §2.1.
[2128] Id., p. 103.
[2129] Although civil society organisations are calling for a ban of these applications. See Fair Trials (2022).

in the range of high-risk systems[2130]. The provision refers to software designed to predict the recurrence of criminal offences, not only based on individuals' profiling, but also on past criminal behaviour of groups. Because predictive policing usually relies on aggregated historical crime data, data governance requirements should apply. Therefore, municipalities should be able to consult the technical documentation demonstrating the statistical representativeness of the training datasets.

The same can hardly be argued for systems predicting mobility patterns in smart cities. Point 2(a) of Annex III refers to safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity. These are included because their failure or malfunctioning may put the life and health of persons at risk on a large scale and disrupt ordinary social and economic activities (Rec. 34). Similarly, products subject to EU harmonisation legislation based on the NLF do not comprise similar systems[2131].

Although these do not have direct consequences on the life and safety of individuals, their use still has salient implications for smart city management. Administering urban transportation systems efficiently can significantly improve citizens' life standards and resource deployment. Policies in this field can also have discriminatory impacts over marginalised or vulnerable communities. For example, research has shown that women's mobility patterns are more complex than men's. Their transfers are less linear because they are generally responsible for household care and thus are more interested in frequency and quality of public transportation. Nonetheless, their needs have not been properly addressed in urban planning strategies so far[2132].

All of this shows that data governance requirements are also needed beyond the boundaries of high-risk systems. If these are trained with unsuitable datasets, AI models may produce predictions that are inaccurate or insensitive to the demographics and social issues of a given city. Once again, an inconsistent conceptualisation of AI risks may be the reason for this legal gap. In fact, the fallacies of AI-based policy making may not be grasped in the short term. Yet, in the long term they have significant repercussions for a human-driven governance of the smart city and thus should be adequately addressed in the Act.

5.4. Policy recommendations

Guidelines for smart city governance. Smart cities are important actors in the data economy and will be highly impacted by the new data governance framework. Therefore, policy recommendations should be put forward to shape how data will be handled in the EU market. Some of these suggestions focus on the overall EU framework, others address the smart city context specifically. These concern:

I. *Nature of the common good in EU governance.* The *European Strategy for data* and the ensuing Acts build upon the concept of common/public good. However, its actual implementation in

[2130] The provision reads: "AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups".

[2131] Specifically, Art. 1(3) of the Directive (EU) 2016/797 on the interoperability of the railway system excludes from its scope metros, trains, and generally urban and local transportation. Regulation (EU) 2018/858 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles may apply to some urban transportation vehicles, but concerns only their physical components, technical units and systems directly managing their functioning. Therefore, stand-alone AI models that analyse patterns in the overall urban mobility system do not seem to be covered by this legislation.

[2132] Study requested by the FEMM Committee of the European Parliament (2021), pp. 15 ff.

legislation needs further normative reflection[2133]. The EU model relies on the assumption that if data circulation is boosted, public value will be generated automatically. Further, data exploitation is considered essential to improve "decision making", but it is not explained what better decision-making is besides increased efficiency[2134], which is a leitmotiv in neoliberal smart cities. Therefore, this approach should be complemented with sectoral insights to identify needs, problems and opportunities for specific communities (e.g., unions, collectives, civic societies organisations)[2135]. These could be public-facing initiatives or union negotiations defining acceptable uses of data and technologies.

A spatial perspective should also be included. This means that smart city stakeholders should be involved as active actors in shaping what kind of public goods are to be generated through data and technologies. This entails involving societal groups *ex ante* in the choice of data-related initiatives and their implementation[2136]. Cultural, social and political perspectives of city inhabitants would thus be accounted for in the process and counter techno-solutionist approaches purported by big corporations. It should be noted that such recommendations already find limited space in the GDPR and are coherent with the more extensive interpretation of participatory DPIAs proposed in Chapter II[2137].

II. *Nature of data and technology.* The EU governance framework should be a chance for the legislator to overcome outdated classifications between data as personal and non-personal, sensitive and non-sensitive[2138]. Such distinctions have salient repercussions on several provisions of the DGA, DA, AIA especially (e.g., the underrepresentation of possible group harm). In smart cities, the separation between personal and non-personal data is often leveraged by technology actors to circumvent the application of data protection law. However, similar strategies should not push away broader assessments over the human rights implications of these technologies (see below).

Furthermore, data is mainly treated as a commodity both in the DA and the DGA. It is advised to conceptualise these resources as a common good. This requires governance structures ensuring data stewardship by relevant stakeholders (see below).

Similar concerns regard AI technologies, which are essentially conceived as products by the AIA. To generate public value and avoid harms, a fundamental rights perspective should be enhanced in the current proposal (see below). Competing interested in their deployment should be addressed both at the design and procurement phase, to ensure that a given system aligns with the public interest and needs of communities[2139].

III. *Balancing.* The EU governance framework is underpinned by mixed rationales. Despite the "public good" narrative, the balance of interests is often tipped in favour of corporate interests.

2133 Solano et al (2022), p. 58.
2134 Id.
2135 Id.
2136 It should be noted that avoiding this process has been turned out to be damaging in the past, as in the case of Quayside Toronto.
2137 Chapter II, §4.5.
2138 The CJEU has recently issued a decision to this effect. It ruled that the processing of (non-sensitive) personal data that can *indirectly* reveal sensitive information about a natural personal should also fall within the more protective regime under Art. 9 GDPR. See CJEU, *OT v Vyriausioji tarnybinės etikos komisija*, judgment of 1 August 2022, Case C-184/20.
2139 Solano et al (2022), p. 59.

Balancing mechanisms are also scattered in different pieces of legislation, which complicates the task of building a coherent framework.

Processing for public interest purposes is severely disadvantaged in the DGA and DA. It is thus advised that administrative burden is reduced for data altruistic entities and that B2G sharing is enlarged beyond circumstances of exceptional need. Outside emergency situations, smart cities should not be obliged to turn to the market for data rather than being able to access it directly through DA instruments. These changes could have a crucial impact on municipalities (especially small and medium-sized ones) that need to rely on corporate datasets to understand the needs of their cities and inhabitants.

Also, conditions for scientific research and statistical repurposing should be aligned for public institutions and data altruistic organisations, as well as for personal and non-personal data. This could ensure a more consistent approach and foster processing for research in the public interest.

IV. *Governance structures.* The EU framework embeds varied governance models. Data economy and surveillance capitalistic logic still underlie many provisions of the Acts. Therefore, alternative and more community-inspired approaches should be enhanced (e.g., data commons and data cooperatives). Governance architectures should be inclusive and enable consultation to understand people's interests over their data[2140]. In smart cities, for instance, public consultations could be carried out to understand which conditions should be set for G2B sharing under the DGA. This would allow data to be treated as a common-pool resource for urban communities and third-party access to be managed in ways that do not counter their interests. In turn, this could downsize the impact of rampant surveillance within and beyond cities. Participatory decision-making mechanisms are included in some provisions of the EHDS proposal. This suggests that the governance of data spaces could follow a commons approach[2141], and thus it is advisable that similar mechanisms are implemented in future sectoral legislation.

V. *Human rights approach and environmental sustainability.* The EU framework lacks a comprehensive vision of harms, vulnerabilities and risks associated with data-driven technologies. An updated conceptualisation thereof is thus needed. Vulnerabilities not only stem from predictable attributes (e.g., age, gender, disability), but are also created by the deployment of the system in a given social context (e.g., AI affecting low-income groups disproportionally). Vulnerabilities may also arise from algorithmic group sorting[2142]. These different instantiations should be incorporated in the provisions concerning unacceptable practices (Art. 5(1)) and listed as general risk factors when assessing the impact of any AI system.

To further tackle such issues, the AI Act should be provided with mechanisms of accountability and redress both at the individual and group level. Specifically, AI users (e.g., local authorities) should be directly tasked with oversight obligations that cover the entire lifecycle of the system, at least under certain circumstances. This entails making prior human rights impact assessments mandatory each time a system is deployed in a specific social environment. In smart cities, such an approach is crucial to fight techno-solutionism and foster a human-driven governance

2140 Solano et al (2022), p. 62.

2141 As advocated by Solano et al (2022), p. 62; Vogelezang (2022).

2142 Solano et al (2022), pp. 61-62.

model. Oversight at the EU level could also narrow down spaces left to manufacturers' self-regulation and introduce hard law mechanisms involving institutions and the public at large. Individual rights to redress accounting for harm beyond the purview of data protection should also be introduced. Collective rights (already existing under the GDPR) should also be incorporated.

The conceptualisation and classification of AI risks is equally flawed. Systems like EFR are built upon "pseudoscience" and could be harmful to the very essence of fundamental rights to privacy and data protection. Yet, they are legitimised under the Act and occasionally labelled as low risk. It would be advisable to ban these systems for their potential incompatibility with the EU human rights framework.

Furthermore, risks are mainly built around product safety law (Annex II) and specific domains and applications (Annex III). It is doubtful that these lists will capture all potential human risks associated with AI risks, especially because these may arise at the deployment phase due to the social specificities of the environment at stake. It may not be appropriate to "petrify" *a priori* the classification of the risk level of AI systems in legislation. Like controllers in the data protection legislation, AI users may be tasked with identifying the contextual risks and require the relevant safeguards from manufacturers or distributors (e.g., through public procurement procedures). In this way, it may be possible to extend the scope of high-risk systems' requirements to other applications, which should be assimilated to the same regime when deployed in particular environments.

Lastly, the Act's conceptualisation of risks is flawed because it does not consider potential environmental impacts of the technology. Protecting the environment is one of the main rationales of the smart city paradigm. Therefore, it is advisable to include obligations in the legislation to address environmental implications, both for manufacturers at the design phase and users are the deployment one.

VI. *"Right" to suitability of datasets.* Exploiting big data entails big risks for smart cities. With a rampant circulation of data within the EU market, municipalities run the risk of using unsuitable datasets, or deploying AI trained with unsuitable datasets, thus leading to biased decisions. The AI Act partially addresses these issues. Nonetheless, data governance requirements only apply to high-risk systems (Art. 10 (2-4)), which may not currently include applications that have salient implications in smart cities (e.g., traffic management). It would thus be advisable to extend a "right" to verify the suitability of datasets also beyond the purview of high-risk systems. Municipalities should be able to check whether the AI systems they intend to acquire have been developed with data that have similar statistical properties (e.g., through public procurement procedures). This would counter a blind techno-solutionist governance approach in smart cities and translate into more accurate policy decisions by local authorities.

VII. *Interoperability and public infrastructure.* It is important for the EU and smart cities to have their own public infrastructure not depend on corporate actors excessively. The *European Strategy for Data* addresses this matter and foresees huge investments to ensure EU technological sovereignty in the future. Nonetheless, this policy should take in specific consideration communities, civil society groups and under-budgeted public sector organisations like schools

and hospitals, so that they have options beyond those of the biggest commercial technology providers[2143].

In a similar vein, it has been argued that interoperability standards bear the risk of strengthening the centralisation of power in the hands of powerful data economy actors[2144]. These technical requirements are not implemented in empty spaces but in complex power relationships that, if not challenged, may lead to the consolidation of the dominant data governance model[2145]. Therefore, policies in this field should be oriented towards enabling processing in the public interest and thus allow access by public and research institutions, media, altruistic organisations. This would embed a commons or data cooperative model in the governance of data spaces.

6. Interim conclusions

Two alternative models of data governance and smart cities. Broadly understood as data collection and circulation, surveillance may be a necessary evil to govern complex information societies, and specifically smart cities. Because data is a necessary ingredient in the equation, its governance is now crucial in how public value is generated in the digital era. At the moment, the dominant framework is that of the data economy, whereby data is conceived as a commodity that can be exchanged freely in the global market. Surveillance capitalism is deeply ingrained in this architecture that leaves large spaces of self-regulation to corporate actors. Alternative models have also emerged: some of these implicitly reproduce the assumptions of the data economy (e.g., PDS, data collaboratives), while others challenge the power relationships that it embeds (e.g., data commons, data cooperatives, PDTs).

This also translates into smart city development. Originally, the smart city paradigm was framed within the data economy model, giving way to reckless data practices and techno-solutionism. Communitarian outlooks stood in contrast with this techno-driven approach and inspired more human-driven ones (e.g., in Barcelona). Several pilot projects were launched to make sure that data is used for the common good of the city. Although experimental, these initiatives offer promising alternatives to the data economy but should be combined with the upcoming EU governance legislation.

Viable data co-governance. From the rise of the Internet, State-based regulation alone has lost its centrality[2146]. On the other hand, self-regulation has often ill served society[2147]. Because private actors play a major role in providing technology infrastructure, a co-governance architecture is the only viable path to manage collective issues in the digital era[2148]. Even in co-governance, however, specific mechanisms may manage competing interests and power relationships differently. For instance, "lighter" co-governance models like enforced self-regulation can still leave a great margin of appreciation of corporate actors in the pursuit of their own ends. Therefore, without strong public accountability and redress mechanisms, the balance between private and public interests may often be tipped in favour of market actors.

Which model to mitigate surveillance? These have indeed profited from large spaces of self-regulation to pursue their surveillance capitalist agenda, including in smart cities. The separated regime between personal and non-personal data and the individualistic focus of data protection legislation have been

[2143] Solano et al (2022), p. 58.
[2144] Id., p. 63.
[2145] Id.
[2146] Marsden (2008).
[2147] Floridi (2021).
[2148] Pagallo et al (2019).

contributing factors in this process. On the contrary, more-community oriented models of data governance may be the ones to mitigate the worrisome effects of large-scale surveillance. Frameworks like the data commons and data cooperatives ensure stewardships of data by communities and curb reckless data exchange between (non-accountable) corporate actors, which can have detrimental consequences for individuals and groups.

Smart cities and the EU governance model. If surveillance is a necessity to govern society, this should be oriented to the common good as much as possible. Regrettably, the prospective EU data governance model does not always foster collective benefits in data processing as it claims to. A systematic review of the legislation (DGA, drafts DA and AIA) reveals that balancing mechanisms often favour corporate interests in data sharing. Large spaces for (enforced) self-regulation are still granted to firms, without sound mechanisms for public contestation and oversight. On the contrary, instruments to exchange data for public interest goals (i.e., data altruism, B2G sharing) are significantly underdeveloped. In such a context, smart cities may struggle to free themselves from the neoliberal influences of big data economy platforms.

Therefore, some policy recommendations were put forward, both at the general and contextual level. Some common threads in this analysis concern the lack of normative reflection of the nature of data as a common good and the lack of a human rights perspective in technology implementation, both of which have repercussions on the governance structures stemming from EU legislation. From the technical standpoint, investments are also needed to build a European public infrastructure and ensure actual control over data. In light of these issues, smart cities alone may not be able to tackle existing power imbalances and the risks of surveillance capitalism. A crucial role in this challenge then is to be played by the EU itself.

Conclusions

This dissertation addressed how to implement surveillance technologies legally and ethically in the specific context of smart cities. With a multidisciplinary approach, diverse knowledge fields (i.e., law, ethics, urban geography, surveillance studies) were combined to explore the regulatory challenges that cities now face in their transition toward pervasive digitisation.

The underlying thesis of this work is that surveillance is a necessary feature to govern complex information societies, but its implementation is still not supported by fine-tuned proportionality assessments. This dissertation aimed at filling this gap. There was an effort to overcome overly dystopian narratives that surround surveillance and offer a more nuanced and ambivalent picture of its implications in society. While concerns over fundamental rights are not discarded, it is stressed that surveillance remains an unavoidable step in the governance of populations and all collective phenomena. Hence, rather than rejecting *any* kind of surveillance altogether, legal experts should be called on to discern *when* and *which* kinds of surveillance are acceptable in democratic societies. This requires a careful exercise of balancing of competing interests, which was the common thread of this investigation. The smart city provided for a stimulating reference setting for this endeavour.

In the first two chapters indeed, the issues of surveillance in smart cities were examined from the angle of the EU data protection legislation. The first addressed question was: *Which legal grounds legitimise data collection in smart cities and what balancing exercises do they entail?* The ensuing analysis brought three findings. Preliminary, it was posited that a permissive rationale for data protection could better account for cities' innovation needs and ensure a more flexible balancing of such interests with fundamental rights. It was highlighted that the application of data protection law itself requires contextual assessments that may conceal value judgements by smart city actors. Most importantly, however, different kinds of balancing were discerned in the legal bases that are the grounds for data collection in smart cities (legal obligation, public task, legitimate interest). These can be distinguished by *intensity* (e.g., necessity vs. proportionality *stricto sensu*) and the *moment* in which they should be performed (e.g., public task vs. legitimate interest, collection vs. repurposing). Potential applications by smart city players were identified. Hopefully, this analysis can bring more rigorous assessments at the moment of deciding when and how much data to collect in these contexts.

Following this preliminary analysis, Chapter II tackled this question: *What are the issues that arise from personal data flows in smart cities and how should these be addressed?* Three main issues were explored through the lens of EU data protection law: purpose limitation, data controllership, and DPIAs. Firstly, because data repurposing implies an interference with the core principles of EU data protection, it was argued that this entails a more intense kind of balancing, i.e., proportionality *stricto sensu*. These exercises may be attuned differently according to the actors involved in data flows (i.e., private sector, public administration, law enforcement). Therefore, criteria guiding the assessment were proposed in varied repurposing scenarios in smart cities, following a multi-layered methodology. Secondly, the balancing of private and public interests in smart cities is also a feature of public-private partnerships, which are fundamental co-governance mechanisms in smart cities. Based on available empirical data, different data protection instruments were identified to ensure that competing stakes are properly managed and that data is exploited for the public interest of the city. Lastly, DPIAs raised the question of *who* should be involved in balancing exercises. The implementation of large-scale smart city projects suffers from

big legitimacy gaps, which could be overcome by involving the wider urban community in the process. Therefore, insights from the ECtHR's case law were applied to the case of large data-driven projects in smart cities. This argument led to an extensive interpretation of mandatory participation of the public in DPIA, which could in turn "democratise" balancing exercises in smart cities.

