European Journal of Law and Technology, Vol 12 No.1 (2021)

EJLT European Journal of Law and Technology

Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?

Athena Christofi, Ellen Wauters and Peggy Valcke [1]

Abstract

Smart city initiatives are projects leveraging information technology and data, often in and/or from the public space, to pursue various public interest and economic related objectives. They process vast amounts of data that in many cases are personal data, triggering the application of the relevant legal framework. This paper analyses the application of the lawfulness principle, which is a fundamental principle of data protection law, in the smart city context. It provides a detailed analysis of the relevant legal bases in the General Data Protection Regulation and the Data Protection Law Enforcement Directive. Two key challenges are demonstrated.

Firstly, in terms of public interest processing, the General Data Protection Regulation and the Data Protection Law Enforcement Directive may be insufficient to ensure the lawfulness of processing. Even though both include provisions on legal bases for public interest processing, such provisions require further implementation at the EU or national level. It is therefore important to reflect on additional and foreseeable laws possibly needed to supplement the EU data protection acts and enable smart city development. Secondly, regarding private interest processing, the data protection's harmonisation objective may be eroded when diverging national practices emerge as a result of regulators' desire to offer citizens increased protection in public spaces.

Keywords: Smart Cities; Data Protection; Lawfulness Principle; Legal Basis

[1] KU Leuven Centre for IT & IP Law. This research was supported by the Research Association Flanders [SPECTRE project- FWO reference number S006318N].

1. Introduction

'Smart cities' is an umbrella-term and buzzword denoting an abstract, yet very real, phenomenon: the digitalisation and computation of the urban environment. This occurs at different paces in cities and towns all over the world through the gradual emergence of smart city initiatives. These initiatives are projects leveraging information technology and data, often in/and/or from public spaces, which pursue public interest and economic-related objectives as diverse as security, environmental protection, optimised public service delivery, as well as increased advertising revenues.

Interest in smart cities by policymakers and researchers has increased over the past decade.[2] It has become evident that as smart city initiatives proliferate, they can contribute to the realisation of not only public interest objectives and a thriving digital economy, but also complex issues in terms of protection of individual rights and societal interests that need to be carefully balanced with the perceived benefits.[3] While European data protection law provides a legal infrastructure that can support such balancing, there is limited legal literature examining its application in smart cities.[4]

---

[2] Smart city strategies coupled with significant government funding and support mechanisms are prevalent in developed and developing nations. In the United States, the Obama Administration announced in 2015 a smart cities initiative that foresaw the investment of over $160 million in research to support cities and towns solve key challenges, such as crime and traffic congestion; see: The White House Office of the Press Secretary, 'FACT SHEET: Administration Announces New 'Smart Cities' Initiative to Help Communities Tackle Local Challenges and Improve City Services' 14 September 2015 <https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help>. The same year, India launched its 100 Smart Cities Mission committing approximately US$6.7 billion for the development of (new) smart cities and the retrofitting of existing ones into 'smart'; see: Government of India, 'Smart Cities Mission' <http://smartcities.gov.in/content/>. In the European Union, in addition to smart city plans adopted in individual countries (e.g. the Netherlands, Spain, Germany), incentive mechanisms also exist at supra-national level (e.g. the European innovation partnership on smart cities and communities, and funding through the Horizon research and innovation program). The smart city has also been a popular area of research; see: Gupta, P, Chauhan, S and Jaiswal, MP (2019) 'Classification of Smart City Research - a Descriptive Literature Review and Future Research Agenda', 21 Information Systems Frontiers 661.

[3] On fundamental rights and ethical challenges raised by smart city initiatives see, e.g.: Finch, K and Tene, O (2014) 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town', 41 Fordham Urban Law Journal 1581; Ranchordás, S (2020) 'Nudging citizens through technology in smart cities', 34(3) International Review of Law, Computers & Technology 254; Privacy International, 'Smart cities: Utopian vision, dystopian reality' (2017), <https://privacyinternational.org/report/638/smart-cities-utopian-vision-dystopian-reality>; Kitchin, R (2014) 'The real-time city? Big data and smart urbanism', 79 GeoJournal 1.

[4] Research pieces focusing on EU data protection law and smart cities notably include: Edwards, L (2016) 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective', 2 European Data Protection Law Review 18; Dalla Corte, L (2020) Safeguarding data protection in an open data word: On the idea of balancing open data and data protection in the development of the smart city environment, (Doctoral dissertation Tilburg University), <https://research.tilburguniversity.edu/en/publications/safeguarding-data-protection-in-an-open-data-world-on-the-idea-of>; von Grafenstein, M (2020) 'How to build data-driven innovation projects

The relevance of data protection law for smart cities cannot be overstated. Smart city initiatives process vast amounts of data that in many cases are personal data, [5] triggering the application of the relevant legal framework. To advance the legal literature on smart cities and EU data protection law, this article analyses the application of the lawfulness principle in the smart city context. Lawfulness is a fundamental principle enshrined in both, Article 8 of the EU Charter of Fundamental Rights (hereinafter Charter) and secondary law. It requires the existence of a legal basis to ground any processing of personal data. Simply put, processing can be lawful only insofar it is legitimised by the data subjects' consent or another legitimate ground provided in data protection law.