Chapter III scrutinised the same issues from the specific angle of the right to privacy, addressing the following question: *Which reasonable expectations of privacy can individuals have in complex IoT environments such as public places in smart cities?* A background analysis on the right to privacy uncovered its multifaceted rationale and wide scope. This led to establishing which kind of activities are liable to be protected under the heading of privacy, especially in public places in smart cities. The impact of digital technologies on the nature of space was also scrutinised, showing why privacy concerns are being magnified in smart urban environments. It was stressed that privacy interferences in these settings can no longer be identified based on hard boundary markers (e.g., the home vs. public spaces). Inversely, this can be done by balancing people's expectations over data flows and collective needs to use such data. Therefore, US and European case law was scrutinised to define a coherent multi-factor test assessing privacy expectations in IoT environments. These were applied to the smart city context specifically, identifying factors that give rise to higher or lower privacy expectations. This methodology should serve as a preliminary balancing effort to determine both the *existence* of a privacy interference and its *seriousness*. Indeed, having a more granular picture of the strength of individuals' privacy expectations in a given situation can help legal interpreters to fine-tune subsequent proportionality assessments.

Proportionality assessments of surveillance measures were tackled in Chapter IV. The following question was addressed: *Which theoretical frameworks can best conceptualise surveillance schemes in smart cities and which proportionality assessments do these require?* At the outset, the analysis combined philosophical and sociological theories on surveillance to grasp current trends in smart cities. Governance studies provide for a theoretical justification for surveillance, which becomes increasingly necessary as urban societies develop in volume and complexity. While different theories can partially describe surveillance dynamics in urban centres (e.g., Zuboff's surveillance capitalism, Foucault's panopticon), the metaphor of the surveillant assemblage is arguably the one that best fits these phenomena which feature a high diversity of goals and means of monitoring. In fact, it is important to acknowledge the manifold nature of surveillance also in the legal analysis. That is why this dissertation provided for a novel taxonomy of surveillance, which is characterised as a *continuum* and classified as purely "mass" surveillance, "mass/hybrid" surveillance, "hybrid/targeted" surveillance, and traditional "targeted" surveillance. Understanding the structure of single surveillance occurrences can help interpreters to pin down the seriousness of interferences in fundamental rights and attune proportionality assessments accordingly. With respect to proportionality, this chapter reviewed the relevant case law of the ECtHR and the CJEU, highlighting its strengths and inconsistencies (e.g., unclear definitions, inapt remedies). Translating the requirements in the smart city context is no easy task. Indeed, conflicting definitions of *public* and *national* security still hamper granular proportionality assessments. Contemporary definitions of national security, broader in scope, may legitimise data collection to counter threats against the very integrity of urban infrastructure and essential services, as well as intense environmental issues affecting the city. On the contrary, mere resource optimisation objectives may only justify hot-spot data collection in certain areas.

In Chapter V, these theoretical insights were applied to some urban surveillance technologies, with a specific focus on the IoT. The addressed sub-research question was: *Which IoT surveillance technologies in*

smart cities can affect individuals' rights to privacy and data protection and how can these be proportionally implemented? Facial recognition, drones, environmental policing and smart nudging were chosen as illustrative technologies. These were framed into the devised surveillance taxonomy and placed into specific scenarios to assess their proportionality. Some of these applications were found to be incompatible with the European human rights system. While these evaluations were purely contextual, some general trends could be detected. Overall, surveillance can be underpinned by varied objectives, ranging from security to commercial and environmental ones. Different weights can be attached to such goals: if the case law looks favourably at environmental objectives, security ones should be scrutinised better for their implications on individuals' rights. On their side, commercial stakes do not seem to bear the same weight for legitimising intense surveillance in public places (e.g., EFR in smart billboards or shopping venues), unless they match other collective needs and are coupled with strong data security measures.

Lastly, Chapter VI took a broader perspective on surveillance and governance by dealing with the following question: *Which data governance frameworks can most mitigate the impacts of surveillance in smart cities, ensuring a fair balancing of public and private interests in the urban sphere?* The analysis reviewed competing data governance models in the digital domain and the smart city specifically. It was highlighted that the smart city is currently dominated by data economy and surveillance capitalist strategies, which exploit data as a commodity. Because data is crucial in how public value is generated in the digital era, its governance should rather be more-community oriented, in order to mitigate the worrisome effects of large-scale surveillance. In particular, frameworks like the data commons and data cooperatives ensure stewardships of data by communities and curb reckless data exchange between (non-accountable) corporate actors, which can have detrimental consequences for individuals and groups. Regrettably, the upcoming EU governance framework (including the AIA, DGA and DA) may not discard the negative effects of the data economy. A systematic review of the legislation in factrevealed that balancing mechanisms often favour corporate interests in data sharing, to the detriment of common good uses of data. In such a context, smart cities may struggle to free themselves from the neoliberal influences of big data economy platforms. In conclusion, some policy recommendations were put forward, both at the general and smart city level. These were aimed at fostering the use of data for the common good, as well as a human rights perspective in the implementation of AI.

Overall, the lesson to be learned is that **as surveillance increases in complexity, so should the balancing exercises, preparing for and reviewing the legal and ethical implementation of monitoring technologies**. Smart cities offer a privileged scenario to engage with such efforts: diverse socio-political contexts and intense environmental challenges in these contexts provide stimulating training material for legal interpreters addressing this task. Some of the necessary theoretical tools were already there, but needed more conceptual systematisation (e.g., reasonable expectation of privacy). This dissertation worked on these concepts and devised new ones (e.g., surveillance taxonomy). It privileged multi-layered balancing exercises as a methodology, both in personal data protection and privacy/surveillance assessments. In this sense, the existence and seriousness of interferences with the right to private life should be established according to degrees of reasonable expectations of privacy. The scope of surveillance schemes should be determined in light of a granular surveillance taxonomy, which also impacts on the strictness of the proportionality assessment. Finally, proportionality embodies the final step of balancing, where individual, private and public stakes on surveillance are weighed against each other. Certainly, these evaluations require challenging value-judgements and involve a plurality of factors, but they impose them as necessary if we mean to harness the potential of digital technologies ethically in cities and beyond.

Bibliography

Legislation

United Nations (1948) Universal Declaration of Human Rights of the United Nations.

Council of Europe (1950) European Convention on Human Rights.

United Nations (General Assembly) (1966) International Covenant on Civil and Political Rights. Treaty Series 999, p. 171.

Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

UNCED/Rio Declaration on Environment and Development (1992) U.N. Doc. A/CONF.151/5/Rev.1, 31 I.L.M. 874.

European Union (2000) Charter of Fundamental Rights of the European Union.

European Union (2012) Consolidated version of the Treaty on the European Union.

European Union (2012) Consolidated version of the Treaty on the Functioning of the European Union.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance.) PE/2/2018/REV/1, OJ L 212, 22.8.2018, p. 1–122.

Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (Text with EEA relevance.) PE/73/2017/REV/1, OJ L 151, 14.6.2018, p. 1–218.

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, Official Journal L 281.

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 sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. OJ L 345, 31.12.2003, p. 90–96

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 L 105, 13.4.2006

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the Assessment of the Effects of Certain Public and Private Projects on The Environment, OJ L 26, 28.1.2012, p. 1–21.

Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings OJ L 65, 11.3.2016, p. 1–11

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 penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149

Directive (EU) 2016/797 on the interoperability of the railway system excludes from its scope metros, trains, and generally urban and local transportation. 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 L 350, 30.12.2008, p. 60–71

Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83

2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision, OJ L 190, 18.7.2002, p. 1–20

LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (1), JORF n°0235 du 8 octobre 2016.

The UK Digital Economy Act (2017) (c. 30)

The Irish Data Sharing and Governance Act (Act No. 5 of 2019)

Jurisprudence

European Court of Human Rights and European Commission of Human Rights

ECommHR, 5 December 1978, *Arrowsmith v. the United Kingdom*, App. No. 7075/75

ECtHR, 6 September 1978, *Klass and Others v. Germany*, App. no. 5029/71

ECtHR, 2 August 1984, *Malone v. the United Kingdom*, App. no. 8691/79

ECtHR, 26 March 1987, *Leander v. Sweden,* App. no. 9248/81

ECtHR, 24 March 1988, *Olsson v. Svezia*, App. no. 10465/83

ECtHR, 24 April 1990, *Kruslin v. France*, App. no. 11801/85

ECtHR, 24 April 1990, *Huvig v. France*, App. no. 11105/84

ECtHR, 30 August 1990, *Fox, Campbell and Hartley v. The United Kingdom*, App. nos. 12244/86, 12245/86 and 12383/86

ECtHR, *Niemietz v. Germany*, judgment of 16 December 1992, App. no. 13710/88

ECtHR, 25 May 1993, *Kokkinakis v. Greece*, App. no. 14307/88

ECtHR, 22 February 1994, *Burghartz v. Switzerland*, App. no. 16213/90

ECommHR, 19 May 1994, *Friedl v. Austria*, App. no. 15225/89

ECtHR, 8 February 1996, *John Murray v. United Kingdom*, App. no. 18731/91

ECtHR, 11 November 1996, *Cantoni v. France*, App. no. 17862/91

ECtHR, 25 June 1997, *Halford v. United Kingdom,* App. no. 20605/92

ECommHR, 14 January 1998, *Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium*, App. nos. 32200/96 and 32201/96

ECtHR, 30 January 1998, *United Communist Party of Turkey and others v. Turkey*, App. No. 19392/92

ECtHR, 19 February 1998, *Guerra and others v. Italy*, App. no. 14967/89

ECtHR, 30 July 1998, *Valenzuela Contreras v. Spain,* App. no. 58/1997/842/1048

ECtHR, 24 August 1998, *Lambert v. France*, App. no. 23618/94

ECtHR, 20 October 1998, *Salabiaku v. France*, App. no. 10519/83

ECtHR, 16 February 2000, *Amann v. Switzerland*, App. no. 27798/95

ECtHR, 4 May 2000, *Rotaru v. Romania*, App. no. 28341/95

ECtHR, 22 June 2000, *Coëme and Others v. Belgium*, App, nos. 32492/96, 32547/96, 32548/96, 33209/96 and 33210/96

ECtHR, 25 September 2001, *P.G. and J. H. v. United* Kingdom, App. no. 44787/98

ECtHR, 7 February 2002, *Mikulić v. Croatia*, App. no. 53176/99

ECtHR, 29 April 2002, *Pretty v. United Kingdom*, App. no. 2346/02

ECtHR, 11 July 2002, *Christine Goodwin v. the United Kingdom*, App. no. 28957/95

ECtHR, 28 January 2003, *Peck v. the United Kingdom*, App. no. 44647/98

ECtHR, 13 February 2003, *Odièvre v. France*, App. no. 42326/98

ECtHR, 18 May 2003, *Prado Bugallo v. Spain*, App. no. 58496/00

ECtHR, 8 July 2003, *Hatton v. the United Kingdom*, App. no. 36022/978

ECtHR, 30 March 2005, *Taşkin v. Turkey*, App. no. 46117/99

ECtHR, 24 June 2004, *von Hannover v. Germany,* App. No. 59320/00

ECtHR, 6 June 2006, *Segerstedt-Wiberg and Others v Sweden*, App. no. 62332/00

ECtHR, 29 June 2006, *Weber and Saravia v. Germany*, App. no. 54934/00

ECtHR, 2 November 2006, *Giacomelli v. Italy*, App. no. 59909-00

ECtHR, 3 April 2007, *Copland v. United Kingdom*, App. no. 62617/00

ECtHR, 26 July 2007, *Peev v. Bulgaria*, App. no. 64209/01

ECtHR, 30 January 2008, *Association For European Integration And Human Rights And Ekimdzhiev V. Bulgaria*, App. no. 62540/00

ECtHR, 20 February 2008, *Saadi v. Italy*, App. no. 37201/06

ECtHR, 3 June 2008, *Steeg and Wenger v. Germany*, App. nos. 9676/05, 10744/05 and 41349/06

ECtHR, 1 July 2008, *Liberty and Others v. the United Kingdom*, App. no. 58243/00

ECtHR, 4 December 2008, *S. and Marper v. United Kingdom*, App. no. 30562/04 and 30566/04

ECtHR, 27 January 2009, *Tătar v. Romania*, App. no. 67021-01

ECtHR, 10 March 2009, *Bykov v. Russia*, App. no. 4378/02

ECtHR, 24 November 2009, *Friend and Others v. United Kingdom*, App. nos. 16072/06 and 27809/08

ECtHR, 12 January 2010, *Gillan and Quinton v. United Kingdom*, App. no. 4158/05

ECtHR, 18 May 2010, *Kennedy v. United Kingdom*, App. no 26839/05

ECtHR, 2 September 2010, *Uzun v. Germany*, App. no. 35623/05

ECtHR, 5 October 2010, *Köpke v. Germany*, App. no. 420/07

ECtHR, 20 March 2011, *Telfner v. Austria*, App. no. 33501/96

ECtHR, 10 May 2011, *Mosley v. United Kingdom*, App. no. 48009/08

ECtHR, 24 May 2011, *Konstas v. Greece*, App. no. 53466/07

ECtHR, 28 November 2011, *Shimolovos v. Russia*, App. no. 30194/09

ECtHR, 3 April 2012, *Boulois v. Luxembourg*, App no. 37575/04

ECtHR, 18 April 2013, *M.K. v France*, App. no. 19522/09

ECtHR, 19 November 2013, *Shyti v. Romania*, App. no. 12042/05

ECtHR, 19 February 2015, *Ernst August von Hannover v. Germany*, App. no. 53649/09

ECtHR, 19 February 2015, *Bohlen v. Germany,* App no. 53495/09

ECtHR, 3 March 2015, *J.S. v. United Kingdom*, App. no. 445/10

ECtHR, 24 May 2015, *Haldimann and Others v. Switzerland*, App. no. 21830/09

ECtHR, 16 June 2015, *Delfi AS v. Estonia,* App. no. 64569/09

ECtHR, 27 October 2015, *R.E. v. the United Kingdom*, App. no. 62498/11

ECtHR, 4 December 2015, *Roman Zakharov v. Russia*, App. no. 47143/06

ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary*, App. no. 37138/14

ECtHR, 26 January 2016, *Iasir v. Belgium*, App. no. 21614/12

ECtHR, 21 June 2016, *Oleynik v. Russia*, App. no. 23559/07

ECtHR, 18 October 2016, *Vukota-Bojić v. Switzerland*, App. no. 61838/10

ECtHR, 23 March 2017, *A.-M.V. v. Finland*, App. no. 53251/13

ECHtR, 20 June 2017, *Bogomolova v Russia*, App. no. 13812/09

ECtHR, 5 September 2017, *Bărbulescu v. Romania*, App. no. 61496/08

ECtHR, 7 November 2017, *Akhlyustin v. Russia*, App. no. 21200/05

ECtHR, 18 January 2018, *National Federation of Sportspersons' Associations and Unions (Fnass) and Others v. France*, App. nos. 48151/11 and 77769/13

ECtHR, 28 February 2018, *Antović and Mirković v. Montenegro*, App. no. 70838/13

ECtHR, 24 April 2018, *Benedik v. Slovenia,* App. no. 62357/14

ECtHR, 8 May 2018, *Ben Faiza v. France*, App. no. 31446/12

ECtHR, 19 June 2018, *Centrum for Rittvisa v Sweden*, App. no. 35252/08

ECtHR, 13 September 2018, *Big Brother Watch v. United Kingdom*, App. no. 58170/13, 62322/14 and 24960/1

ECtHR, 27 September 2018, *Brazzi v. Italy*, App. no. 57278/1

ECtHR, 24 January 2019, *Cordella and others v. Italy*, App. nos 54414/13 and 54264/15

ECtHR, 10 April 2019, *Khadija Ismayilova v. Azerbaijan*, App. nos. 65286/13 and 57270/14

ECtHR, 14 May 2019, *Garamukanwa v. United Kingdom*, App. no. 70573/17

ECtHR, 17 October 2019, *López Ribalda and Others v. Spain*, App. nos. 1874/13 and 8567/13

ECtHR, 25 May 2021, *Centrum För Rättvisa v. Sweden,* App. no. 35252/08

ECtHR, 25 May 2021, *Big Brother Watch and Others v. the United Kingdom*, App. nos. 58170/13, 62322/14 and 24960/15

Court of Justice of the European Union

CJEU, *Nold v Commission,* judgment of 14 May 1974, Case C-4/73

CJEU, *Procureur de la République v Association de défense des brûleurs d'huiles usagées (ADBHU)*, judgment of 7 February 1985, Case C-240/83

CJEU, *Commission v Belgium*, judgment of 9 July 1992, Case C-2/90

CJEU, *Montecatini S.p.A*, judgment of 8 July 1999, Case C-235/92

CJEU, *Criminal proceedings against Bodil Lindqvist*, judgment of 6 November 2003, Case C-101/01

CJEU, *Bavarian Lager,* judgment of 8 November 2007, Case T-194/04

CJEU, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, judgment of 29 January 2008, Case C-275/06

CJEU, *Volker und Markus Schecke GbR) and Hartmut Eifert v Land Hessen*, judgment of 9 November 2010, Joined Cases C-92/09 and C-93/09

CJEU, *Land Baden-Württemberg v Panagiotis Tsakouridis*, judgment of 23 November 2010, Case C-145/09

CJEU, *Scarlet Extended,* judgment of 24 November 2011, Case C-70/10

CJEU, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado,* judgment of 24 November 2011, Joined Cases C-468/10 and C-469/10

CJEU, *Fra.bo SpA v Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) — Technisch-Wissenschaftlicher Verein*, judgment of 12 July 2012, Case C-171/11.

CJEU, *Nexans v Commission*, judgment of 14 November 2012, Case T-135/09

CJEU, *Schwarz v Stadt Bochum*, judgment of 17 October 2013, Case C-291/12

CJEU, *Digital Rights Ireland and Others*, judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12

CJEU, *Google Spain,* judgment of 13 May 2014, Case C-131/12

CJEU, *YS and M. and S. v Minister of Immigration, Integration and Asylum*, judgment of 17 July 2014, Joined cases C-141/12 and C- 372/12

CJEU, *Client Earth,* judgment of 16 July 2015, Case C-615/13 *P*

CJEU, *Smaranda Bara and Others*, judgment of 1 October 2015, Case C-201/14

CJEU, *Maximilian Schrems v Data Protection Commissioner*, judgment of 6 October 2015, Case C-362/14

CJEU, *Patrick Breyer v Bundesrepublik Deutschland*, judgment of 19 October 2016, Case C-582/14

CJEU, *Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union,* 26 July 2017

CJEU, *Tele 2 Sverige AB/Watson*, judgment of 21 December 2016, Joined cases C-203/15 e C-698/15

CJEU, *Peter Nowak v Data Protection Commissioner,* judgment of 20 December 2017, Case C-434/16

CJEU, *Ministerio Fiscal,* judgment of 2 April 2018, Case C-207/16

CJEU, *Wirtschaftsakademie,* judgment of 5 June 2018, Case C-201/16

CJEU, *Jehovah's witnesses,* judgment of 10 July 2018, Case C-25/17

CJEU, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, judgment of 29 July 2019, Case C-40/17

CJEU, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, judgment of 6 October 2020, Case C-623/17

CJEU, *La Quadrature du Net and Others*, judgment of 6 October 2020, Joined cases C-511/18, C-512/18 and C-520/18

CJEU, *Criminal proceedings against Marcello Costa and Ugo Cifone*, judgment of 16 February 2021, Joined Cases C-72/10 and C-77/10

CJEU, *G.D. v Commissioner of An Garda Síochána and Others*, judgment of 5 April 2022, Case C-140/20

CJEU, *Meta Platforms Ireland Limited, formerly Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V,* judgment of 28 April 2022, Case C-319/20

CJEU, *Ligue des droits de l'homme v Conseil des Ministres*, judgement of 21 June 2022, Case C-817/19

CJEU, *OT v Vyriausioji tarnybinės etikos komisija*, judgment of 1 August 2022, Case C-184/20

CJEU, *VD and SR,* judgment of 20 September 2022, Joined cases C-339/20 and C-397/20

CJEU, *Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH*, judgement of 20 September 2022, Joint Cases C-793/19 and C-794/19

CJEU, *Spetsializirana prokuratura*, judgement of 17 November 2022, Case C-350/21

Opinions of CJEU Advocate Generals

Opinion of Advocate General Sharpston delivered on 12 December 2013. *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*

Opinion of Advocate General Kokott delivered on 30 June 2016. *Peter Nowak v Data Protection Commissioner*

National jurisprudence

Urteil des BVerfG v. 15.12.1983 zum VZG 83 (1 BVerfGE 65).

Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Apr. 20, 2016, 1 BvR 966/09

Conseil d'État, 10ème - 9ème chambres réunies, 08/02/2017, n. 393714.

Cass. pen., sec. III, n. 5818/2015, Rv. 266267 – 01

Cass. pen., sec. VI, n. 14395/2018, Rv. 275534 – 01

R (Bridges) v Chief Constable of the South Wales Police [2019] EWHC 2341

R (Bridges) v the Chief Constable of South Wales Police [2020] EWCA CIV 1058

Dutch Council of State, 27 July 2022, *VoetbalTV BV and the AP*, 20100045/1/A3. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RVS:2022:2173. Accessed 27 August 2022.

United States

Pavesich v. New England Life Insurance Co., 122 Ga. 190, 50 S.E. 68 (1905)

Olmstead v. United States, 277 U.S. 438 (1928)

Katz v. United States, 389 U.S. 347, 351 (1967)

United States v. White, 401 U.S. 745 (1971)

United States v. Knotts, 460 U.S. 276 (1983)

Oliver v. United States, 466 U.S. 170 (1984)

United States v. Karo, 468 U.S. 705 (1984)

California v. Ciraolo, 476 U.S. 207 (1986)

Dow Chemical Co. v. United States, 476 U.S. 227 (1986)

Cardwell v. Lewis, 417 U.S. 583 (1974)

United States v. Miller, 425 U.S. 435 (1976)

Smith v. Maryland, 442 U.S. 735 (1979)

Arizona v. Hicks, 480 U.S. 321 (1987)

Florida v. Riley, 488 U.S. 445 (1989)

Soldal v. Cook County, 506 U.S. 56 (1992)

Kyllo v. United States, 533 U.S. 27 (2001)

United States v. Jones, 565 U.S. 400 (2012)

Riley v. California, 573 U.S. __ (2014)

Carpenter v. United States, 585 U.S. (2018)

Opinions and decisions of Data Protection Authorities

Agencia española de protección datos (AEPD) Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf. Accessed 28 December 2021.

Autoriteit Persoongegevens (2019) AP informeert branche over norm camera's in reclamezuilen. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-informeert-branche-over-norm-camera%E2%80%99s-reclamezuilen. Accessed 11 December 2021.

Autoriteit Persoongegevens (2020) Onderzoek smart cities. Update augustus 2020. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_smart_cities_update_aug_2020.pdf. Accessed 1 September 2020.

Autoriteit Persongegevens, 11 March 2021, *Gemeente Enschede*.. https://gdprhub.eu/index.php?title=AP_(The_Netherlands)_-_Gemeente_Enschede. Accessed 20 December 2021.

Article 29 WP (2003) Opinion 7/2003 on the re-use of public sector information and the protection of personal data - Striking the balance -. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp83_en.pdf. Accessed 19 November 2021.

Article 29 WP (2005) Working document on data protection issues related to RFID technology. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf. Accessed 3 December 2021.

Article 29 WP (2007) Opinion 4/2007 on the concept of personal data. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf. Accessed 17 August 2022

Article 29 WP (2010) Opinion 1/2010 on the concepts of "controller" and "processor",. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Accessed 30 December 2021.

Article 29 WP (2011) Opinion 15/2011 on the definition of consent. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf. Accessed 14 December 2021

Article 29 WP (2012) Opinion 02/2012 on facial recognition in online and mobile services. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. Accessed 27 June 2022.

Article 29 WP (2013a) Opinion 03/2013 on purpose limitation. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Accessed 17 August 2022.

Article 29 WP (2013b) Opinion 06/2013 on open data and public sector information ('PSI') reuse. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp207_en.pdf. Accessed 19 November 2021

Article 29 WP (2014a) Opinion 8/2014 on the on Recent Developments on the Internet of Things. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. Accessed 7 December 2021.

Article 29 WP (2014b) Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accessed 17 November 2021.

Article 29 WP (2014c) Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks,. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf. Accessed 23 December 2021.

Article 29 WP (2014d) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Article 29 WP (2014e) Opinion 01/14 on the application of necessity and proportionality concepts and data protection within the law enforcement sector. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf. Accessed 19 August 2022.

Article 29 Working Party (2015) Opinion 1/15 on Privacy and Data Protection Issues relating to the Utilisation of Drones, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf. Accessed 21 June 2022.

Article 29 WP (2017a) Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679. WP 248 rev 0.1 (4 April 2017).

Article 29 WP (2017b) Opinion on some key aspects of the Law Enforcement Directive (EU 2016/680). https://ec.europa.eu/newsroom/article29/items/610178/en. Accessed 19 August 2022.

Article 29 Working Party (2018) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Accessed 29 June 2022.

CNIL, Délibération n° 2015-255 du 16 juillet 2015 refusant la mise en œuvre par la société JCDecaux d'un traitement automatisé de données à caractère personnel ayant pour finalité de tester une méthodologie d'estimation quantitative des flux piétons sur la dalle de La Défense (demande d'autorisation n° 1833589). https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000031159401/. Accessed 19 December 2021.

CNIL, 1 November 2021, Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI. https://www.cnil.fr/sites/default/files/atoms/files/decision_ndeg_med_2021-134.pdf. Accessed 27 June 2022.

Commission de la Protection de la Vie Privée (CPVP) (2018) Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2018-001), §82. https://www.fedil.lu/wp-content/uploads/2019/03/Recommandation-concernant-lAIPD-du-28-f%C3%A9vrier-2018-de-lautorit%C3%A9-de-contr%C3%B4le-belge-Autorit%C3%A9-de-protection-des-donn%C3%A9es-APD.pdf. Accessed 27 December 2021.

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (2021) Guidelines on Facial Recognition. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Accessed 8 July 2021.

EDPB (2015) Opinion 4/15. Towards a Digital Ethics. https://edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf. Accessed 2 February 2022.

EDPB (2018) Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf. Accessed 19 August 2022

EDPB (2019) Guidelines 3/2019 on processing of personal data through video devices. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf. Accessed 20 December 2021.

EDPB (2020) Guidelines 07/2020 on the concepts of controller and processor in the GDPR - Version 2.0. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf. Accessed 30 December 2021.

EDPB (2022) Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf. Accessed 27 June 2022.

EDPB, EDPS (2021a) Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) https://edps.europa.eu/system/files/2021-03/edpb-edps_joint_opinion_dga_en.pdf. Accessed 23 November 2021

EDPB-EDPS (2021b) Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf. Accessed 9 August 2022.

EDPB, EDPS (2022) Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), §79 ff. https://edpb.europa.eu/system/files/2022-05/edpb-edps_joint_opinion_22022_on_data_act_proposal_en.pdf. Accessed 8 August 2022.

EDPS (2014) Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner". https://edps.europa.eu/sites/edp/files/publication/14-11-26_opinion_rpas_en.pdf. Accessed 23 June 2022

EDPS (2015) Opinion 6/2015. EDPS recommendations on the Directive for data protection in the police and justice sectors, pp. 5-6. https://edps.europa.eu/sites/edp/files/publication/15-10-28_directive_recommendations_en.pdf. Accessed 11 May 2022.

EDPS (2017a) Developing a "toolkit" for Assessing the Necessity of Measures that Interfere with Fundamental Rights. https://edps.europa.eu/sites/edp/files/publication/16-06-16_necessity_paper_for_consultation_en.pdf. Accessed 16 November 2021.

EDPS (2017b) EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf. Accessed 10 December 2021.

EDPS (2020) Opinion 3/2020 on the European strategy for data. https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf. Accessed 23 November 2021.

Garante per la protezione dei dati personali (2017) Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria. Decision no. 551 of 21 December 2017.

Garante della Privacy, 10 February 2022, Ordinanza ingiunzione nei confronti di Clearview AI - 10 febbraio 2022 [9751362]. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362. Accessed 27 June 2022.

The Hamburg Commissioner for Data Protection and Freedom of Information (Hmb BfDI) (2021) Clearview AI Inc. https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF. Accessed 27 June 2022.

ICO (2018) Guide to the General Data Protection Regulation (GDPR). https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Accessed 2 Nov 2021.

ICO (2019) The Use of Live Facial Recognition Technology by Law Enforcement in Public Places. https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf. Accessed 28 June 2022.

ICO (2020) Data sharing code of practice. https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice-1-0.pdf. Accessed 17 November 2021.

ICO, 18 May 2022, Clearview AI Inc. Enforcement Notice. https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-20220518.pdf. Accessed 27 June 2022

Irish Data Protection Commission (2019) Guide to Data Protection Impact Assessments (DPIAs). https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29_Oct19_0.pdf. Accessed 28 December 2021.

Policy documents

Ajuntament de Barcelona (2017) Manifesto in Favor of Technological Sovereignty and Digital Rights for Cities. Available at: https://www.barcelona.cat/digitalstandards/manifesto/0.2/. Accessed 27 August 2020

Australian Government Guide to Regulation (2014) https://apo.org.au/sites/default/files/resource-files/2014-03/apo-nid270966.pdf. Accessed 24 August 2022.

Barcelona City Digital Plan (2017) https://ajuntament.barcelona.cat/digital/sites/default/files/LE_MesuradeGovern_EN_9en.pdf. Accessed 1 August 2022.

COMMISSION STAFF WORKING DOCUMENT Advancing the Internet of Things in Europe Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Digitising European Industry Reaping the full benefits of a Digital Single Market. SWD/2016/0110 final

COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE EVALUATION Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information. SWD/2018/129 final - 2018/0111 (COD)

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European strategy for data. COM/2020/66 final

Committee of Ministers of the Council of Europe (2010) The protection of individuals with regard to automatic processing of personal data in the context of profiling. Recommendation CM/Rec(2010)13.

Council of Europe (2017) Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data. https://rm.coe.int/16806ebe7a. Accessed 23 December 2021.

Council of the European Union (2022) Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach. https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf. Accessed: 7 February 2023.

Declaration of Cities Coalition for Digital Rights. https://citiesfordigitalrights.org/#declaration. Accessed: 27 August 2020.

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_EN.html. Accessed 12 May 2022

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act). COM/2020/767 final

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. COM/2021/206 final.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act). COM/2022/68 final

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space. COM/2022/197 final

OECD (1980) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 15 Sept 2021

WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust. COM/2020/65 final

Books

Adam R, Tizzano A (2014) Manuale di Diritto dell'Unione Europea, 1st edn. Giappichelli Editore, Torino

Ashworth A, Zedner L (2014) Preventive Justice. Oxford.

Bauman Z, Lyon D (2013) Liquid surveillance. Polity Press

Beauchamp T (1991) Philosophical Ethics. An Introduction to Moral Philosophy. McGraw-Hill

Bevir M (2009) Key Concepts in Governance. SAGE Publishing

Bevir M (2010) Democratic Governance. Princeton: Princeton University Press

Bell DA, de-Shalit A (2012) The Spirit of Cities: Why the Identity of a City Matters in a Global Age. Princeton University Press.

Bibri SE (2018) Smart Sustainable Cities of the Future. Springer International Publisher

Burchell G, Gordon C, Miller P (1991) The Foucault Effect. Studies in Govern-mentality. The University of Chicago Press

Cameron I (2000) National Security and the European Convention on Human Rights. Kluver Law

Cardullo P, Di Feliciantonio C, Kitchin R (2019a) The Right to the Smart City. Emerald Publishing Limited.

Cresswell T (2004) Place. A Short Introduction. Blackwell Publishing

Durante M (2017) Ethics, law and the politics of information: A guide to the philosophy of Luciano Floridi. Springer

Finck M (2019) Blockchain, Law and Technological Innovation in Blockchain Regulation and Governance in Europe. Cambridge University Press

Floridi L (2014) The Fourth Revolution. Oxford University Press

Floridi L (2015) The Onlife Manifesto. Springer.

Foucault M (2020, original work of 1975) Discipline and Punish. Penguin Books

Goffman E (1963). Behaviour in public places. Notes on the social organizations of gatherings. New York: The Free Press

González Fuster G (2014) The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer, New York.

Graham M, Kitchin R, Mattern S, Shaw J (2019) How to Run a City Like Amazon and Other Fables. London: Meatspace Press.

Green B (2019) The Smart Enough City. The MIT Press

Habermas J (1989, original work of 1967) The Structural Transformation of the Public Sphere. An Inquiry into a Category of Bourgeois Society. MIT Press

Harris DJ, O'Boyle M, Bates EP, Buckley CM (2014) Law of the European Convention on Human Rights. Oxford

Harvey D (2008, original work of 1973) Social Justice and the City. University of Georgia Press

Henschke A (2017) Ethics in an Age of Surveillance. Cambridge.

Kindt E (2013) Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis. Springer

Kitchin (2015) The Data Revolution. SAGE Publishing

Kitchin R, Dodge M (2014) Code/Space: Software and Everyday Life. MIT Press

Kuntze JH (2018) The Abolishment of the right to privacy. Tectum Verlag

LaFave WR (1996) Search and seizure: a treatise on the fourth amendment. 3rd edn. West Publishing

Lefebvre H (1991, original work of 1974) The Production of Space. Blackwell

Linskey O (2015) The Foundations of EU Data Protection Law. Oxford University Press.

Lyon D (1994) The Electronic Eye: The Rise of the Surveillance Society. University of Minnesota Press

Lyon D (2017) Surveillance Studies. An Overview. Polity Press

Madanipour A (2003) Public and Private Spaces of the City. Routledge

Mantovani F (2013) Diritto Penale: Parte Speciale I. Delitti Contro la Persona, 5th edn. Cedam.

Mayer-Schoenberger V, Cukier K (2013) Big Data. A Revolution that will transform how we live, work, and think. London, John Murray Publishers.

Mitchell D (2003) The Right to the City. Social Justice and the Fight for Public Space. The Guilford Press

Ning H (2011) Unit and Ubiquitous Internet of Things, New York: CRC Press

Nissenbaum H (2009) Privacy in Context. Technology, Policy and the Integrity of Social Life. Stanford University Press, Stanford.

Nussbaum MC (2001) Upheavels of Thought: The Intelligence of Emotions. Cambridge University Press

Peers S, Hervey T, Kenner J, Ward A (2021) The EU Charter of Fundamental Rights: A Commentary, 2nd ed. Hart Publishing, London.

Petersen JK (2012) Introduction to Surveillance Studies. Routledge

Rayes A, Salam S (2019) Internet of Things From Hype to Reality The Road to Digitization. Springer

Savas ES (2000) Privatization and Public-Private Partnerships. New York: Chatham House.

Solove (2008) Understanding Privacy. Harvard University Press

Taylor L, Floridi L, van der Sloot (2017a) Group Privacy. New Challenges of Data Technologies. Springer

Tzanou M (2017) The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. Oxford: Hart Publishing.

Van Dijck J, Poell T, De Waal M (2018) The Platform Society: Public Values in a Connective World. Oxford University Press

Westin A (2018, original work of 1967) Privacy and Freedom. Ig Publishing, New York

Wright D, de Hert P (2012) Privacy Impact Assessment, Media. Dordrecht: Springer Netherlands.

Zuboff S (2019) The Age of Surveillance Capitalism. Profile Books.