EU secondary law exhaustively lists the available legal bases. As the General Data Protection Regulation (hereinafter GDPR) includes six possible legal bases, some of which have a potentially broad scope of application, whereby the lawfulness of the processing may often be assumed to be fulfilled. However, we consider that such an assumption can be challenged and that discussions on lawfulness should be more prominent in smart city research and practice. Our paper provides a detailed analysis of the legal bases deemed most relevant for smart city projects, unravelling the challenges that emerge when seeking to operationalise them. It argues that important *'grey areas'* exist when it comes to the lawfulness of personal data processing in a smart city context (i.e. smart city processing). This can impact the development of smart city initiatives in a climate of legal certainty and citizen trust. The analysis is based on doctrinal research relying on legislation –in particular the GDPR and its predecessor,[6] as well as the Data Protection Law Enforcement Directive (i.e. LED). It also relies on case-law from the Court of Justice of the EU (hereinafter CJEU) and the European Court of Human Rights (i.e. ECtHR), opinions and guidelines issued by relevant data protection authorities, as well as literature.

The paper is structured as follows. Section 2 briefly introduces the data protection's lawfulness principle and identifies the legal bases that are most pertinent for smart city processing by extracting certain key characteristics of such processing. These legal bases are then investigated in more detail in the ensuing sections. Section 3 assesses the responsibilities and balancing mechanisms behind the *'public task'* and *'legitimate interests'* legal bases, as well as the public interest related conditions that permit the processing of sensitive personal data. Section 4 attempts to explain the differences in the operationalisation of the lawfulness principle depending on the public or private nature of

---

at large with data protection by design: A scientific-legal Data Protection Impact Assessment with respect to a hypothetical Smart City scenario in Berlin', HIIG Discussion Paper Series, 2020(3).

[5] The definition of *'personal data'* in EU law is particularly broad as it covers any information relating to an identified or identifiable natural person (Article 4(1) General Data Protection Regulation). With the proliferation of data and progresses in data analytics it has been argued that technology is moving towards perfect identifiability of information, meaning that in smart environments any information is likely to relate to a person and thereby fall under the definition of personal data. See: Purtova, N (2018) 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law', 10 Law, Innovation and Technology 40.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281 (no longer in force).

the interest served by the processing. It argues that they are a consequence of the recognition of data protection as a fundamental right. It also reflects on the challenge of ensuring legitimacy and legal certainty when it comes to smart city processing. The particularities and challenges associated with law enforcement-related processing are outlined in Section 5. Section 6 concludes, by acknowledging that, even though the lawfulness principle makes a distinction between public and private interests and actors, it is difficult to ascertain this distinction in practice due to the blurring lines between public and private in smart cities.

2. The lawfulness principle in the smart city context

As mentioned in the introduction, the lawfulness principle is concerned with the legitimacy of processing.[7] Such legitimacy stems from the decision of the individual to agree to the processing, which is embodied in the concept of consent, or due to legitimate reasons that may justify personal data processing.

The EU secondary legal framework reflects this approach. The GDPR, after proclaiming in Article 5(1) that personal data shall be *'processed lawfully, fairly and in a transparent manner in relation to the data subject'*, lists in Article 6 six legal bases that can ground a processing operation. For processing to be lawful, one of these legal bases must be identified and validly applied. In addition to consent, the GDPR also includes as legal bases: contractual necessity; compliance with a legal obligation; the protection of the vital interests of the data subject; performance of a task carried out in the public interest; and the legitimate interests pursued by the controller or by a third party. A requirement that personal data processing must be *'necessary'* in relation to the pursued interest is included in most legal bases.

It is also important to consider the different legitimacy considerations behind each legal basis. For instance, regarding consent, legitimacy derives from the ability of the individual to freely consent to the processing. In terms of legal obligation and contractual necessity there is a need to ensure respect and effective application of laws and contracts. Moreover, public task and legitimate interests also entail that there can be public or private interests, which may legitimise the processing. Legitimacy considerations also justify a stricter understanding of the lawfulness principle for the processing of sensitive data. Such processing is prohibited, unless one of the exceptions provided in Article 9(2) applies and one of the legal bases of Article 6 is satisfied.[8]

As regards law enforcement-related processing, while the LED recognises the lawfulness principle,[9] the legal bases that operationalise it are different to those included in the

[7] Lynskey, O (2015), The Foundations of EU Data Protection Law (Oxford: Oxford University Press), 31-34.
[8] Georgieva, L and Kuner, C (2020), 'Article 9. Processing of special categories of personal data' in Kuner, Bygrave and Docksey (eds) The EU General Data Protection Regulation (GDPR): A Commentary (Oxford: Oxford University Press), 376-377.
[9] Article 4(1)(a) LED.

GDPR. This is hardly surprising as consent, contractual necessity and broad public or private legitimate interests are irrelevant in a law enforcement context. In those cases, the processing would only be lawful if it is necessary for the performance of a task carried out by a competent authority for the purposes of the Directive and based on Union or Member State law.[10]

While it is for the controller to decide on the applicable legal basis, its choice is determined by the characteristics of the case and legitimacy considerations underlying the different legal bases. For example, does the processing fall under legislation on general or law enforcement-related processing? Is the individual in a position to give meaningful consent? Does the processing serve public or private interests? Does it entail personal or sensitive personal data? Does it bring high risks to the rights of individuals, which may question its necessity and call for alternative, less intrusive means to achieve its said aims? All these are questions that should be answered by data controllers. Transposing these considerations into the smart city context, we have identified the legal bases that, in our view, are most relevant for smart city development.

Smart city initiatives can differ considerably in terms of the interests being sought, the actor(s) behind them and the position of the data subject – these are some of the reasons that make smart cities exceptionally difficult to define. Despite such diversity though, smart city projects have some general characteristics that are rather common.

First, data collection technologies are often deployed in public spaces. By embedding sensors, cameras and other smart devices in urban public spaces, smart city projects essentially tie the use of public spaces to the collection and processing of personal information about citizens.[11]

Second, projects are usually driven by local authorities and such projects have a *'paternalistic'* mission, pursuing utility objectives such as, *'smarter urban transport networks'*, *'upgraded water supply and waste disposal facilities'*, *'a more interactive and responsive city administration'*, and *'safer public spaces'*.[12] When city services become smart, important power imbalances may arise between city dwellers and local authorities as data controllers. This is because the former is dependent on the latter to access services.

Third, in addition to municipality-driven projects, we are witnessing smart city initiatives, which pursue private-commercial objectives and do not have any kind of link with city authorities. For example, smart billboards in public or semi-public spaces. These types of initiatives are also pertinent to consider because they are part of the increased scrutiny under which urban dwellers find themselves in the modern city.

---

[10] Article 8(1) LED.

[11] Edwards, L (2016) 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective', 2 European Data Protection Law Review 18; Finch, K and Tene, O (2014) 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town', 41 Fordham Urban Law Journal 1581.

[12] European Commission, Smart Cities <https://ec.europa.eu/info/eu-regional-and-urbandevelopment/topics/cities-and-urban-development/city-initiatives/smart-cities_en.> (accessed 28 August 2020).

Finally, with the advent of facial detection and recognition technologies, biometric-based smart city projects are increasingly popular.

All the above characteristics influence the lawfulness principle's application. There is not much scope for free choice, which is one of the main elements of the notion of consent in the smart city environment.[13] The smart city thus provides an excellent opportunity to shift the focus away from consent to legal bases that place responsibility on the controller rather than the data subject. As will be discussed below, these legal bases include: public task; legitimate interests; legal grounds enabling the processing of sensitive data; and legal bases for law enforcement-related processing.

3. Legal bases for general processing

3.1 Public task

Article 6(1)(e) GDPR enables processing *'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.'* This legal basis is pertinent in the smart city context as many projects have public interest related objectives. Although the provision has a particularly broad scope of application, there are two constraints on its validity regarding smart city processing: firstly, the processing must be *'necessary'*; and secondly, it must also have a basis in EU or national law.

3.1.1 The requirement for processing to be 'necessary'

A requirement that personal data processing must be *'necessary'* is included in all legal bases in Article 6(1), except for consent. Even though the GDPR does not specify what is to be understood by necessary, CJEU case-law on Directive 95/46/EC –which similarly featured necessity in its provisions on legal bases- provides useful insights. In Huber, a judgment that concerned the *'public task'* legal basis, necessity was understood as *'the need for an inextricable link between the purpose and the processing operation'*. In other words, *'a purpose cannot be effectively achieved without the respective processing'*.[14] Applying this to the facts of the case, the Court held that processing could be deemed necessary if it contributed to the more effective application of legislation on EU citizens' rights of residence, which was at stake.[15]

This suggests that processing is legitimate not only if it is necessary for an entity to perform its public interest tasks, but also if it allows it to perform such tasks more effectively. Under this lens, necessity in the context of the *'public task'* legal basis could be particularly far-reaching, because personal data and processing technologies could be invoked as a means to optimise practically everything. Critical smart city literature has noted that smart city

[13] Article 4(11) GDPR.
[14] Clifford, D and Ausloos, J (2018), 'Data Protection and the Role of Fairness', Yearbook of European vol. 37, 21.
[15] Judgment in Heinz Huber v Bundesrepublik Deutschland, C-524/06 ECLI:EU:C:2008:724, para. 62.

projects often deploy vague and promise-style language,[16] with a *'presumption that all aspects of city functioning and life can be mediated or treated or optimized'* through data and technological solutions.[17]

It could be argued that the exercise of cities' planning missions would be more effective were they able to process more than *'basic'* data allowing them to know and predict how people move across the city. To what extent should beliefs in effectiveness and optimisation legitimize the extensive use of data processing technologies in urban spaces? If it is understood so broadly as in the Huber case, necessity would hardly be a constraint to the processing.

Yet, Huber was decided in 2008, and since then there has been a stricter interpretation of necessity by EU data protection authorities. The latter view it as demanding more than a causal link between the processing and the pursued objective. This entails a test similar to the one implied in the application of the *'necessity'* requirement under Article 52(1) of the Charter. In other words, necessity is not only a requirement under Article 6(1) of the GDPR. It is also one of the conditions listed in Article 52(1) of the Charter that may legitimise limitations on fundamental rights: limitations must, among other things, *'be necessary and genuinely meet objectives of general interest […]'*.