Chapters in edited books

Altman I, Zube E (1992) Introduction. In: Altman I, Zube E (eds) Public Places and Spaces. Plenum Press

Andersen A, Karlsen R, Weihai Yu (2018) Green Transportation Choices with IoT and Smart Nudging. In: Maheswaran M, Badidi E (eds) Handbook of Smart Cities. Springer, pp. 338-339.

Andrejevic M (2012) Ubiquitous Surveillance. In: Ball K, Haggerty K, Lyon D (eds.) Routledge handbook of surveillance studies. Routledge

Andrejevic M (2016) Theorizing Drones and Droning Theory. In: Završnik A (ed) Drones and Unmanned Aerial Systems. Springer

Atlam HF, Wills G (2020) IoT Security, Privacy, Safety and Ethics. In: Farsi M et al (eds) Digital Twin Technologies and Smart Cities. Springer

Barocas S, Nissenbaum H (2013) Big Data's End Run around Anonymity and Consent. In: Lane J, Stodden V, Bender S, Nissenbaum H (eds) Privacy, Big Data and Public Good: Frameworks for engagement. Cambridge University Press.

Becker M (2019) Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. Ethics and Information Technology (2019) 21:307–317

Beckwith R, Sherry J, Prendergast D (2019) Data Flow in the Smart City: Open Data Versus the Commons. In: de Lange M., de Waal M. (eds) The Hackable City, 205-221. Springer, Singapore

Bell D (Fall 2020) Communitarianism. In: Zalta EN (ed) The Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/archives/fall2020/entries/communitarianism/. Accessed 19 August 2022.

Bexell M, Moerth U (2010) Introduction: Partnerships, Democracy, and Governance. In: Bexell M, Moerth U (eds) Democracy and Public-Private Partnerships in Global Governance. Palgrave Macmillan.

Bloustein EJ (1984, original work of 1964) Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser. In: Schoeman F (ed) Philosophical Dimensions of Privacy. An Anthology. Cambridge University Press

Bosco F, Creemers N, Ferraris V, Guagnin D, Koops BJ (2015) Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. In: Gutwirth S, Leenes R, De Hert P (eds) Reforming European Data Protection Law. Springer.

Brill M (1992) Transformation, Nostalgia, and Illusion in Public Life and Public Place. In Altman I, Zube E (eds) Public Places and Spaces. Plenum Press

Bröckling U, Krasmann S, Lemke T (2010) From Foucault's Lectures at the Collège de France to Studies of Governmentality. In: Bröckling U, Krasmann S, Lemke T (eds) Governmentality: Current Issues and Future Challenges. Routledge

Brouwer E (2011) Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation. In: Besselink LFM, Prechal S, Pennings F (eds) The Eclipse in the European Union. Kluwer Law International. pp. 273-294.

Catanzariti M, Curtin D (2023a) Data at the boundaries of (European) law: A first cut. In: Curtin D, Catanzariti M (eds) Data at the Boundaries of European Law. Oxford University Press

Catanzariti M, Curtin D (2023b) Beyond Originator Control of Personal Data in EU Interoperable Information Systems: Towards Data Originalism. In: Curtin D, Catanzariti M (eds) Data at the Boundaries of European Law. Oxford University Press

Cayford M, van Gulijk C, van Gelder, P (2015) All swept up: An initial classification of NSA surveillance technology. In: Nowakowski T, Młyńczak M, Jodejko-Pietruczuk A, Werbińska-Wojciechowska S (eds) Safety and Reliability: Methodology and Applications. Routledge, pp. 643-650

Christofi A, Breuer J, Wauters E, Valcke P, Pierson J (2022) Data Protection, Control and Participation beyond Consent - 'Seeking the views' of data subjects in Data Protection Impact Assessments. In: Kosta E, Leenes R, Kamara I (eds) Research Handbook on EU Data Protection Law, pp. 503-529

Cocchia A (2014) Smart and Digital City: A Systematic Literature Review. In: Dameri R, Rosenthal-Sabroux C (eds) Smart City: How to Create Public and Economic Value with High Technology in Urban Space. Springer International Publishing

Custers B (2016) Drones here, there and everywhere Introduction and Overview. In: Custers B (ed) The Future of Drone Use. Springer, Asser Press

Daily SB, James MT, Cherry D, Porter JJ, Darnell SS, Isaac J, Roy T (2017) Affective Computing: Historical Foundations, Current Applications, and Future Trends. In: Jeon M (ed)Emotions and Affect in Human Factors and Human-Computer Interaction. Associated Press. pp. 213-231

De Hert P, Gutwirth S (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In: Claes E, Duff A, Gutwirth A (eds) Privacy and the criminal law. Antwerp/Oxford, Intersentia, pp. 61-104

De Hert P, Gutwirth S (2008) Regulating Profiling in a Democratic Constitutional State. In: Hildebrandt M, Gutwirth S (eds) Profiling the European Citizen: Cross-Disciplinary Perspectives. Springer.

De Hert P, Gutwirth S (2009a) Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In: Gutwirth S, Poullet Y, de Hert P (eds) Data Protection in a Profiled World. Springer

De Hert P (2023) Post- GDPR Lawmaking in the Digital Data Society: Mimesis without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law. In: Curtin D, Catanzariti M (eds) Data at the Boundaries of European Law. Oxford University Press

De Lange M (2019) The Right to the Datafied City: Interfacing the Urban Data Commons. In: Cardullo P, Di Feliciantonio C, Kitchin R (eds) The Right to the Smart City. Emerald Publishing Limited

Della Torre J (2022) Quale spazione per i *tools* di riconoscimento facciale nella giustizia penale? In: Di Paolo G, Pressacco L (eds) Intelligenza Artificiale e Processo Penale: Indagini, Prove e Giudizio. Quaderni della Facoltà di Giurisprudenza, Università di Trento, pp. 7-61

De Terwangne C (2020) Article 5. Principles relating to the processing of personal data. In: Kuner C, Bygrave LA, Docksey C, Drechsler L (eds) The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press

De Waal M (2017) The City is not a Galaxy: Understanding the City through Urban Data. In: Kitchin R, Lauriault TP, McArdle G (eds) Data and the City. Routledge, London.

Dodge M, Kitchin R (2019) The Challenges of Cybersecurity for Smart Cities. In: Coletta C, Leighton E, Heaphy L, Kitchin R (eds) Creating Smart Cities. Routledge, pp. 205-216.

Eijkman Q (2017) Indiscriminate Bulk Data Interception and Group Privacy: Do Human Rights Organisations Retaliate through Strategic Litigation? In: Taylor L, Floridi L, van der Sloot B (eds) Group Privacy. New Challenges of Data Technologies, pp. 123-138. Switzerland: Springer

Etzioni A (2013) Communitarianism. Encyclopædia Britannica. Available at: https://www.britannica.com/topic/communitarianism. Accessed 7 September 2020)

Ferguson AG (2017a) Big Data Surveillance: The Convergence of Big Data and Law Enforcement. In: Gray D, Henderson SE (eds) The Cambridge Handbook of Surveillance Law. Cambridge University Press, New York.

Finn R, Donovan A (2016) Big Data, Drone Data: Privacy and Ethical Impacts of the Intersection Between Big Data and Civil Drone Deployments. In: Custers B (ed) The Future of Drone Use. Springer, Asser Press

Foster RS, Iaione C (2019) Ostrom in the City: Design Principles and Practices for the Urban Commons. In: Hudson B, Rosenbloom J, Cole D (eds) The Routledge Handbook of the Study of the Study of the Commons. Routledge. Available at SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130087. Accessed 7 October 2020

Foucault M (1991) Governmentality. In: Burchell G, Gordon C, Miller P (eds) The Foucault Effect. Studies in Governmentality, 1st ed. Chicago University Press, Chicago

Fried C (1984, original work of 1968) Privacy [A moral analysis]. In: Schoeman F (ed) Philosophical Dimensions of Privacy. An Anthology. Cambridge University Press

Friedland SI (2018) The Internet of Things and Self-Surveillance Systems. In: Gray D, Henderson SE (eds) The Cambridge Handbook of Surveillance Law, pp. 198-224

Gruszczak A (2016) The EU criminal intelligence model – Problems and Issues. In: Banach-Gutierrez JB, Harding C (eds) EU Criminal Law and Crime Policy. Values, Principles and Methods. London – New Work: Routledge, pp. 149-167

Haggerty KD (2006) Tear down the walls: on demolishing the panopticon. In: Lyon D (ed) Theorizing surveillance: The panopticon and beyond. Willan Publishing

Haggerty K, Ericson R (2006) The New Politics of Surveillance and Visibility. In: Haggerty K, Ericson R (eds) The New Politics of Surveillance and Visibility. University of Toronto Press

Henne K (2019) Surveillance in the Name of Governance: Aadhaar as a Fix for Leaking Systems in India. In: Haggart B, Henne K, Tusikov N (eds) Information, Technology and Control in a Changing World. Understanding Power Structures in the 21st Century, pp. 233-245

Hildebrandt M (2006) Privacy and identity. In: Claes E, Duff A, Gutwirth S (eds) Privacy and the Criminal law. Antwerp-Oxford: Intersentia. https://works.bepress.com/mireille_hildebrandt/6/. Accessed 6 January 2022.

Hildebrandt M (2008) A vision of ambient law. In: Brownsword R, Yeung K (eds) Regulating Technologies. Hart;

Hubbard P, Kitchin R (2011) Introduction: Why Key Thinkers?. In: Hubbard P, Kitchin R (eds) Key Thinkers On Space And Place. SAGE Publications

Hussain W (Spring 2018 Edition) The Common Good. In: Zalta EN (ed) The Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/archives/spr2018/entries/common-good/. Accessed: 17 November 2020.

Jülicher T, Delisle M (2018) Step into "The Circle"—A Close Look at Wearables and Quantified Self. In: Hoeren T, Kolany-Raiser B (eds) Big Data in Context. Springer, pp. 81-91

Juszack A, Sason E (2021) Recalibrating Data Retention in the EU. The Jurisprudence of the CJEU – Is this the end or the beginning?. Eucrim 4:238-262

Kitchin R (2017b) Data-driven Urbanism. In: Kitchin R, Lauriault TP, McArdle G (eds) Data and the City. Routledge

Kitchin R, Coletta C, Evans L, Heaphy L (2019a) Creating Smart Cities. In: Kitchin R, Coletta C, Evans L, Heaphy L (eds) Creating Smart Cities. Routledge

Koops BJ, Galič M (2017b) Conceptualizing space and place: lessons from geography for the debate on privacy in public. In: Timan T, Newell BC, Koops BJ (eds) Privacy in Public Space. Conceptual and Regulatory Challenges. Edward Elgar Publishing

Kosta E (2020a) Article 7. Conditions for Consent. In: Kuner C, Bygrave LA, Docksey C, Drechsler L (eds) The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

Kosta (2022) A divided data protection framework: A critical reflection on the choices of the European legislator post-Lisbon. In: Kosta E, Leenes R (eds) Research Handbook on EU Data Protection Law. Edward Elgar Publishing

Kostoris RE (2018) European Law and Criminal Justice. In: Kostoris RE (ed) Handbook of European Criminal Procedure. Springer

Kotschy W (2020) Article 6. Lawfulness of Processing. In: Kuner C, Bygrave LA, Docksey C, Drechsler L (eds) The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press, pp. 329-330.

Kranenborg H (2014) Protection of Personal Data. In: Peers S, Hervey T, Kenner J, Ward A (eds) The EU Charter of Fundamental Rights: A Commentary. Hart Publishing, London, pp. 223–266.

Lock T (2019) Article 8 CFR: Protection of Personal Data. In: Kellerbauer M, Klamert M, Tomkin J (eds) The EU Treaties and the Charter of Fundamental Rights. Oxford University Press.

Loi M, Christen M (2020) Ethical Frameworks for Cybersecurity. In: Christen M et al (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology 21. Springer

Lyon D, Haggerty K, Ball K (2012) Introducing Surveillance Studies. In: Ball K, Haggerty K, Lyon D (eds) Routledge handbook of surveillance studies

Mann S, Nolan J, Wellman B (2003) Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. Surveillance and Society 1(3):331–55

Mantelero A (2019) Comment to Article 35 and 36. In Cole M, Boehm F (eds) GDPR Commentary. Edward Elgar Publishing, Forthcoming. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362747 Accessed 23 February 2021.

Marsch N (2020) Artificial Intelligence and the Fundamental Right to Data Protection: Opening the Door for Technological Innovation and Innovative Protection. In: Wischmeyer T, Rademacher T (eds) Regulating Artificial Intelligence. Springer, pp. 33-52.

Marx GT (2015) Coming to terms: The kaleidoscope of privacy and surveillance. In: Roessler B, Mokrosinska D (eds) Social Dimensions of Privacy: Interdisciplinary Perspectives. Cambridge University Press

McCrudden C, King J (2017) The Dark Side of Nudging: The Ethics, Political Economy, and Law of Libertarian Paternalism. In: Kemmerer A, Möllers C, Steinbeis M, Wagner G (eds) Choice Architectures in Democracies. Exploring the Legitimacy of Nudging. Hart/Nomos, pp. 75-139

Merricks White J (2019) Politicising Smart City Standards. In: Kitchin R, Coletta C, Evans L, Heaphy L (eds) Creating Smart Cities. Routledge

McGarrity N, Williams G (2010) When extraordinary measures become normal: pre-emption in counter-terrorism and other laws. In: Mc Garrity N, Lynch A, Williams G (eds) Counter-terrorism and Beyond. The Culture of Law and Justice after 9/11. Routledge, pp. 131-149

Neroni Rezende I (2021) Predictive Policing: Safeguards for the Choice of Data and Automated Processing in the Preventive Context. In: Barona Vilar S (ed) Justicia algorítmica y neuroderecho. Una mirada multidisciplinar. Tirant lo Blanch.

Neroni Rezende I (2022) Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces. In: Bachmaier Winter L, Ruggeri S (eds) Investigating and Preventing Crime in the Digital Era. Springer, pp. 67-98

Newell BC (2018) Privacy and Surveillance in the Streets. In: Newell BC, Timan T, Koops BJ (eds) Surveillance, privacy and public space. Routledge.

Pagallo U, Durante M, Monteleone S (2017) What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT. In: Leenes et al. (eds) Data Protection and Privacy: (In)visibilities and Infrastructures. Springer, pp. 59- 62.

Patton (2000) Protecting privacy in public? Surveillance technologies and the value of public places. Ethics and Information Technology 2(3):181-187

Poullet Y (2014) About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?. In: Gutwirth S, Poullet Y, de Hert P (eds) Data Protection in a Profiled World. Springer

Prosser WL (1984, original work of 1960) Privacy [A legal analysis]. In: Schoeman F (ed) Philosophical Dimensions of Privacy. An Anthology. Cambridge University Press.

Regan P (2015) Privacy and the Common Good: Revisited. In: Roessler B, Mokrosinska D (eds) The Social Dimensions of Privacy: Interdisciplinary Perspectives. Cambridge University Press

Richter H (2020) The law and policy of government access to private sector data ('B2G data sharing'). In: Max-Planck-Institut für Innovation und Wettbewerb (ed) Data Access, Consumer Interests and Public Welfare. https://www.nomos-elibrary.de/10.5771/9783748924999-529.pdf. Accessed 22 November 2021.

Rodotà S (2009) Data Protection as a Fundamental Right. In: Gutwirth S, Poullet Y, De Hert P, De Terwangne C, Nouwt S (eds) Reiventing Data Protection?. Springer.

Rosenthal L (2018) The case for surveillance. In: Gray D, Henderson SE (eds) The Cambridge Handbook of Surveillance Law

Rouvroy A, Poullet Y (2009) The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth S, Poullet Y, De Hert P, De Terwangne C, Nouwt S (eds) Reiventing Data Protection?. Springer, pp. 45-76.

Rudinow Saetnam A (2018) Security, Concepts of. In: Arrigo BA (ed) The SAGE Encyclopedia of Surveillance, Security, and Privacy. SAGE

Schoeman F (1984) Privacy: philosophical dimensions of the literature. In: Schoeman F (ed) Philosophical Dimensions of Privacy. An Anthology. Cambridge University Press

Schreurs W, Hildebrandt M, Kindt E, Vanfleteren M (2008) *Cogitas, Ergo Sum*. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. In: Hildebrandt M, Gutwirth S (eds) Profiling the European Citizen. Springer, pp. 246-256.

Solove DJ (2015) The meaning and value of privacy. In: Roessler B, Mokrosinska D (eds) Social Dimensions of Privacy: Interdisciplinary Perspectives. Cambridge University Press

Stoddart E (2012) A Surveillance of Care. Evaluating Surveillance Ethically. In: Ball K, Haggerty K, Lyon D (eds.) Routledge handbook of surveillance studies

Taylor L (2019) Ethics. In Ash J, Kitchin R, Leszczynski A (eds) Digital geographies. Sage, 260-270. Author's Final Draft, p. 5. https://research.tilburguniversity.edu/en/publications/ethics. Accessed 31 July 2022.

Thorne C, Griffiths C (2014) Smart, Smarter, Smartest: Redefining Our Cities. In: Dameri R, Rosenthal-Sabroux C (eds) Smart City. How to Create Public and Economic Value with High Technology in Urban Space. Springer

Valverde M (2008) Police, Sovereignty and Law. Foucauldian Reflections. In: Dubber M, Valverde M (eds) Police and the Liberal State. Stanford University Press

van Brakel R (2017) Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing. In: van der Sloot B et al (eds) Exploring the Boundaries of Big Data. Amsterdam: Amsterdam University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2772469. Accessed 24 February 2022

van Brakel R, de Hert P (2011) Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. Cahiers Politiestudies 3(20):165-192

van der Sloot B (2016a) Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities. In: Gutwirth S et al. (eds) Data Protection on the Move. Springer

van der Sloot B, Lanzing M (2021a) The Continued Transformation of the Public Sphere: On the Road to Smart Cities, Living Labs and a New Understanding of Society. In: Nagenborg M, Stone T, González Woge M, Vermaaspp PE (eds) Technology and the City. Towards a Philosophy of Urban
Technologies. Springer, pp. 319-345

Viganò E, Loi M, Yaghmaei E (2020) Cybersecurity of Critical Infrastructure. In: Christen M et al. (eds.), The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology 21. Springer: 157-177

Vogiatzoglou P, Fantin S (2020d) National and Public Security within and beyond the Police Directive. In: Vedder A, Schroers J, Ducuing C, Valcke P (eds) Security and Law. Intersentia, p. 37. See also Harris DJ, O'Boyle M, Bates EP, Buckley CM (2014) Law of the European Convention on Human Rights. Oxford

Vogler R, Fouladvand S (2016) Standards for making factual determinations in arrest and pre-trial detention: a comparative analysis of law and practice. In: Ross, Jacqueline E and Thaman, Stephen C (eds) Comparative criminal procedure. Research handbooks in comparative law . Edward Elgar, pp. 191-216

Warren DS, Brandeis LD (1984, original work of 1890) The Right to privacy [The implicit made explicit]. In: Schoeman F (ed) Philosphical dimensions of privacy. An Antology. Cambridge University Press

Washington M, Richards N (2019) Digital Civil Liberties and the Translation Problem. In: Brown DK, Turner JI, Weisser B (eds) The Oxford Handbook of Criminal Process. Oxford University Press, New York.

Wendell WC (2018) National Security. In: Arrigo BA (ed) The SAGE Encyclopedia of Surveillance, Security, and Privacy. SAGE

Wiig A (2019) Urban Revitalization through Automated Policing and "Smart" Surveillance in Camden, New Jersey. In: Coletta C, Leighton E, Heaphy L, Kitchin R (eds) Creating Smart Cities. Routledge, pp. 49-58.

Wright D, Finn R (2016) Making Drones More Acceptable with Privacy Impact Assessments. In: Custers B (ed) The Future of Drone Use. Springer, Asser Press, pp. 325-321

Završnik A (2016) Introduction: Situating Drones in Surveillance Societies. In: Završnik A (ed) Drones and Unmanned Aerial Systems. Springer

Articles

Albrechtslund A, Lauritsen P (2013) Spaces of everyday surveillance: Unfolding an analytical concept of participation. Geoforum49:310-316

Albino V et al (2015) Smart Cities: Definitions, Dimensions, Performance and Initiatives. Journal of Urban Technology 1

Alemanno A, Spina A (2014) Nudging legally: On the checks and balances of behavioural regulation. International Journal of Constitutional Law 12(2):429-456

Argomaniz J (2009) When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms. Journal of European Integration 31(1):119 -136

Ashby M (2017) The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. European Journal on Criminal Policy and Research 23:441-459

Balkin J (2008) The Constitution in the National Surveillance State. Minnesota Law Review 93(1):1-25

Ball K (2009) EXPOSURE. Information, Communication & Society 12(5):639-657

Bassi E (2020) Urban Unmanned Aerial Systems Operations: On Privacy, Data Protection, and Surveillance. Law in Context 36(2):61-72

Bassi E, Bloise N, Dirutigliano J, Fici GP, Pagallo U, Primatesta S, Quagliotti F (2019) The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win–Win Approach to Data Protection, Aerospace Engineering, and Risk Management. Minds and Machines 29:579–601.

Berman E (2020) Individualized suspicion in the age of big data. Iowa Law Review 105:463-506

Brkan M (2018) The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core. European Constitutional Law Review 14:332-368

Bennett C, Raab C (2020) Revisiting the governance of privacy: Contemporary policy instruments in global perspective. Regulation and Governance 14(3): 447-464

Binns R (2017) Data Protection Impact Assessments: A Meta-Regulatory Approach. International Data Privacy Law 7(1):22-35.

Black J (2012) Paradoxes and Failures: 'New Governance' Techniques and the Financial Crisis." Modern Law Review 75 (6):1037–63

Borgia G (2021) Profili Sistematici delle Tecnologie di Riconoscimento Facciale Automatizzato, anche alla Luce dei Futuribili Sviluppi Normativi sul Fronte Eurounitario. La Legislazione Penale, 11 December 2021.

Borrás S, Edler J (2020) The roles of the state in the governance of socio-technical systems' transformation. Research Policy 49(5): 103971

Braun T, Fung BCM, Iqbal F, Shah B (2018) Security and privacy challenges in smart cities. Sustainable Cities and Society 39:499-507.

Brayne S (2017) Big Data Surveillance: The Case of Policing. American Sociological Review 82:977

Browning M, Arrigo B (2020) Stop and Risk: Policing, Data, and the Digital Age of Discrimination. American Journal of Criminal Justice. https://link.springer.com/article/10.1007%2Fs12103-020-09557-x. Accessed 29 June 2022.

Bu-Pasha S (2020) The Controller's Role in Determining "High Risk" and Data Protection Impact Assessment (DPIA) in Developing Digital Smart City. Information & Communications Technology Law 29(3):391-402.

Caianiello M (2019) Criminal Process faced with the Challenges of Scientific and Technological Development. European Journal of Crime, Criminal Law and Criminal Justice 27(4):267-291

Caianiello M (2021) Dangerous Liasons. Potentialities and Risks Deriving from the interaction between Artificial Intelligence and Preventive Justice, en European Journal of Crime, Criminal Law and Criminal Justice 29:1-23

Calzada I, Amirall E (2020) Data Ecosystems for Protecting European Citizens' Digital Rights. Transforming Government: People, Process and Policy 14(2)

Campbell F (2019) Data Scraping – What Are the Privacy Implications. Privacy & Data Protection 20:3

Cardullo P, Kitchin R (2019b) Smart Urbanism and Smart Citizenship: The Neoliberal Logic of "Citizen-focused" Smart Cities in Europe. Politics and Space 37(5): 813-830

Cassese S (2017) Exploring the Legitimacy of Nudging. Kemmerer A, Möllers C, Steinbeis M, Wagner G (eds) Choice Architectures in Democracies. Exploring the Legitimacy of Nudging. Hart/Nomos

Castelvecchi D (2020) Is Facial Recognition Too Biased to Be Let Loose? Nature 587:347-349, p. 348. https://www.nature.com/articles/d41586-020-03186-4. Accessed 27 June 2022.

Chen J, Edwards L, Urquhart L, McAuley D (2020) Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. International Data Privacy Law 10(4): 279-293

Christofi A, Verdoodt V (2019) Exploring the essence of the right to data protection and smart cities. CiTiP Working Paper. https://ssrn.com/abstract=3483616. Accessed 29 September 2021.

Clifford D, Auloos J (2018) Data Protection and the Role of Fairness. Yearbook of European Law 37(1):130-187.

Cohen J (2013) What privacy is for. Harvard Law Review 126(7):1904-1933

Cohen J (2015a) Studying Law Studying Surveillance. Surveillance & Society 13(1): 91-101.

Cohen J (2015b) The Surveillance-Innovation Complex: The Irony of the Participatory Turn. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466708. Accessed 14 April 2022.

Cohen J (2019) Turning Privacy Inside Out. Theoretical Inquiries in Law 20(1):1-31

Cole MD, Vandendriessche A (2016) From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance. European Data Protection Law Review 1:121-128.

Contissa G, Lasagni G (2020) When it is (also) Algorithms and AI that decide on Criminal Matters: In Search of an Effective Remedy. European Journal Of Crime, Criminal Law And Criminal Justice 28:280-304
Crawford K (2021) Time to regulate AI that interprets human emotions. Nature 592(7853):167. https://www.nature.com/articles/d41586-021-00868-5. Accessed 15 August 2022

Curtin D, Brito Bastos F (2020) Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue. European Public Law 26(1): 59–70

Custers B, Uršič H (2016) Big data and data reuse: A taxonomy of data reuse for balancing big data benefits and personal data protection. International Data Privacy Law 6(1):4-15

Dalla Corte L (2019) Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protecton Law. European Journal of Law and Technology 10(1).

Dalton CM, Taylor L, Thatcher J (2016) Critical Data Studies: A dialog on data and space. Big Data & Society January–June 2016: 1–9

DeCew (2018) Privacy. In: Zalta EN (ed) The Stanford Encyclopedia of Philosophy. Spring 2018 Edition. https://plato.stanford.edu/archives/spr2018/entries/privacy/. Accessed 14 January 2022

Degeling M, Berendt B (2018) What is wrong about Robocops as consultants? A technology-centric critique of predictive policing. AI & Soc 33:347–356

Degrave E (2009) Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée. Chroniques de Droit Public 1:46-71.

De Hert P (2005) Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11. Utrecht Law Review 1(1):69-96.

De Hert P, Gutwirth S, Moscibroda A, Wright D, González Fuster G (2009b) Legal safeguards for privacy and data protection in ambient intelligence. Pers Ubiquit Comput (2009) 13:435–444.

De Hert P, Papakostantinou V (2009c) The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for. Computer law & security review 25:403-414.

De Hert P, Papakonstantinou V (2012) The Police and Criminal Justice Data Protection Directive: Comment and Analysis. Society for Computers and Law (SCL, UK) https://ssrn.com/abstract=3447091 or http://dx.doi.org/10.2139/ssrn.3447091.

De Hert P, Papakostantinou V (2013) The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer Law and Security Review 28(2):130-142.

De Hert P, Malgieri G (2020) Article 8 ECHR Compliant and Foreseeable Surveillance: The ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law. Brussels Privacy Hub Working Paper 6(21):1-42.

Deleuze G (1992, original work of 1990) Postscripts on the Societies of Control. October 59:3-7

Demetzou K (2020) Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. Computer Law & Security Review 35 (2019) 105342

Docksey C (2019) Ministerio Fiscal: Holding the line on ePrivacy. Maastricht Journal of European and Comparative Law 26(4): 585-594

Ducuing C, Schroers J (2020) The recent case law of the CJEU on (joint) controllership: have we lost the purpose of 'purpose'?. Computerrecht Tijdschrift voor Informatica, Telecommunicatie en Recht 6:424-429. Preprint version retrieved from the KU Leuven LIRIAS database

Durante M (2013) Dealing with Legal Conflicts in the Information Society. An Informational Understanding of Balancing Competing Interests. Philos. Technol. 26:437–457.

Earls Davis (2020) Facial Detection and Smart Billboards : Analysing the ' Identified ' Criterion of Personal Data in the GDPR. European Data Protection law Review 6(3):365-377.

Edwards L (2016) Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective. European Data Protection Law Review 1(2):28-58

Egbert S, Krasmann S, Predictive policing: not yet, but soon preemptive? Policing and Society 30:905-919

Emanuilov I, Fantin S, Marquenie T, Vogiatzolgou P (2020) Purpose Limitation by Design as a Counter to Function Creep and System Insecurity in Police AI. In: United Nations Interregional Crime and Justice Research Institute (UNICRI) (ed) Special Collection: Artificial Intelligence

Eskens S (2022) The ever-growing complexity of the data retention discussion in the eu: an in-depth review of la quadrature du net and others and privacy international joined cases c-511/18, c-512/18 and c-520/18 la quadrature du net and others [2020] ecli:eu:c:2020:791; case c-623/17 privacy international [2020] ecli:eu:c:2020:790. European Data Protection Law Review 8(1):143-155

Etzioni A (1996) The Responsive Community: A Communitarian Perspective. American Sociological Review 61(1):1-11

Falkenhayner N (2021) The Cultural Turn in Surveillance Studies: Possibilities and Challenges. European Data Protection Law Review 7(1):9-10

Ferro E, Gennaro C, Nordio A, Paonessa F, Vairo C, Virone G, Argentieri A, Berton A, Bragagnini A (2020) 5G-Enabled Security Scenarios for Unmanned Aircraft: Experimentation in Urban Environment. Drones 4(22):1-13

Feldman Barrett L (2017) The theory of constructed emotion: an active inference account of interoception and categorization. Soc Cogn Affect Neurosci 12(11):1–23

Ferguson AG (2017b) Policing Predictive Policing. Washington University Law Review 94(5):1109-1190

Ferguson AG (2020) Structural sensor surveillance. Iowa Law Review 106(1):47-112

Ferretti F (2014) Data protection and the legitimate interest of data controllers: Much ADO about nothing or the winter of rights?. Common Market Law Review 51(4): 843-868.

Ferretti MP (2010) Risk and Distributive Justice: The Case of Regulating New Technologies. Sci Eng Ethics 16:501–515.

Finch K, Tene O (2016) Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town. Fordham Urban Law Journal 41(5): 1581-1615

Finch K, Tene O (2017) Smart Cities: Privacy, Transparency, and Community. In: Selinger E, Polonetsky J, Tene Omer (eds) The Cambridge Handbook of Consumer Privacy. Cambridge University Press

Finger M, Razaghi M (2017) Conceptualizing "Smart Cities". Informatik-Spektrum 40(1):6-13

Flor R (2014) La Corte di giustizia considera la direttiva europea 2006/24 sulla cd. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?. Dir. Pen. Cont. – Riv. trim. 2:178-188

Floridi L (2005) The ontological interpretation of informational privacy. Ethics and Information Technology (2005) 7:185–200

Floridi L (2017) Infraethics–on the Conditions of Possibility of Morality. Philosophy and Technology 30(4):391-394

Floridi L (2021) The End of an Era: From Self-Regulation to Hard Law for the Digital Industry. Philosophy & Technology 34(4):619–622

Froomkin A (2015) Regulating mass surveillance as privacy pollution: Learning from environmental impact statements. University of Illinois Law Review 5: 1713-1790.

Fussey P, Coaffe J (2012) Urban Spaces of Surveillance. In: Ball K, Haggerty K, Lyon D (eds.) Routledge handbook of surveillance studies

Fuster Morel M, Espelt R (2018) A Framework for Assessing Democratic Qualities in Collaborative Economy Platforms: Analysis of 10 Cases in Barcelona. Urban Science 61(2):1-13.

Galetta A, De Hert P (2014) Complementing the surveillance law principles of the ECtHR with its environmental law principles: An integrated technology approach to a human rights framework for surveillance. Utrecht Law Review 10(1):55-75

Galič M, Gellert R (2021) Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. Computer Law and Security Review 40:105486.

Galič M, Timan T, Koops BJ (2017) Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. Philosophy and Technology 30(1):9-37

Gandy OH, Nemorin S (2019) Toward a political economy of nudge: smart city variations, Information, Communication & Society 22(14):2112-2126

Gavinson R (1980) Privacy and the Limits of the law. The Yale Law Journal 89(3):421-471

Gómez-Arosteguei T (2005) Defining Private Life under the European Convention on Human Rights by Referring to Reasonable Expectations. California Western International Law Journal 35:155-202

Gonçalves ME (2020) The Risk-based Approach under the New EU Data Protection Regulation: A Critical Perspective. Journal of Risk Regulation 23(2):139-152.

Goodman EP, Powles J (2019) Urbanism under Google: Lessons from Sidewalk Toronto. Fordham Law Review 88:457-498

Graham S, Wood D (2003) Digitizing surveillance: Categorization, space, inequality. Critical Social Policy 23(2): 227-248

Greze B (2019) The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives. International Data Privacy Law 9:109

Guild E, Carrera S (2014) The political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. CEPS Liberty and Security in Europe Paper no. 65, p. 3. https://www.ceps.eu/download/publication/?id=8503&pdf=EG%20and%20SC%20Data%20retention.pdf. Accessed 2 May 2022.

Hadjimatheou K (2017) Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence. Philos. Technol. (2017) 30:39–54

Haggerty KD, Ericson RV (2000) The Surveillance Assemblage. British Journal of Sociology 51(4):605-622

Hahn I (2021) Purpose limitation in the time of data power: Is there a way forward?. European Data Protection Law 7(1):31-44.

Halper T (1996) Privacy and autonomy: From Warren and Brandeis to *Roe* and *Cruzan*. Journal of Medicine and Philosophy 21(2):121-135

Hardyns W, Rummens A (2018) Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. European Journal on Criminal Policy and Research 24:201-218

Harrison C et al (2010) Foundations for Smarter Cities. IBM Journal of Research and Development 54(4):1-16

Heaven D (2019) Deep Trouble for Deep Learning. Nature 574:163-166

Hildebrandt M (2010) Law As Computation in the Era of Artificial Legal Intelligence. Speaking Law to the Power of Statistics. https://repository.ubn.ru.nl/bitstream/handle/2066/189773/189773-1.pdf?sequence=1&isAllowed=y. Accessed 3 December 2021.

Hildebrandt M (2013) Balance or Trade-off? Online Security Technologies and Fundamental Rights. Philosophy and Technology 26(4):357-379.

Hildebrandt, Koops (2010) The Challenges of Ambient Law and Legal Protection in the Profiling Era. Modern Law Review 73(3):228-260.

Hiller JS, Blanke JM (2017) Smart cities, big data, and the resilience of privacy. Hastings Law Journal 68(2):309-356

Hofmann J, Katzenbach C, Gollatz K (2017) Between coordination and regulation: Finding the governance in Internet governance. New Media and Society 19(9): 1406-1423

Hollands RG (2008) Will the Real Smart City Please Stand Up?. City 12:303-320

Hoofnagle CJ, van der Sloot B, Borgesius FZ (2019) The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law 28(1):65-98

Hummel P, Braun M, Dabrock P (2020) Own Data? Ethical Reflections on Data Ownership. Philosophy & Technology. https://doi.org/10.1007/s13347-020-00404-9

Hung TW, Yen CP (2020) On Person-based Predictive Policing of AI. Ethics and Information Technology. https://doi.org/10.1007/s10676-020-09539-x

Iaione C, De Nictolis E, Berti Suman A (2019) The Internet of Humans (IoH): Human Rights and Co-Governance to Achieve Tech Justice in the City. Law & Ethics of Human Rights 13(2): 263-299.

Ienca M, Malgieri G (2021) Mental Data Protection and the GDPR. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840403. Accessed 8 July 2021

Jacobs F (2006) The Role of the European Court of Justice in the Protection of the Environment. Journal of Environmental Law 18(2):185–205

Janeček V (2018) Ownership of personal data in the Internet of Things. Computer Law & Security Review 34:1039-1052

Jansen F (2018) Data Driven Policing in the Context of Europe. DATAJUSTICE Working Paper.