Case-law on Article 52(1) Charter understands necessity strictly. It calls for the legislator to choose, among several appropriate measures to achieve a given objective, one that is the least intrusive on fundamental rights.[18] The European Data Protection Supervisor, specifically referring to the fundamental right to data protection follows a similar approach. Limitations of the right are necessary under Article 52(1) of the Charter if, after a detailed consideration of the objective of a measure limiting the right, the regulators explore alternative measures that are *'real, sufficiently and comparably effective in terms of the problem to be addressed'* and then choose the least intrusive one.[19]

Guidelines issued by European data protection authorities suggest that in fact, there is convergence between the two necessity tests. Concerning the *'legitimate interests'* legal basis, Article 29 Working Party (WP29) argued that when determining the necessity of the processing the controller should consider *'whether other less invasive means are available to serve the same end'*.[20] Guidelines on video surveillance go even more in-depth to illustrate how necessity, mandating the choice of the least intrusive means should be assessed for each aspect of a processing operation: from '*when'* and '*where'* it is necessary

[16] Greenfield, A (2013), Against the smart city (New York: Amazon Media - Kindle edition).
[17] Kitchin, R and Cardullo, P (2019) 'Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused' smart cities in Europe', 37(5) EPC: Politics and Space 813, 821.
[18] Judgment in Digital Rights Ireland, C-293/12 and C-594/12 ECLI:EU:C:2014:238; Judgment in Tele2 Sverige AB, Joined Cases C-203/15 and C-698/15 ECLI:EU:C:2016:970.
[19] EDPS (2017), 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.>.
[20] WP29 (2014), 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', WP 217, 49.

to deploy a surveillance measure to '*how*' it is necessary to preserve evidence.[21] For smart city initiatives this stricter understanding of necessity requires controllers to at least specifically define the processing's objectives, properly reflect on alternative measures and be able to justify why, considering these factors, processing may be necessary.

3.1.2 The Requirement for a further legal basis in EU or national Law

An optional or mandatory obligation?

In addition to ascertaining *'necessity',* controllers relying on the public task or legal obligation legal bases should also demonstrate that the processing has a basis in EU or national law. This requirement provides, for legal bases that largely concern public authorities and interests, an additional layer of legality and more possibilities for oversight and holding public authorities accountable.[22]

How this requirement is to be understood is not imminently clear from the text of Article 6 GDPR. After enumerating the six legal bases in points (a) to (f) of paragraph (1), paragraph (2) provides that Member States *'may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) ['legal obligation'] and (e) ['public task'] of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing [...]'*. The use of *'may'* suggests that more specific legal rules to operationalise those legal bases are optional. Yet, paragraph (3) provides that the basis for legal obligation and public task processing *'shall'* be laid down by EU or Member State law to which the controller is subject.

Paragraph (3) suggests that *'legal obligation'* and *'public task'* are not self-standing provisions: they necessitate other EU or national measures to act as further or additional legal bases. Certain requirements regarding the aim and content of the further legal bases are already provided for in the provision. They must meet a public interest objective and be proportionate. Moreover, they must also determine the purpose of the processing, or, for the *'public task'* legal basis, the processing shall be necessary for the performance of the public interest task at stake. Then, paragraph (3) provides suggestions as to how those further legal bases could be made more specific: they may contain specific provisions on, for example, the types of personal data to be processed, the categories of affected data subjects, and the data storage periods.

The need for additional legal bases to ground the processing is not limited to Article 6(3). It accompanies several provisions related to public interest processing. The GDPR is nevertheless not always consistent in terms of the requirements that additional legal bases should meet. This is illustrated in Figure 1 below.

---

[21] EDPB (2020), 'Guidelines 3/2019 on processing of personal data through video devices' Version 2.0 Adopted on 29 January 2020, 10-11.

[22] Butler, O (2018) 'Obligations imposed on private parties by the GDPR and the UK Data Protection Law: Blurring the public-private divide', 24(3) European Public Law 555, 559.

Article	Subject matter	Criteria for additional legal basis – Mentioning of:		
		Respect of essence of the right to DP	**Necessity and/or proportionality**	**Suitable and specific safeguards**
6(4)	Exception from the purpose limitation principle for processing based on a Union or Member State law that aims to safeguard the (public interest related) objectives listed in Art. 23(1).	No	Yes	No
9(2)(g)	Exception from the prohibition to process sensitive data where processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law.	Yes	Yes	Yes
9(2)(i)	Exception from the prohibition to process sensitive data where processing is necessary for reasons of public interest in the area of public health, on the basis of Union or Member State law.	No	No	Yes
9(2)(j)	Exception from the prohibition to process sensitive data where processing is necessary for archiving purposes in the public interest, scientific or historical	Yes	Yes	Yes

	research purposes or statistical purposes, on the basis of Union or Member State law.			
23	Possibility for the EU or national legislators to restrict *by way of a legislative measure* the scope of certain rights and obligations found in the GDPR where such restriction serves public interest related objectives listed in Art. 23(1).	Yes	Yes	Yes

Figure 1 Provisions requiring additional legal bases in EU or Member State law.

In the provisions listed in Figure 1, the additional legal bases seemingly aim to legitimise derogations to otherwise essential principles of the Regulation, such as the purpose limitation principle or the prohibition of sensitive data processing. Therefore, conceptually, their role is not necessarily identical to the role additional bases may play in the context of Article 6(3). At the same time, the broad formulation, and lack of consistency on the requirements that additional bases should meet in the GDPR, beg important questions on the application of the *'public task'* legal basis. What type(s) of laws are required to legitimise smart city processing under public task? And what should the content of such laws be, especially regarding the delineation of the permitted processing activities?