Jasserand C (2018) Subsequent use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?. Eur. Data Prot. L. Rev. 4(2): 152-167

Jin J, Gubbi J, Marusic S, Palaniswami M (2014) An Information Framework for Creating a Smart City Through Internet of Things. IEEE Internet of Things Journal 1(2):112-121.

Johnson JA (2014) From Open Data to Information Justice. Ethics Inf Technol (2014) 16:263–274

Kamara I, De Hert P (2018) Understanding the Balancing Act behind the Legitimate Interest of the Controller Ground. Brussels Privacy Hub Working Paper 4(12).

Kaminski M, Malgieri G (2021) Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations, p. 11. Available at SSRN. https://ssrn.com/abstract=3456224. Accessed 27 December 2021.

Keymolen E, Voorwinden A (2019) Can we negotiate? Trust and the rule of law in the smart city paradigm. International Review of Law, Computers and Technology 34(3):233-253.

Kindt E (2018) Having Yes, Using No? About the New Legal Regime for Biometric Data. Computer Law & Security Review 34:523

Kitchin R (2016a) The ethics of smart cities and urban science. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 374374:20160115.

Kitchin R (2017a) The Realtimeness of Smart Cities. TECNOSCIENZA Italian Journal of Science & Technology Studies 8(2):19-41.

Kitchin R, Cardullo P, Di Feliciantonio C (2019b) Citizenship, Justice and the Right to the Smart City. In: Cardullo P, Di Feliciantonio C, Kitchin R (eds) The Right to the Smart City, 1st edn. Emerald Publishing

Kitchin R, Dodge M (2019c) The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. Journal of Urban Technology, 26(2):47-65.

Koerner M (2015) Drones and the fourth amendment: Redefining expectations of privacy. Duke Law Journal 64(6): 1130-1172

Koops BJ (2014a) The Trouble with EU data protection law. International Data Privacy Law 4(4):250-260.

Koops BJ (2014b) On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy. Politica e Società 3(2):247-264.

Koops BJ (2018) Privacy Spaces. West Virginia Law Review 121(2):611-665

Koops BJ (2021) The Concept of Function Creep. Law, Innovation and Technology 13(1):29-56.

Koops BJ, Clayton Newell B, Timan T, Škorvánek I, Chokrevski T, Galič M (2017) A Typology of Privacy. U. Pa. J. Int'l L. 38:483-575

Kosta E (2020b) Algorithmic state surveillance: Challenging the notion of agency in human rights. Regulation and Governance. May Issue

Kosti N, Levi-Faur D, Mor G (2019) Legislation and regulation: three analytical distinctions, The Theory and Practice of Legislation 7(3):169-178

Kotsoglou KN, Oswald M (2020) The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention. Forensic Science International: Synergy 2:86-69

Krassmann S (2017) Imagining Foucault. On the digital subject and "visual citizenship". Foucault Studies 23:10-26

Kroll JA, Huey J, Barocas S, Felten EW, Reidenberg JR, Robinson D., Harlan YUH (2016) Accountable Algorithms. University of Pennsylvania Law Review 165:1-66

Kuklin B (1997) The Plausibility of Legally Protecting Reasonable Expectations. Valparaiso University Law Review 32(1):19-66

Kumar K, Makarova E (2008) The Portable Home: The Domestication of Public Space. Sociological Theory 26(4):324-343

Kummitha RKR, Crutzen N (2017) How do we understand smart cities? An evolutionary perspective. Cities 67:43-52

Lacerda F et al (2019) An Information Architecture Framework for the Internet of Things. Philosophy & Technology 32:727–744

Lasagni G (2018) Tackling phone searches in Italy and the United States: Proposals for a technological rethinking of procedural rights and freedoms. New Journal of Criminal Law 9(3): 386–401

Leenes R (2007) Do they know me? Deconstructing Identifiability. University of Ottawa Law and Technology Journal 4(1-2):137-161.

Lin Y, Shen Z, Teng X (2021) Review on Data Sharing in Smart City Planning Based on Mobile Phone Signaling Big Data: From the Perspective of China Experience: Anonymization VS De-anonymization. International Review for Spatial Planning and Sustainable Development 9(2):76-93.

Linder S (1999) Coming to Terms with the Public-Private Partnerships. A Grammar of Multiple Meanings. American Behavioural Scientist 43(1):35-51

Linskey O (2014) Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order. International and Comparative Law Quarterly 63(3):569-597.

Linskey O (2019) Criminal justice profiling and EU data protection law: precarious protection from predictive policing. International Journal of Law in Context 15:162–176.

Lotte H (2020) Stop the creep of biometric surveillance technologies. European Data Protection Law Review 6(2):173-174

Lyon D (2003a) Introduction. In: Lyon D (ed) Surveillance as social sorting: Privacy, risk and automated discrimination. Routledge

Lyon (2003b) Surveillance as Social Sorting. In: Lyon D (ed) Surveillance as social sorting: Privacy, risk and automated discrimination. Routledge

Lyon D (2010) National IDs in a Global World: Surveillance, Security, and Citizenship. Case Western Reserve Journal of International Law 42(3):607-623

Lyon D, Bennett C (2008) Playing the ID Card: Understanding the Significance of Identity Card Systems. In: Lyon D, Bennett C (eds) Playing the Identity Card. Surveillance, security and identification in a global perspective. Routledge

MacMahon A, Buyx A, Prainsack B (2020) Big Data Governance Needs More Collective Responsibility: The Role of Harm Mitigation in the Governance of Data Use in Medicine and Beyond. Medical Law Review 28(1):155–182

Macnish K (2015) An Eye for an Eye: Proportionality and Surveillance. Ethical Theory and Moral Practice 18(3): 529-548

Madison M (2020) Tools for Data Governance. Technology and Regulation: 29-43.

Mantelero A (2016) Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection. Computer Law & Security Review 32:238–255.

Mantelero A (2018) AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. Computer Law & Security Review 34:754–772

Mantelero A, Vaciago G, Esposito S, Monte N (2021) The Common EU Approach to Personal Data and Cybersecurity Regulation. International Journal Of Law And Information Technology (forthcoming), p. 21.

Marat E, Sutton Deborah (2021) Technological Solutions for Complex Problems: Emerging Electronic Surveillance Regimes in Eurasian Cities. Europe-Asia Studies 73(1):243-267.

March H, Ribera-Fumaz R (2016) Smart Contradictions: The Politics of Making Barcelona a Self-Sufficient City. European Urban and Regional Studies 23(4): 816-830

Marcuse P (2009) From critical urban theory to the right to the city. City 13(2–3):185-196

Marin L (2016) The fate of the Data Rentention Directive: about mass surveillance and fundamental rights in the EU legal order. In: Mitsilegas V, Bergström M, Konstadinides T (eds) Research Handbook on EU Criminal Law. Edward Elgar Publishing,

Marsden C (2008) Beyond Europe: The Internet, regulation, and multistakeholder governance – Representing the consumer interest?. Journal of Consumer Policy 31(1):115-132

Marsden C (2011) Internet Co-regulation and Constitutionalism: Towards a More Nuanced View, 10. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1973328. Accessed 5 August 2021

Marx G (2001) Murky Conceptual Waters: The Public and the Private. Ethics and Information Technology 3: 157–169

Matzner T (2017) Opening Black Boxes Is Not Enough - Data-based Surveillance in Discipline and Punish. Foucault Studies 23:24-45

Mc Stay A (2020) Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. Big Data & Society January-June 2020:1-12

Melgaço L, van Brakel R (2021) Smart Cities as Surveillance Theatre. Surveillance & Society 19(2): 244-249

Meijer A, Thaens M (2018) Urban Technological Innovation: Developing and Testing a Sociotechnical Framework for Studying Smart City Projects. Urban Affairs Review 54(2):363-387

Micheli M (2022) Public bodies' access to private sector data. The perspectives of twelve European local administrations. First Monday 27(2). https://firstmonday.org/ojs/index.php/fm/article/view/11720/10600. Accessed 8 August 2022.

Micheli M, Ponti M, Craglia M, Berti Suman A (2020) Emerging models of data governance in the age of datafication. Big Data and Society July-December:1-15

Milaj J, Ritsema van Eck GJ (2020) Capturing licence plates: police-citizen interaction apps from an EU data protection perspective. International Review of Law, Computers & Technology, 34(1):1-21.

Miller K (2014) Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm. J. Tech. L. & Pol'y 19:105-149

Mitsilegas V, Guild E, Kuskonmaz E, Vavoula N (2022) Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. European Law Journal:1-36

Mitsilegas V (2015) The Transformation of Privacy in an Era of Pre-emptive Surveillance. Tilburg Law Review 20(1):35-57

Mittelstadt BD, Allo P, Taddeo M, Watcher S, Floridi L (2016) The Ethics of Algorithms: Mapping the Debate. Big Data & Society

Moerel L, Prins C (2016), Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things. https://ssrn.com/abstract=2784123. Accessed 9 September 2021.

Mohanty SP, Choppali U, Kougianos E (2016) Everything you wanted to know about smart cities. IEEE Consumer Electronics Magazine 5(3):60-70

Mokrosinska D (2018) Privacy and Autonomy: On some misconceptions concerning the political dimensions of privacy. Law and Philosphy37(2):117-143

Moore A (2003) Privacy: Its meaning and value. American Philosophical Quaterly 40(3):215-227

Moreham N (2006) Privacy in Public Places. Cambridge Law Journal 65(3):606-63

Mulligan D, Koopman C, Doty N (2016) Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. Phil.Trans.R.Soc.A 374: 20160118.

Murakami Wood D (2013) What is global surveillance? Towards a relational political economy of the global surveillant assemblage. Geoforum 43:317-326

Murakami Wood D, and Steeves V (2021) Smart Surveillance. Surveillance & Society 19(2): 150-153

Neroni Rezende I (2020a) Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention. Sistema Penale 5:183-198, pp. 196-197

Neroni Rezende I (2020b) Facial recognition in police hands: Assessing the "Clearview case" from a European perspective. New Journal of European Criminal Law 11(3):375-389.

Nissenbaum H (1998) Protecting privacy in an information age: The problem of privacy in public. Law and Philosophy 17(5-6): 559-596

O'Flaherty M (2020) Facial recognition technology and fundamental rights. European Data Protection Law Review 6(2):170-173

Ojanen T (2016) Making the essence of fundamental rights real: The court of justice of the European Union clarifies the structure of fundamental rights under the Charter. European Constitutional Law Review 12(2):318-329

Pagallo U, Casanovas P, Madelin R (2019) The Middle-Out Approach: Assessing Models of Legal Governance in Data protection, Artificial Intelligence, and the Web of Data. The Theory of Practice and Legislation 7(1):1-25.

Pagallo U, Ciani Sciolla J, Durante M (2022) The environmental challenges of AI in EU law: lessons learned from the Artificial Intelligence Act (AIA) with its drawbacks. Transforming Government: People, process and policy. https://www.emerald.com/insight/content/doi/10.1108/TG-07-2021-0121/full/html?skipTracking=true. Accessed 13 August 2022.

Papakonstantinou V, De Hert P (2022) The Regulation of Digital Technologies in the EU: The law-making phenomena of "act-ification", "GDPR-mimesis" and "EU law brutality". Technology and Regulation:48-60.

Peppet S (2014) Regulating the internet of things: First steps toward managing discrimination, Privacy, Security, and Consent. Texas Law Review 93(1):85-179.
Picon A (2019) Smart cities, privacy and the pulverisation/reconstruction of individuals. European Data Protection Law Review 5(2):154-155.

Pino G (2006) Conflitto e Bilanciamento tra Diritti Fondamentali. Una mappa dei problemi. Etica e Politica 1:1-57

Pollicino O, Bassini M (2017) La Corte di giustizia ed una trama ormai nota: la sentenza Tele 2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico. Dir. pen. cont., 9 January 2017.Poullet Y (2021) Artificial Intelligence and Public Services – the Role of Public Authorities in the Service of the "Third Way" Drawn up by the European Commission. European Review of Digital Administration & Law - Erdal 2:(2)129-148

Prainsack B (2019) Logged out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons. Big Data and Society 6(1):1-15

Purcell M (2002) Excavating Lefebvre: The Right to the City and Its Urban Politics of the Inhabitant. GeoJournal 58:99-108

Purcell M (2016) Possible Worlds: Henri Lefebvre and the Right to the City. Journal of Urban Affairs 36(1):141-154

Purtova N (2015) Illusion of Personal Data as No One's Property. Law, Innovation and Technology 7(1). Available at SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2346693. Accessed 7 October 2020

Purtova N (2018a) The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology 10(1):40-81, pp. 57-59.

Purtova N (2018b) Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnership. International Data Privacy Law 8:52

Quattrocolo S (2019a) Equità del processo penale e automated evidence alla luce della Convezione europea dei diritti dell'uomo. Revista Ítalo-Española de Derecho Procesal 2:1-17.

Raab C (2020) Information privacy, impact assessment, and the place of ethics. Computer Law and Security Review 37: 105404.

Ranchordás S (2018) Citizens as Consumers in the Data Economy: The Case of Smart Cities. Journal of European Consumer and Market Law 4:154-161.

Ranchordás S (2019) Nudging Citizens through Technology in Smart Cities. University of Groningen Faculty of Law Research Paper Series No. 1/2019. Available at SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333111. Accessed 1 April 2022

Ranchordás S (2020) Nudging citizens through technology in smart cities. International Review of Law, Computers & Technology 34(3):254-276

Ranchordás S, Goanta C (2020) The New City Regulators: Platform and Public Values in Smart and Sharing Cities. Computer Law and Security Review 36:105375.

Rao U, Nair V (2019) Aadhaar: Governing with Biometrics. South Asia: Journal of South Asian Studies 42(3):469-481

Rauhofer J (2014) "Look to yourselves, that we lose not those things which we have wrought". What do the proposed changes to the purpose limitation principle mean for public bodies' rights to access third-party data?. International Review of Law, Computers and Technology 28(2):144-158.

Reidenberg J (2014) Privacy in Public. University of Miami Law Review 69(1):141-159

Reynaers A (2014) Public Values in Public–Private Partnerships. Public Administration Review 74(1):41-50

Ross TW, Yan J (2015) Comparing Public–Private Partnerships and Traditional Public Procurement: Efficiency vs. Flexibility. Journal of Comparative Policy Analysis: Research and Practice 17(5):448-466

Ruppert E (2006) Rights to public space: Regulatory reconfigurations of liberty. Urban geography 27(3):271-292

Sacchetto E (2020) *Face to Face* : Il complesso rapporto tra *automated facial recognition* e processo penale. La legislazione penale, 16 October 2020.

Sadowski J, Pasquale F (2015) The Spectrum of Control: A Social Theory of the Smart City. University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2015–26. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2653860. Accessed 10 August 2020.

Sadowski J, Bendor R (2019) Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary. Science Technology and Human Values 44(3): 540-563.

Sánchez-Monedero J, Dencik L (2020) The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl. Information, Communication & Society. doi: 10.1080/1369118X.2020.1792530.

Sedenberg E, Chuang J (2017) Smile for the Camera: Privacy and Policy Implications of Emotion AI. http://arxiv.org/abs/1709.00396. Accessed 3 July 2021

Schuilenburg M, Peeters R (2018) Smart cities and the architecture of security: pastoral power and the scripted design of public place. City Territ Archit 5(13)

Schwartz P, Solove D (2011) The PII problem: Privacy and a new concept of personally identifiable information. New York University Law Review 86(6):1814-1894

Sharon T, Koops BJ (2021) The ethics of inattention: revitalising civil inattention as a privacy-protecting mechanism in public spaces. Ethics and Information Technology. https://doi.org/10.1007/s10676-020-09575-7.

Shaw J, Graham M (2017) An Informational Right to the City? Code, Content, Control, and the Urbanization of Information. Antipode 49(4):907–927

Singh PJ, Vipra J (2019) Economic Rights Over Data: A Framework for Community Data Ownership. Development 62:53-57

Sunstein C (2015) The Ethics of Nudging. Yale Journal on Regulation 32(2):413-450

Taddeo M (2016) Data philanthropy and the design of the infraethics for information societies. Phil.Trans.R.Soc.A 374: 20160113

Taekema S (2018) Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice. Law and Method. Available at SSRN: https://ssrn.com/abstract=3123667. Accessed 5 Aug 2021.

Tavani HT (2008) Floridi's ontological theory of informational privacy: Some implications and challenges. Ethics and Information Technology 10(2-3): 155-166

Taylor J (2002) Privacy and autonomy: A reappraisal. Southern Journal of Philosophy 40(4):587-604

Taylor L (2016a) What is data justice? The case for connecting digital rights and freedoms globally. Big Data & Society July–December 2017: 1–14

Taylor L (2016b) The Ethics of Big Data as a Public Good: Which Public? Whose Good?. Phil.Trans.R.Soc.A 374: 20160126

Taylor L, Purtova N (2019) What is Responsible and Sustainable Data Science?. Big Data and Society. July-December 2019:1-6

Taylor L, Richter C (2017b) The Power of Smart Solutions: Knowledge, Citizenship, and the Datafication of Bangalore's Water Supply. Television & New Media 18(8):721 –733

Thomsen F (2020) The Teleological Account of Proportional Surveillance. Res Publica 26:373-401

Timan T, Galič M, Koops BJ (2017) Surveillance Theory and Its Implications for Law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3098182. Accessed 13 April 2022.

Tracol X (2019) Ministerio fiscal: access of public authorities to personal data retained by providers of electronic communications services. European Data Protection Law Review 5(1):127-135

Trubek DM, Trubek, LG (2007) New governance & legal regulation: Complementarity, rivalry, and transformation. Columbia Journal of European Law 13(3):539-564

Tversky A, Kahneman D (1981) The Framing of Decisions and the Psychology of Choice. Science 211(4481): 453-458

Tzanou M, Karyda S (2022) Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga? European Public Law 28(1):123-154

Uchida G (2009) A National Discussion on Predictive Policing: Defining our Terms and Mapping Successful Implementation Strategies, US National Institute of Justice Working Paper. https://www.ncjrs.gov/pdffiles1/nij/grants/230404.pdf. Accessed 29 June 2022.