Requirements for additional legal bases and foreseeability in the smart city

Some insights on the additional legal bases needed in the context of *'public task'* can be found in recitals of the GDPR and guidelines from data protection authorities. For instance, Recital 45 clarifies that one law may be sufficient as a basis for several processing operations. ICO, the United Kingdom's Information Commissioner, considers that no specific legal authority is needed for the particular processing activity, and that what needs to have a sufficiently clear basis in law is the public interest task to be exercised by the entity concerned.[23]

[23] ICO, 'Lawful basis for processing: Public task' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/>. It should be noted that in her commentary on Article 6 GDPR, Waltraut Kotschy seems to share a similar position explaining that *the 'assignment of task [...] will often not result in precisely determined obligations for the controller but rather in a more general authorisation to act as necessary in order to fulfil the task'*. See: Kotschy, W (2020), 'Article 6. Lawfulness of Processing' in Kuner, Bygrave and Docksey (eds) The EU General Data Protection Regulation (GDPR): A Commentary (Oxford: Oxford University Press), 336.

Prior to the adoption of the GDPR, WP29 considered that (general) laws would typically attribute the official authority or public task but *'if the processing implies an invasion of privacy or if this is otherwise required under national law to ensure the protection of the individuals concerned, the legal basis should be specific and precise enough in framing the kind of data processing that may be allowed*'.[24]

Basing *'public task'* processing on broad additional legal bases does not sit comfortably with what is provided in Recital 41, and how the conditions on limitations of fundamental rights are generally understood. According to Recital 41:

'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 [CJEU] and the European Court of Human Rights'.

This recital does not distinguish between the requirement for additional legal basis for *'public task'* under Article 6(3), and the other GDPR provisions listed in Figure 1 above. Clarity, precision and foreseeability are seemingly pertinent whenever the GDPR refers to the need for legal basis in further law. Importantly, the case-law of the CJEU and of the ECtHR is explicitly mentioned and is, therefore, the *'point of reference'* when it comes to how clarity and foreseeability should be understood.

It is sufficiently clear from Recital 41 that when referring to (additional) legal bases the GDPR does not mandate parliament acts, as it is for the legal order of the Member States to establish what may constitute a legal measure. This flexibility in the type(s) of measures allowed is aligned with how ECtHR case-law applies the requirement that limitations on fundamental rights must be *'in accordance with the law*'.[25] The caveat that emerged is that they should be accessible to the citizen, meaning that measures that are not published or otherwise made known cannot be regarded as *'law*'.[26]

---

[24] WP29 (2014) 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', WP 217, 22.

[25] ECtHR frequently examines the *'in accordance with the law'* requirement. As regards the CJEU, Peers and Prechal have noted in their commentary on Article 52(1) of the Charter that *'the Court has not made any specific reference to the 'provided for by law' requirement in a large number of the cases where it has applied Article 52(1) expressly or implicitly*', explaining, however, that it was clear in those cases that the *'the limitations on the relevant Charter rights were indeed set out in some national or EU law*'. Peers, S and Prechal, S (2014), 'Scope and Interpretation of Rights and Principles' in Peers, S, Hervey, T, Kenner, J and Ward, A (eds), The EU Charter of Fundamental Rights: A Commentary (London: Hart Publishing) 1455, 1470.

[26] Publication does not necessarily need to be at an official publication in the legal journal of a State, since some orders, in particular of technical nature, may not be subject to such publication. In Zakharov v Russia, the ECtHR considered that the fact that the measure had been published in a specialised magazine, and made available in an online legal database, was enough to meet the accessibility requirement. See: Judgment in Roman Zakharov v. Russia (ECtHR) Application no. 47143/06, paras. 180, 181, 239-242. The importance of accessibility was also affirmed by the CJEU in

The demands for clarity, precision and foreseeability in the legal bases are arguably more complex to unfold. They relate to the *'quality of the law'* requirement developed by the ECtHR as an intrinsic part of the assessment of whether or not a measure is *'in accordance with the law'*. To be clear and foreseeable, laws must state with sufficient clarity, the scope and manner of exercise of discretion of public authorities so that their effects are foreseeable to the citizen. De Hert and Malgieri provide an in-depth analysis of foreseeability in the context of ECtHR's case-law on Article 8 ECHR (right to privacy) about surveillance measures.[27] They explain that in Huvig[28] the Court established rather detailed criteria on foreseeability that to date, still guide judges.[29]

According to such criteria, foreseeability entails, among other things, that laws specify the categories of people liable to be monitored, the nature of the offenses that may trigger surveillance, the limits placed on the duration of the processing and the circumstances in which data needs to be erased or destroyed. The authors' analysis further reveals that where the ECtHR considered surveillance measures to be less severe, thus interferences with the right to privacy being less serious, the Court set a lower threshold for foreseeability. This threshold still required some specifications to be included in the laws, at least on the grounds needed for ordering surveillance measures and their duration.[30] Ultimately the Court has developed an *'impact-related rule'*, whereby the deeper the interference with privacy, the stricter the criteria on foreseeability need to be.[31]

The above case-law concerned surveillance in the context of policing and security. The surveillance that smart city initiatives falling under the rules on general processing entail is admittedly different. The aim is to render urban spaces sentient, that is, enabling a data-driven and networked form of urbanism where data and algorithms dynamically shape and control how city systems work.[32] Often the interest is not in identifying and targeting

---

the Bara case. Bara concerned the transfer of the applicants' income data, from the tax administration authority to the national health insurance fund, both of which were public authorities. The transfer happened without the knowledge of the applicants, in violation of their right to be informed about the recipients of their data and about the fact they had the right to access their data. The CJEU held that restrictions on data subjects' rights could only be imposed by legislative measures. The contentious transfer was in fact based on a protocol agreed between the authorities, which was not subject to official publication. The requirement for *'law'* was thus not met. See: Judgment in Smaranda Bara and Others, Case C-201/14 ECLI:EU:C:2015:638, paras. 39-41.

[27] De Hert, P and Malgieri, G (2020) 'Article 8 ECHR compliant and foreseeable surveillance: The ECHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law', Brussels Privacy Hub Working Paper Vol. 6 No. 21.

[28] Judgment in Huvig v. France (ECtHR) Application no. 11105/84.

[29] De Hert, P and Malgieri, G (2020) 'Article 8 ECHR compliant and foreseeable surveillance: The ECHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law', Brussels Privacy Hub Working Paper Vol. 6 No. 21, 9.

[30] De Hert and Malgieri, 'Article 8 ECHR compliant and foreseeable surveillance: The ECHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law', 11.

[31] De Hert and Malgieri, 'Article 8 ECHR compliant and foreseeable surveillance: The ECHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law', 16-17.

[32] Kitchin, R (2015) 'Data-driven, networked urbanism', The Programmable City Working Paper 14, 2.

specific persons, but *'on the management and nudging of individuals conceived as a multiplicity –a combination of the environment, persons and all of their interactions'*.[33]

These practices, enabled by the processing of vast amounts of data, are nevertheless not without risks on the fundamental rights of city dwellers. For instance, several projects concern location data, which as studies have shown, are particularly difficult to anonymise,[34] and allow to infer information on a person's behaviours, habits, and lifestyles – information that the right to privacy seeks to protect. Moreover, projects aiming to nudge citizens towards certain responsible behaviours may impact individual autonomy.[35]

Considering the above, one must thus wonder whether broad legal authorisations linked to the tasks of local authorities are enough to legitimise smart city processing. Challenges mainly concern foreseeability and the (in)ability to curtail the discretion of local authorities solely on the basis of general laws. In other words, when it comes to public authorities with clearly delineated tasks, it may be reasonably clear, based on their mandate, that they (are entitled to) process personal data to perform such tasks. But local authorities' tasks are normally wide encompassing. Under Belgian law, for instance, their powers cover everything that is in the *'communal interest'*, a notion that has not been defined nor are the municipal powers listed somewhere.[36] The potentially risky nature of smart city processing should also be stressed.

The ECtHR employs an impact-related rule that mandates greater foreseeability where impacts on privacy are serious. In the context of the GDPR, which aims to protect the fundamental rights and freedoms of natural persons, in particular the right to the protection of personal data[37] the notion of *'risk'* arguably has a similar role in triggering enhanced obligations where processing is likely to result in a *'high risk'* to the rights and freedoms.[38] Examples of *'high risk'* include: the systematic monitoring of areas accessible to the public; the use of automated decision making with legal or similar significant effects; data processed on a large scale; the matching or combining of different datasets and the

[33] Galič, M and Gellert, R (2021) 'Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab', 40 Computer Law & Security Review, 12.
[34] De Montjoye, YA, Hidalgo, C, Verleysen, M and Blondel, V (2013) 'Unique in the crowd: The privacy bounds of human mobility', 3 Scientific Reports.
[35] Ranchordás, S (2020) 'Nudging citizens through technology in smart cities', 34(3) International Review of Law, Computers & Technology, 14-15.
[36] However, in practice, matters of municipal interest are understood to mean: all matters that are clearly local and territorial, up to and including the municipality, have a limited character and were not assigned by the legislator to the decision-making rights of other authorities. See: Van den Eeckhout, P (2017), 'Hoofdstuk 3. De gemeenten en de lokale openbare instellingen' in Van den Eeckhout, P & Vanthemsche, G (eds) Bronnen voor de studie van het hedendaagse België, 19e-21e eeuw (Brussel: Koninklijke Commissie voor Geschiedenis), 34.
[37] Article 1(2) and Recital 4 GDPR.
[38] E.g. the obligation to conduct a Data Protection Impact Assessment.

innovative use or application of new technological solutions.[39] These examples are often relevant in the smart city. The foreseeability criterion would call for such high risks to be considered and specified in the additional legal basis.

In the smart city context, a broad legal basis simply grounding the public interest task would not only fail to sufficiently curtail the discretion of public authorities to process personal data, but also fall short of providing a clear understanding of the effects of the processing. Foreseeability in the smart city could entail that the specifications the additional legal basis may have as per Article 6(3) indeed ought to be included in the law.

3.2 Legitimate interests

The *'legitimate interests'* legal basis is arguably more flexible in a smart city context as its valid application does not depend on the existence of additional legal bases. Indeed, according to Article 6(1)(f) GDPR, processing shall be lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where the rights and freedoms of the data subject override such legitimate interests.