Urgessa WC (2017) The Protective Capacity of the Criterion of "Identifiability" under EU Data Protection Law. European Data Protection Law Review 2(4):521-531, pp. 524-525.

Vaele M, Borgesius FZ (2021) Demystifying the Draft EU Artificial Intelligence Act. https://osf.io/preprints/socarxiv/38p5f. Accessed 8 July 2021

van Brakel R, de Hert P (2011) Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. Cahiers Politiestudies 3(20):165-192

Vandercruysse L, Buts C, Dooms M (2019) Data control in smart city services: Pitfalls and how to resolve them. European Data Protection Law Review 5(4):554-560.

Vandercruysse L, Buts C, Dooms M (2020) A typology of Smart City services: The case of Data Protection Impact Assessment. Cities 104:102731

van der Sloot B (2016b) The Practical and Theoretical Problems with "Balancing": Delfi, Coty and the Redundancy of the Human Rights Framework. Maastricht Journal of European and Comparative Law 23(3):439-459

van der Sloot B, Kosta E (2019) Big Brother Watch and Others v UK: Lessons from the latest Strasbourg Ruling on Bulk Surveillance. European Data Protection Law Review 5(2):252-261

van der Sloot B, van Schlendel S (2021b) Procedural law for a data-driven society. Information and Communications Technology Law 30(3):304-332.

Van Dijk J (2014) Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. Surveillance and Society 12(2):197-208.

Van Dijk N, Gellert R, Rommetveit K (2016) A Risk to a Right? Beyond Data Protection Risk Assessments. Computer Law & Security Review 32:286-306.

Vanolo A (2014) Smart Mentality: The Smart City as Disciplinary Strategy. Urban Studies 51(3):883-898

Vanolo A (2016) Is There Anybody Out There? The Place and Role of Citizens in Tomorrow's Smart Cities. Futures 82:26-36

van Zoonen L (2016) Privacy concerns in smart cities. Government Information Quarterly 33(3):472-480

Vervaele JAE (2005) Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?. Revue internationale de droit pénal 76(3-4):409-443

Vogelmann F, Bernardy J (2017) 40 Years After Discipline and Punish. Foucault Studies 23:4-9

von Grafenstein M (2020) Refining the concept of the right to data protection in article 8 ECFR - part I: Finding an appropriate object and concept of protection by re-connecting data protection law with concepts of risk regulation. European Data Protection Law Review 6(4):509-521.

Voorwinden A (2021) The privatised city: technology and public-private partnerships in the smart city. Law, Innovation and Technology 13(2):439-463

Vogiatzoglou P (2018) Centrum för Rättvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy. European Data Protection Law Review 4(4):563-567

Vutsova A, Ignatova O (2014) The role of public-private partnership for effective technology transfer. Applied Technologies and Innovations 10(3):83-90

Walzer M (1986) Pleasures & Costs of Urbanity. Dissent 3: 470–475

Wilkins R (1987) Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis. Vanderbilt Law Review 40(5): 1077-1129

Winter JS (2014) Surveillance in ubiquitous network societies: Normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. Ethics and Information Technology 16(1):27-41

Wisman THA (2013) Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things. European Journal of Law and Technology 4(2).

Woo JW (2017) Smart cities pose privacy risks and other problems, but that doesn't mean we shouldn't build them. UMKC Law Review 85(4):953-972, pp. 960-961.

Zachariadis M (2019) Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. Information and Organization 29(2):105-11

Zalnieriute M, Churches G (2020) When a "Like" Is Not a "Like": A New Fragmented Approach to Data Controllership. Modern Law Review 83(4):861-876.

Ziosi M, Hewitt B, Juneja P, Taddeo M, Floridi L (2022) Smart Cities: Mapping their Ethical Implications. https://ssrn.com/abstract=4001761. Accessed 31 July 2022.

Zuboff S (2015) Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology 30:75–89

Conference proceedings

Breuer J, Van Zeeland I, Pierson J, Heyman R (2019) The Social Construction of Personal Data Protection in Smart Cities. 2019 CTTE-FITCE: Smart Cities and Information and Communication Technology, CTTE-FITCE 2019.

Calzada I, Almirall E (2019), Barcelona's Grassroots-led Urban Experimentation: Deciphering the 'Data Commons' Policy Scheme. Zenodo. DOI:10.5281/zenodo.2604618. Conference Data for Policy 2019, London (UK), 11-12 June. https://www.compas.ox.ac.uk/wp-content/uploads/Barcelonas-grassroots-led-urban-experimentation-Deciphering-the-data-commons-policy-scheme.pdf. Accessed 8 October 2020

Chen C et al (2018) Distinct Facial Expressions Represent Pain and Pleasure Across Cultures. Proceedings of the National Academy of Sciences of the United States of America 115(43):E10013–E10021. https://www.pnas.org/content/pnas/115/43/E10013.full.pdf. Accessed 2 July 2021.

Resmini A, Lacerda F (2016) The Architecture of Cross-channel Ecosystems: From Convergence to Experience. Proceedings of the 8th International Conference of Digital Ecosystems: 17-21

Doctoral theses

Dalla Corte L (2020) Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development of the smart city environment. Doctoral dissertation. https://research.tilburguniversity.edu/en/publications/safeguarding-data-protection-in-an-open-data-world-on-the-idea-of. Accessed 19 November 2021.

Galič M (2019) Surveillance and Privacy in Smart Cities and Living Labs: Conceptualizing Privacy for Public Space. Doctoral Thesis. Rotterdam, Optima Graphische Communicatie.

Palka P (2017) Virtual Property. Towards a General Theory. Doctoral Dissertation

Reports

Amnesty International (2017) Smart Cities: Utopian Vision, Dystopian Reality, pp. 22-23. https://privacyinternational.org/report/638/smart-cities-utopian-vision-dystopian-reality#:~:text=The%20smart%20city%20market%20is,data%20to%20provide%20better%20services. Accessed 21 January 2022.

Amnesty International (2018) Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database. https://www.amnesty.org.uk/files/reports/Trapped%20in%20the%20Matrix%20Amnesty%20report.pdf. Accessed 28 February 2022.

Article 19 (2021) Emotional Entanglement: China's emotion recognition market and its implications for human rights. https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf. Accessed 22 June 2020

Bass T, Sutherland E, Symons T (2018) Reclaiming the Smart City. Personal data, trust and the new commons. DECODE.

Bertuzzi L (2022) AI regulation filled with thousands of amendments in the European Parliament. EURACTIV. https://www.euractiv.com/section/digital/news/ai-regulation-filled-with-thousands-of-amendments-in-the-european-parliament/. Accessed 5 August 2022

Bollier D (2016) The City as a Platform: How Digital Networks Are Changing Urban Life and Governance. Aspen Institute. https://csreports.aspeninstitute.org/documents/CityAsPlatform.pdf. Accessed 8 August 2020.

Centre de recherches routières – Service public régional de Bruxelles (2018) Méthodes de comptages piétons dans l'espace public, p. 6. https://mobilitepietonne.ch/wordpress/wp-content/uploads/2018/05/vm5-comptages-pietons.pdf. Accessed 21 December 2021.

Christofi A (2021) Smart Cities and the Data Protection Framework in Context. SPECTRE Project Deliverable D 1.2.

Davis R (2015) The Internet of Things: Challenges and Opportunities. EPRS Briefings, 1. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI%282015%29557012_EN.pdf. Accessed 27 July 2017

ECtHR Press Unit (2022) Factsheet – Mass Surveillance. https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf. Accessed 20 April 2022.

European Union Agency for Fundamental Rights (2019) Facial recognition technology: fundamental rights considerations in the context of law enforcement

European Court of Auditors (2018) Public Private Partnerships in the EU: Widespread shortcomings and limited benefits, p. 12. https://www.eca.europa.eu/Lists/ECADocuments/SR18_09/SR_PPP_EN.pdf. Accessed 3 January 2022.

European Parliament's Committee on Industry, Research and Energy (2014) Mapping Smart Cities in the EU. https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOLITRE_ET%282014%29507480_EN.pdf. Accessed 24 Jun 2021.

FEMM Committee of the European Parliament (2021) Women and Transport, pp. 15 ff. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/701004/IPOL_STU(2021)701004_EN.pdf. Accessed 11 August 2022.

Finn R, Wright D, De Hert P, Jacques L (2015) Privacy, data protection and ethical risks in civil RPAS operations - Final Report, p. 27. https://op.europa.eu/en/publication-detail/-/publication/6343df3f-a30d-4a76-943f-f5b810526596/language-en/format-PDF. Accessed 21 June 2022

Giffinger R, Fertner C, Kramar H et al (2007) Smart Cities: Ranking of European Medium-sized Cities. Center of Regional Science Vienna. http://www.smart-cities.eu/download/smart_cities_final_report.pdf. Accessed 24 Jun 2021.

González Fuster G (2020) Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights, Study requested by the LIBE Committee.

High-Level Expert Group on Business-to-Government Data Sharing (2020) Towards a European strategy on business-to-government data sharing for the public interest. https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf. Accessed 8 August 2022.

iBorderCrtl (2016) The Project. https://www.iborderctrl.eu/The-project. Accessed 11 July 2021.

ICAO (2011) Unmanned Aircraft Systems (UAS), p. x. https://www.icao.int/meetings/uas/documents/circular%20328_en.pdf. Accessed 21 June 2022.

Kitchin R (2016b) Getting smarter about smart cities: Improving data privacy and data security. Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Morozov E, Bria F (2018) Rethinking the Smart City: Democratizing Urban Technology. Rosa Luxemburg Stiftung (New York Office), pp. 2-4. Available at: http://www.rosalux-nyc.org/rethinking-the-smart-city/. Accessed 23 Jul 2020.

OECD (2016) The Internet of Things: Seizing the Benefits and Addressing the Challenges. https://www.oecd-ilibrary.org/docserver/5jlwvzz8td0n-en.pdf?expires=1661336048&id=id&accname=guest&checksum=3E3CF32E812FD8A33188BD9AC549A0EF. Accessed 24 August 2022.

Pellegrin J, Colnot L, Delponte L (2021) Research for REGI Committee – Artificial Intelligence and Urban Development. European Parliament, Policy Department for Structural and Cohesion Policies, Brussels. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690882/IPOL_STU(2021)690882_EN.pdf. Accessed 21 December 2021.

Perry LW, Mc Innis B, Price CC, Smith S, Hollywood J (2013) Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. RAND Corporation

Privacy International (2017) Smart Cities. Utopian Vision, Dystopian Reality. https://privacyinternational.org/sites/default/files/2017-12/Smart%20Cities-Utopian%20Vision%2C%20Dystopian%20Reality.pdf. Accessed 1 September 2021.

Research Group of the Office of the Privacy Commission of Canada (2013) Drones in Canada – Will the proliferation of domestic drone use in Canada raise new concerns for privacy?. https://publications.gc.ca/collections/collection_2015/priv/IP54-60-2013-eng.pdf. Accessed 21 June 2022

Solano JL, Martin A, de Souza S, Taylor L (2022) Governing data and artificial intelligence for all. Models for sustainable and just data governance. European Parliamentary Research Service, p. 18. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf. Accessed 1 August 2022.

Van Zeeland DJ, Breuer J, Christofi A, Pierson J (2019) Personal data protection in smart cities: Roundtable report: for Chair 'Data Protection on the Ground'. Brussels.

Veil W (2021) Data altruism: how the EU is screwing up a good idea. Algorithm Watch. https://algorithmwatch.org/de/wp-content/uploads/2022/01/2022_AW_Data_Altruism_final_publish.pdf. Accessed 8 August 2022.

Venice Commission (2015) Report on the democratic oversight of signals intelligence agencies

Online sources

2021/0106(COD) Artificial Intelligence Act, Legislative Observatory. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en. Accessed 9 July 2021

Access Now (2022) Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance. https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf. Accessed 27 June 2022

Ackerman S (2017) TSA screening program risks racial profiling amid shaky science – study. The Guardian. https://www.theguardian.com/us-news/2017/feb/08/tsa-screening-racial-religious-profiling-aclu-study. Accessed 3 July 2021.

Adler L (2016) How Smart City Barcelona Brought the Internet of Things to Life. https://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789. Accessed 3 Aug 2021.

Aldegheri L (2021) Verona, attivati i sensori che rilevano i cellulari per evitare assembramenti in centro. Corriere del Veneto. https://corrieredelveneto.corriere.it/verona/cronaca/21_novembre_02/verona-attivati-sensori-che-rilevano-cellulari-evitare-assembramenti-centro-f31e8952-3be8-11ec-9e44-142d5e884850.shtml. Accessed 7 December 2021.

Bacchi U (2021) Fears raised over facial recognition use at Moscow protests. Reuters. https://www.reuters.com/article/russia-protests-tech-idUSL8N2KA54T. Accessed 28 February 2022.

Badger E (2017) Google's Founders Wanted to Shape a City. Toronto Is Their Chance. New York Times. https://www.nytimes.com/2017/10/18/upshot/taxibots-sensors-and-self-driving-shuttles-a-glimpse-at-an-internet-city-in-toronto.html. Accessed 6 August 2020

Brewster T (2021) Drones With Facial Recognition Are Primed To Fly—But The World Isn't Ready Yet. https://www.forbes.com/sites/thomasbrewster/2021/02/15/drones-with-facial-recognition-are-primed-to-fly-but-the-world-isnt-ready-yet/. Accessed 21 June 2022.

Briodagh K (2019) Smart City IoT Project Launches for New York City DoT. https://www.iotevolutionworld.com/smart-transport/articles/443661-smart-city-iot-project-launches-new-york-city.htm. Accessed 3 Aug 2021

Clearview AI (2020) Privacy Policy. Clearview AI, Inc. https://staticfiles.clearview.ai/privacy_policy.html. Accessed 31 May 2020.

Castro P (2021) Smart Cities Slash Emission. https://www.innovatorsmag.com/smart-cities-slash-emissions/. Accessed 3 Aug 2021.

Chandran R (2019) Use of facial recognition in Delhi rally sparks privacy fears. Reuters. https://www.reuters.com/article/us-india-protests-facialrecognition-trfn/use-of-facial-recognition-in-delhi-rally-sparks-privacy-fears-idUSKBN1YY0PA. Accessed 28 June 2022.

Christofi A, Peeters B (2022) B2G data sharing for smart city development in Europe: a first look at the Data Act Proposal (Part I). CiTiP Blog. https://www.law.kuleuven.be/citip/blog/b2g-data-sharing-for-smart-city-development-in-europe-a-first-look-at-the-data-act-proposal-part-i/. Accessed 8 August 2022.

Cisco (2013) The Internet of Everything. Global Public Sector Economic Analysis. https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf. Accessed 28 February 2022.

Clearview AI, ' EU/UK/Switzerland Deletion Request Form' <https://clearviewai.typeform.com/to/Icakh3> accessed 28 May 2020.

Combs V (2020) IDC names top 10 trends for smart cities in policing, cybersecurity, and high-speed internet connections. https://www.techrepublic.com/article/idc-names-top-10-trends-for-smart-cities-in-policing-cybersecurity-and-high-speed-internet-connections/. Accessed 3 Aug 2021.

Comune di Bari (2020) Drone living lab: Comune, Enac e Distretto tecnologico pugliese firmano protocollo per fare di Bari sede di sperimentazioni di nuove tecnologie. https://www.comune.bari.it/-/drone-living-lab-comune-enac-e-distretto-tecnologico-pugliese-firmano-protocollo-per-fare-di-bari-sede-di-sperimentazioni-di-nuove-tecnologie. Accessed 24 June 2022.

Data Guidance (2017) Ireland: DPC releases statement on use of facial detection technology in advertising. https://www.dataguidance.com/news/ireland-dpc-releases-statement-use-facial-detection-technology-advertising. Accessed 11 December 2021.
D-Cent (Decentralized Citizens Engagement Technologies), see: https://dcentproject.eu/. Accessed: 27 August 2020.

DECODE Official website. https://www.decodeproject.eu/. Accessed 19 August 2022.

DECIDIM Official website. https://www.decidim.barcelona/?locale=ca. Accessed 19 August 2022.

Digital Freedom Fund. https://digitalfreedomfund.org/about/. Accessed 30 May 2022.

Douglas T (2018) What Can We Learn from Atlanta?. Government Technology. https://www.govtech.com/security/What-Can-We-Learn-from-Atlanta.html. Accessed 1 December 2020.

Dragonetti W (2021) (Data) Act 1 of Business to Government data sharing. EUROCITIES. https://eurocities.eu/latest/data-act-1-of-business-to-government-data-sharing/. Accessed 8 August 2022.

EASA (2022) Urban Air Mobility (UAM). https://www.easa.europa.eu/domains/urban-air-mobility-uam. Accessed 22 June 2022.

El País (2021) Mercadona paga una sanción de 2,5 millones de euros a Protección de Datos. https://elpais.com/economia/2021-07-22/mercadona-paga-una-sancion-de-25-millones-de-euros-a-proteccion-de-datos.html?prm=enviar_email. Accessed 28 June 2022.

European Commission (2018a) Smart Cities. https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en. Accessed 3 Aug 2021.

European Commission (2018b) Commission Staff Working Document - Evaluation Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on the Re-Use of Public Sector Information COM(2018) 234 Final - SWD(2018) 129 Final. https://eur-lex.europa.eu/resource.html?uri=cellar:4e790e4c-4969-11e8-be1d-01aa75ed71a1.0001.02/DOC_1&format=PDF. Accessed 19 November 2021

European Commission (2019) Capacity Building for Litigating Cases Relating to Democracy, Rule of Law and Fundamental Rights Violations. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic- details/just-pppa-liti-ag-2018. Accessed 30 May 2022

European Commission (2022a) Data Act & amended rules on the legal protection of databases. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en. Accessed 17 August 2022.