3.2.1 Legitimate interests and public authorities

For smart city processing, which pursues a public interest and considering the challenges associated with the *'public task'* legal basis, a relevant question is the extent to which local authorities could rely on *'legitimate interests'*, as a more flexible legal basis. Article 6(1) of the GDPR seems to limit this possibility by providing that the legitimate interests legal basis *'shall not apply to processing carried out by public authorities in the performance of their tasks'*. This limitation is linked to the need for additional legal bases for processing based on a *'public task'*. As it is for the legislator to set by law the legal basis for public authorities to process personal data, the *'legitimate interests'* legal basis that entrusts the determination of the interest at stake and the ensuing balancing exercise to the individual controller, should not apply.[40] However, it concerns processing that public authorities carry out in the performance of their tasks. Therefore, it is arguable that the formulation leaves some scope to use the legal basis for processing that falls outside such performance. What would need to be ascertained on a case-by-case basis is to what extent the processing's purpose and interest pursued is linked to the performance of an authority's public functions as attributed to it by law.

The context around a smart city initiative, in particular the actors involved, its objectives and stage of development may influence this assessment. Projects developed by research consortia comprising cities and other entities, which aim to develop or test new technologies may be a case in point. In a research context, it could be argued that *'legitimate interests'* could be used even for processing involving local authorities as

[39] See: Recital 91 GDPR and in addition, WP29 (2017) 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' WP 248 rev.01, 8-10.
[40] Recital 47 GDPR.

controllers or co-controllers, because processing serving a research interest would not normally fall under local authorities' public functions as set out in law. Some data protection authorities maintain that for public authorities, the performance of tasks relates to their substantive tasks, that is, tasks relating to the purposes for which those authorities have been established.[41]

At the same time, research – even where this is understood broadly, as entailing the development, testing and piloting of new technologies - is only a pre-step towards smart city development. Projects should ultimately get out of the pilot and proof of concept phase, scale up and realise their potential, achieving their public interest related objectives. Yet, as these projects move away from *'experimentation'* towards using technology to improve city governance and public services - which are municipalities' public missions - local authorities reach the limits of the *'legitimate interests'* legal basis. To put differently, *'public task'* is indeed more appropriate.

3.2.2 Legitimate interests and smart city processing serving private interests

Citizens' exposure to data processing technologies deployed in the urban environment does not only result from projects oriented towards the public interest. Video surveillance and other technologies enabling the tracking of passers-by movements and behaviour, or recognising basic demographic characteristics, and even their emotions, are used in public and semi-public spaces[42] by private entities in the pursuit of private interests. Considering the difficulty of relying on consent in public spaces, we discuss whether the *'legitimate interests'* legal basis can legitimise the processing.

3.2.3 The balancing test

The *'legitimate interests'* legal basis involves a three-step test: a legitimate interest must be determined; the necessity of the processing must be established; and the legitimate interest must be juxtaposed with the rights and interests of the data subjects to determine whether the latter override the interest of the controller or the third party.[43] It is for the controller to conduct this test and decide on the outcome of the balancing exercise in the specific situation at stake. In the following paragraphs we illustrate some challenges that

[41] See: Ireland's Data Protection Commission, 'Guidance Note: Legal Bases for Processing Personal Data' December 2019, 21. ICO, the UK's Data Protection Authority, expressed a similar position albeit in the context of re-use of public sector information. According to it, *'Public task' means [the public authority's] core role and functions, as defined in legislation or established through custom and practice'*. See: ICO, 'Guide to RPSI/ What is re-use of public sector information?' <https://ico.org.uk/for-organisations/guide-to-rpsi/what-is-rpsi>.

[42] We understand *'public spaces'* as spaces that are generally open and accessible to individuals and that have a particular political and social significance. *'Semi-public spaces'* are then spaces that are accessible to the public, but may be at the hands of private owners – business districts and malls would be examples.

[43] Kamara, I and De Hert, P (2018) 'Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach', Brussels Privacy Hub Working Paper Vol. 4 No. 12, 11-14.

arise in the smart city context when it comes to operationalising the test, using the example of smart billboards in public and semi-public spaces.

Billboards - those conventional advertising tools we are so accustomed to in cities - can nowadays be equipped with technologies that allow marketers to better understand their audience and optimise the message to be delivered. For instance, there have been efforts to equip billboards with Wi-Fi metering boxes that capture the addresses of mobile phones with an activated Wi-Fi functionality in the immediate environment. This allows to measure the number of people who have daily contact with the advertisement, repetition rates and mobility patterns in a certain area.[44]

Taken together, this information enables companies to optimise the sale and price of advertising space. Moreover, these billboards may also have cameras and software which, using face detection technologies, can recognise the gender, age and even emotions of the passers-by to serve them with the *'correct'*, most engaging ad.[45] Whether or not these technologies process personal data is a contentious issue because of the *'ephemeral'*[46] or *'transient'*[47] nature of the processing. Yet, an argument can be made that even for a short period of time those systems involve personal data processing, and therefore the processing needs a legal basis.[48]

The identification of a legitimate interest to process data poses no difficulty. Marketing, marketing research, advertising and advertising optimisation can all constitute a legitimate

---

[44] CNIL (2015) '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/>.

[45] For a detailed analysis of the phenomenon and issues raised by 'emotiveillance' in public spaces, see: McStay, A (2016) 'Empathetic media and advertising: industry, policy, legal and citizen perspectives (the case for intimacy)', Big Data & Society; McStay, A and Urquhart, L (2019) ''This time with feeling?' Assessing EU data governance implications of out of home appraisal based emotional AI', 24 First Monday 10 <https://doi.org/10.5210/fm.v24i10.9457>. For further reflections on the use of so-called emotional AI, see: Valcke, P, Clifford D and Steponėnaitė VK (2020) 'Constitutional Challenges in the Emotional AI Era' in Giovanni S, Micklitz, HW, Longo E, Pollicino O, Reichman, A and Simoncini A (eds) Constitutional Challenges in the Algorithmic Society (Cambridge: Cambridge University Press, forthcoming).