European Commission (2022b) Urban Air Mobility. Smart City Market Place. https://smart-cities-marketplace.ec.europa.eu/action-clusters-and-initiatives/action-clusters/sustainable-urban-mobility/urban-air-mobility-uam. Accessed 21 June 2022.

European Council of the European Union (2022) Council approves Data Governance Act. https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees/. Accessed 28 August 2022.

European Parliament (2021) Artificial Intelligence in policing: safeguards needed against mass surveillance. Press Release. https://www.europarl.europa.eu/news/en/press-room/20210624IPR06917/artificial-intelligence-in-policing-safeguards-needed-against-mass-surveillance. Accessed 30 June 2021.

Evans D (2012) Internet of Everything in Action: Today and Tomorrow #IoE. Cisco. https://blogs.cisco.com/digital/internet-of-everything-in-action. Accessed 21 June 2021.
Fan K (2020) Clearview AI Responds to Cease-and-Desist Letters by Claiming First Amendment Right to Publicly Available Data. JoltDigest. https://jolt.law.harvard.edu/digest/clearview-ai-responds-to-cease-and-desist-letters-by-claiming-first-amendment-right-to-publicly-available-data. Accessed 5 June 2020

Fair Trials (2022) AI Act: EU must ban predictive AI systems in policing and criminal justice. https://www.fairtrials.org/articles/news/ai-act-eu-must-ban-predictive-ai-systems-in-policing-and-criminal-justice/. Accessed 11 August 2022

Federal Commission Communication (2013) In the Matter of Google, [emphasis added]. https://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0416/DA-12-592A1.pdf. Accessed 31 July 2022.

Financial Post (2020) IDEMIA Launches Converged Card to Enable Financial Inclusion with Identity and Payment Card Solution. https://financialpost.com/pmn/press-releases-pmn/business-wire-news-releases-pmn/idemia-launches-converged-card-to-enable-financial-inclusion-with-identity-and-payment-card-solution. Access 29 November 2021

Flying Forward 2020 (2022) Deliverable 6.1. Specification of the UAM Demonstrators. pp. 36 ff. https://www.ff2020.eu/assets/files/ff2020-d-6-1-specification-of-the-uam-demonstrators-v1-0-1.pdf. Accessed 24 June 2022.

Foucault M (1982) Space Knowledge and Power. Interview by Paul Rabinow in *Skyline*. Rizzoli Communications, Inc. https://foucault.info/documents/foucault.spaceKnowledgePower/. Accessed 23 February 2022.

Gallagher R, Jona L (2019) We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive. The Intercept. https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/. Accessed 8 July 2021

Glowacki M (2016) Nudging Cities: Innovating with Behavioral Science. Data-Smart City Solutions. https://datasmart.ash.harvard.edu/news/article/nudging-cities-innovating-with-behavioral-science-833. Accessed 7 June 2022

Glasco J (2019) Barcelona City Profile. Smart City World. https://www.smartcitiesworld.net/opinions/smart-cities-reports/smartcitiesworld-city-profile--barcelona. Accessed 26 August 2020

Graham J (2017) Walmart wants to monitor shoppers' facial expressions. Usa Today. https://eu.usatoday.com/story/money/2017/08/08/walmart-wants-monitor-shoppers-facial-expressions/550671001/. Accessed 28 June 2022.

Goldsmith S (2021) 5 Ways COVID-19 Pushed Digital Services into the Spotlight. https://www.govtech.com/computing/5-ways-covid-19-pushed-digital-services-into-the-spotlight.html. Accessed 3 Aug 2021.

Hardesty L (2013) How Hard Is It to "De-Anonymize" Cellphone Data?. MIT News. https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data. Accessed 7 December 2021.

Hill K (2020) The Secretive Company That Might End Privacy As We Know It. New York Times. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Accessed 4 March 2020.

Hui M (2020) Hong Kong's subway is sending robots to disinfect trains of coronavirus. https://qz.com/1816762/coronavirus-hong-kongs-mtr-subway-uses-robot-to-disinfect-trains/. Accessed 3 Aug 2021.

Hogdson C (2019) AI lie detector developed for airport security. The Financial Times. https://www.ft.com/content/c9997e24-b211-11e9-bec9-fdcab53d6959. Accessed 8 July 2021.

https://landsec.com/policies/privacy-policy/visitors. Accessed 10 December 2021.

Kapadia A (2021) Can Facebook's smart glasses be smart about security and privacy?. The Conversation. https://theconversation.com/can-facebooks-smart-glasses-be-smart-about-security-and-privacy-170002. Accessed 2 March 2022.

Korte A (2020) Facial-Recognition Technology Cannot Read Emotions, Scientists Say. American Association for the Advancement of Science. https://www.aaas.org/news/facial-recognition-technology-cannot-read-emotions-scientists-say. Accessed 8 July 2020.

Kruope A (2020) Moscow's Use of Facial Recognition Technology Challenged. Human Rights Watch. https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged. Accessed 28 February 2022.

Kuang C (2012) In The Cafeteria, Google Gets Healthy. Fast Company. https://www.fastcompany.com/1822516/cafeteria-google-gets-healthy. Accessed 7 June 2022.

Las Naves (2020) Red Ciudadana "Frena la Curva". https://www.lasnaves.com/estrategias-ciudad/red-ciudadana-frena-la-curva/?lang=es. Accessed 3 Aug 2021.

Lohr S (2018) Facial recognition is accurate, if you're a white guy. New York Times. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html. Accessed 25 May 2020.

Luxmoore M (2019) Russian Challenges Use Of Facial-Recognition Technology That Has Facilitated Protest Crackdown. RadioFreeLiberty Radio Europe. https://www.rferl.org/a/russian-challenges-use-of-facial-recognition-technology-that-has-facilitated-protest-crackdown/30204309.html. Accessed 24 March 2022.

MacDonald A (2020) Kenya's Huduma Namba Digital ID Scheme Could Exclude Millions of Citizens, Forum Warns. Biometric Update. https://www.biometricupdate.com/202101/kenyas-huduma-namba-digital-id-scheme-could-exclude-millions-of-citizens-forum-warns. Access 29 November 2021.

Madrigal AC (2012) Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days. https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/. Accessed 21 Oct. 2021.

Malgieri G, Ienca M (2021) The EU regulates AI but forgets to protect our mind. European Law Blog. https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/. Accessed 9 August 2022.

Marshaal A (2019) NYC Now Knows More Than Ever About Your Uber and Lyft Trips. Wired. https://www.wired.com/story/nyc-uber-lyft-ride-hail-data/. Accessed 26 November 2021.

Melendez S (2020) D.C. and NYC built digital COVID-19 portals within days, thanks to this tool. https://www.fastcompany.com/90516276/this-tool-helped-dc-and-nyc-build-digital-covid-19-portals-within-days. Accessed 3 Aug 2021.

McCulloch K (2020) How can drones contribute to a smart city? Overview of their use and their legality in Canada. Dentons. https://www.dentons.com/en/insights/articles/2020/december/1/how-can-drones-contribute-to-a-smart-city. Accessed 21 June 2022.

Mitchell B (2020) Is it possible to trace a MAC address? Lifewire. https://www.lifewire.com/tracing-mac-address-stolen-computer-3971329. Accessed 24 March 2022.

Murgia M (2021) Emotion recognition: can AI detect human feelings from a face?. Financial Times. https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452. Accessed 30 January 2022.

Noorman M, Taylor L (2020) Tada's Blind Spots. https://tada.city/en/nieuws/opinion-tadas-blind-spots/. Accessed 12 October 2020
NWO. https://www.nwo.nl/en/projects/314-99-112-0. Accessed 16 June 2022.

Octoparse (2019) 5 Things You Need to Know Before Scraping Data From Facebook. https://www.octoparse.com/blog/5-things-you-need-to-know-before-scraping-data-from-facebook. Accessed 21 May 2020.

O' Sullivan D (2020) This man says he's stockpiling billions of our photos. CNN Business. https://edition.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html. Accessed 21 May 2020.

Oxford English Dictionary (2022) Expectation. https://www-oed-com.ezproxy.unibo.it/view/Entry/66455?redirectedFrom=expectation#eid. Accessed 5 March 2022.

Papakostantinou V, De Hert P (2021) EU lawmaking in the Artificial Intelligent Age: Act-ification, GDPR Mimesis, and Regulatory Brutality. European Law Blog. https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality/#more-7788. Accessed 8 July 2021.

Peers S (2014) The Domino Effect: How Many EU Treaties Violate the Right to Privacy and Data Protection?. EULawAnalysis. https://eulawanalysis.blogspot.com/2014/11/the-domino-effect-how-many-eu-treaties.html. Last accessed 21 April 2022

Poon L (2021) Automating the War on Noise Pollution. Bloomberg CityLab. https://www.bloomberg.com/news/features/2021-12-02/can-sensor-technology-cut-noise-pollution-in-cities. Accessed 13 December 2021.

Poon L (2018) Sleepy in Songdo, Korea's Smartest City. CityLab. https://www.citylab.com/life/2018/06/sleepy-in-songdo-koreas-smartest-city/561374/. Accessed 3 January 2022

Quividi Privacy Policy. https://quividi.com/%20privacy/. Accessed 10 December 2021.

Rasul I, Hollywood D (2012) Can nudges help to cut household energy consumption?. The Guardian. https://www.theguardian.com/sustainable-business/behaviour-change-energy-consumption. Accessed 7 June 2022.

Reich O (2020) Clearview AI – The Privacy-breaching App That Gives Us the Creeps. EU Liberties. https://www.liberties.eu/en/news/clearview-privacy-busting-app/18762. Accessed 5 March 2020.

Reuters (2020) Alibaba facial recognition tech specifically picks out Uighur minority – report. https://www.reuters.com/article/us-alibaba-surveillance-idUKKBN28R0IR. Accessed 27 June 2022.

Schaklett M (2019) Paris' Beautiful Park Benches Are Also Smart, Thanks to IoT Devices. TechRepublic. https://www.techrepublic.com/article/paris-beautiful-park-benches-are-also-smart-thanks-to-iot-devices/. Accessed 10 August 2020.

Schmit C, Larson NB, Kum HC (2021) Data privacy laws in the US protect profit but prevent sharing data for public good – people want the opposite. https://theconversation.com/data-privacy-laws-in-the-us-protect-

profit-but-prevent-sharing-data-for-public-good-people-want-the-opposite-166320. Accessed 18 November 2021.

Schwartz O (2019) Don't look now: why you should be worried about machines reading your emotions. The Guardian. https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science Accessed 3 July 2021.

Science Daily (2017) Emotions are cognitive, not innate, researchers conclude. https://www.sciencedaily.com/releases/2017/02/170215121100.htm. Accessed 12 July 2021.

Sentilo. https://connecta.bcn.cat/connecta-catalog-web/component/map

SESAR (2022) Demonstrating The Everyday Benefits Of U-Space. https://www.sesarju.eu/U-space_everyday_benefits. Accessed 24 June 2022.
Sharing Cities (2020) Smart Cities Have Responded to Covid-19. https://www.sharingcities.eu/sharingcities/news/Smart-Cities-have-responded-to-COVID-19-WSWE-BQ8JJZ. Accessed 3 Aug 2021.

Sidewalk Labs (2017) Request For Proposals No. 2017-13 Response: Project Vision. https://storage.googleapis.com/sidewalk-toronto-ca/wp-content/uploads/2017/10/13210553/Sidewalk-Labs-Vision-Sections-of-RFP-Submission.pdf. Accessed 11 August 2020.

Smart Citizen Kit initiative. https://www.seeedstudio.com/Smart-Citizen-Kit-p-2864.html. Accessed 13 December 2021.

Soffel J (2013) Rio's "big brother" control room watches over the city. https://edition.cnn.com/2013/08/29/world/americas/rio-big-brother-control-room/index.html. Accessed 3 Aug 2021.

Statista (2021) Estimated size of the global commercial drone market in 2021 with a forecast for 2026. Statista. https://www.statista.com/statistics/878018/global-commercial-drone-market-size/. Accessed 21 June 2022.

Stolton S (2020) After Clearview AI scandal, Commission "in close contact" with EU data authorities. Euractiv. https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/. Accessed 5 March 2020.

Tarantola A (2020) Why Clearview AI is a threat to us all. Endgadget. https://www.engadget.com/2020/02/12/clearview-ai-police-surveillance-explained/. Accessed 5 March 2020.

Swan B (2020) Facial-Recognition Company That Works With Law Enforcement Says Entire Client List Was Stolen DailyBeast. https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen?source=twitter&via=desktop. Accessed 29 May 2020.

Teale C (2020) Knoxville, TN Still Quiet on Details of Cyberattack. Smart Cities Dive. https://www.smartcitiesdive.com/news/knoxville-tn-still-quiet-on-details-of-cyberattack/579753/. Accessed 1 December 2020.

Thomas D (2018) The Cameras that Know if You're Happy – or a Threat. BBC. https://www.bbc.com/news/business-44799239. Accessed 2 July 2021.

US Government Accountability Office (2013) Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities. https://www.gao.gov/products/gao-14-159. Accessed 3 July 2021.

Vincent J (2014) London's bins are tracking your smartphone. *The Independent*. http://www.independent.co.uk/life-style/gadgets-and-tech/news/updated- londons-bins-are-tracking-your-smartphone-8754924.html. Accessed 16 October 2020.

Vogelezang F (2022) A Closer Look at Data Intermediaries and the Risk of Platformization. https://openfuture.eu/blog/a-closer-look-at-data-intermediaries-and-the-risk-of-platformization/. Accessed 8 August 2022.

Vogiatzoglou P, Bergholm J (2020a) Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security – Part 1. CiTiP Blog. https://www.law.kuleuven.be/citip/blog/privacy-international-la-quadrature-du-net-part-1/. Accessed 4 May 2022

Vogiatzoglou P, Bergholm J (2020b) Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security – Part 2. CiTiP Blog. https://www.law.kuleuven.be/citip/blog/privacy-international-la-quadrature-du-net-part-2/. Accessed 4 May 2022

Vogiatzoglou P, Bergholm J (2020c) Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security – Part 3. CiTiP Blog. https://www.law.kuleuven.be/citip/blog/privacy-international-la-quadrature-du-net-part-3/. Accessed 4 May 2022.

Walker S (2016) Face recognition app taking Russia by storm may bring end to public anonymity. The Guardian. https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte. Accessed 2 March 2022.

Whittacker Z (2020) Security Lapse Exposed Clearview AI Source Code. TechCrunch. https://techcrunch.com/2020/04/16/clearview-source-code-lapse/. Accessed 29 May 2020.

Wilding M (2017) The Age of the ASBO: How Britain Became a Police State. Vice. https://www.vice.com/en/article/gy594q/the-age-of-the-asbo-how-britain-became-a-police-state. Accessed 24 February 2022

Wray S (2021) Sidewalk Labs spinout Replica plans expansion to Europe and Asia. https://cities-today.com/sidewalk-labs-spinout-replica-plans-expansion-to-europe-and-asia/. Accessed 3 Aug 2021.

Yalcinkaya G (2017) Piccadilly Circus billboard uses recognition technology to deliver targeted adverts. Dezeen. https://www.dezeen.com/2017/11/10/piccadilly-circus-digital-billboard-screen-targeted-advertisements-algorithm-news-technology/. Accessed 11 December 2021.

Yang Y (2019) Why Hong Kong protesters fear the city's "smart lamp posts". *The Financial Times*. https://www.ft.com/content/f0300b66-30dd-11ea-9703-eea0cae3f0de. Accessed 1 September 2021

Abbreviations

AFR: Automated Facial Recognition

AI: Artificial Intelligence

AIA: Artificial Intelligence Act

AIAs: Algorithmic Impact Assessments

AISs: Algorithmic Impact Statements

AP: Autoriteit Persongegevens

ANPR: Automatic Number Plate Recognition

B2B: Business to Business

B2G: Business to Government

BVLOS: beyond visual line-of-sight

CFREU: Charter of Fundamental Rights of the European Union

CJEU: Court of Justice of the European Union

CNIL: Commission nationale de l'informatique et des libertés

CSLI: Cell-site Location Information

DA: Data Act

DGA: Data Governance Act

DPD: Data Protection Directive

DPIAs: data protection impact assessments

EASA: European Union Aviation Safety Agency

ECHR: European Convention on Human Rights

ECtHR: European Court of Human Rights

EDPB: European Data Protection Board

EDPS: European Data Protection Supervisor

EFR: Emotion Facial Recognition

EHDS: European Health Data Space

EIAs: Environmental Impact Assessments

EIP-SCC: European Innovation Partnership for Smart Cities and Communities

EPA: Environmental Protection Agency

EU: European Union

FBI: Federal Bureau of Investigation

HRESIA Impact Assessments: Human Rights, Ethical and Social Impact Assessments

HTCE: High Tech Campus Eindhoven

G2B: Government to Business

G2G: Government to Government

ICAO: International Civil Aviation Organization

GDPR: General Data Protection Regulation

ICO: Information Commissioner Office

ICTs: Information and Communication Technologies

IoT: Internet of Things

IoE: Internet of Everything

IP: Internet Protocol

IPT: Investigatory Powers Tribunal

ISP: Internet Service Provider

JCAs: Joint Control Agreements

LEAs: Law Enforcement Agencies

LED: Law Enforcement Directive

NWO: Dutch Research Council

PDS: Personal Data Sovereignty

PDT: Public Data Trust

PIAs: Privacy Impact Assessments

PPP: Public-private Partnership

PSID: Public Sector Information Directive

QS: Quantified Self

RFID: Radio Frequency Identification

RIPA: Regulation of Investigatory Powers Act 2000

RPAS: Remotely Piloted Aircraft Systems

SLL: Stratumseind Living Lab

STS: socio-technical systems

SurvIA: Surveillance impact assessments

UAM: urban air mobility

UASs: unmanned aerial systems

UAVs: unmanned aerial vehicles

USSC: United States Supreme Court

UTM: Unmanned Aircraft System Traffic Management

Figures