[46] Davis, P (2020) 'Facial detection and smart billboards: Analysing the 'identified' criterion of personal data in the GDPR', University of Oslo Legal Studies Research Paper Series No. 2020-01.

[47] George, D, Reutimann, K and Tamò-Larrieux, A (2019) 'GDPR bypass by design? Transient processing of data under the GDPR', International Data Privacy Law 9(4) 285.

[48] This appears to be the view the Italian Data Protection Authority, for instance, has taken with regard to the installation of 'digital signage' promotional equipment at a train station in Milan. See: Garante per la protezione dei dati personali (2017) 'Installazione di apparati promozionali del tipo 'digital signage' (definiti anche Totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252]. Authors have also argued that, since the possible harms of these technologies are similar to the harms against which data protection law aims to protect, a broad understanding of the notion of *'personal data processing'* may be justified. See: Davis, P (2020) 'Facial detection and smart billboards: Analysing the 'identified' criterion of personal data in the GDPR', University of Oslo Legal Studies Research Paper Series No. 2020-01.

interest according to WP29.[49] Moreover, it should not be forgotten that the EU Charter recognises a *'freedom to conduct a business'*.[50] *'Necessity'* requires the controller to look for the least intrusive means of achieving the processing's intended purpose. Yet, when this is about obtaining better knowledge of the audience that otherwise cannot be achieved with conventional means, conventional alternative measures are hardly comparable and as effective: the processing may indeed be necessary. Controllers are then required to weigh in the rights and interests of data subjects. Evidently, the rights to privacy and data protection come to mind.

In terms of privacy, it should be noted that national and European courts tend to consider expectations of privacy to be lower in public spaces, and hence the intensity of interferences with the right occurring in public spaces to be less severe compared with interferences affecting the privacy of communication data.[51] Concerning data protection (a right distinct to privacy in the EU legal order), when the processing complies with the safeguards provided for in EU secondary legislation, it is difficult to argue that the right's enjoyment is unduly restricted. Beyond fundamental rights, there might be other *'interests'* at stake. Displaying different ad messages based on gender or age could, for instance, entrench stereotypes on consumer behaviour that may ultimately prove harmful to the data subject.[52] Yet, *'personalised ads'* are so normalised in the online environment that a controller could wonder whether transposing some degree of (and indeed more limited) personalisation in the offline world poses any real risk. Emotion detection raises additional issues, as data subjects may face discomfort and distress in the thought that their emotions are observed.[53]

---

[49] WP29 (2014) 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', WP 217, 24.

[50] Article 16 EU Charter.

[51] Judgment n° 27/2020 of 20 February 2020 Belgian Constitutional Court, Action for annulment of the Law of March 21, 2018 'amending the law on the police function, with a view to regulating the use of cameras by the police services, and amending the law of March 21, 2007 regulating the installation and the 'use of surveillance cameras, the law of 30 November 1998 on the intelligence and security services and the law of 2 October 2017 regulating private and specific security', at B.7.6. In the context of the ECHR and the right to privacy, the ECtHR has also examined the concepts of *'reasonable'* or *'legitimate'* privacy expectations in public spaces. In Uzun v Germany it clarified that even though *'a person walking along the street will inevitably be visible to any member of the public who is also present'* and monitoring of the same public space by a security guard, for instance through CCTV would have a similar character, *'once any systematic or permanent record comes into existence of such material from the public domain'* privacy considerations may arise; see: Judgment in Uzun v Germany (ECtHR) Application no. 35623/05, para. 44.

[52] An interesting example was given by Tobias Judin (Norwegian Data Protection Authority) during the Computers, Privacy and Data Protection (CPDP) 2020 Conference in the *'Digital Signage, Facial Detection and Data Privacy: Exploring the Boundaries of Smart Advertising in Public Spaces'* panel. The example included a pizza ad that displays an image featuring a pizza slice and salad, when the audience is female, and an image with a full pizza, a large soft drink and no salad for male audience, because one could assume that is generally more appealing to them.

[53] This may be the case because, as McStay argues, emotion detection makes use of information about emotions, which is inherently intimate information. A survey of about 2000 people in the UK

The challenge with the balancing test is that even where controllers are not ill-intentioned nor wish to undermine the rights and interests of data subjects, its outcome is likely to favour their interests. Controllers' interests will often be real, tangible and quantifiable (e.g. expected increased revenue from optimised advertising methods). Alternatively, the rights and interests of data subjects are broad, elusive, and difficult to grasp. The extent to which there are expectations of privacy and what are these in public spaces still sparks interesting debates. Other potential harms, which can arise from the processing, raise what controllers could consider as vague and hypothetical issues when it comes to individual autonomy and freedom.

3.2.4 The public space challenge

The discretion that the *'legitimate interests'* legal basis leaves on controllers is significant as they are the ones that have to balance interests. Yet, increased surveillance and the monetisation of citizens data can challenge not only citizens' rights and interests, but also, the nature and character of public spaces.[54] By implication, protecting data subjects and the nature of public spaces might call for a limit in controllers' discretion.

Such protecting trends have already emerged in some Member States. The emergence of laws regulating video surveillance is a case in point. Belgium, for instance, adopted in 2007 an act on the installation and use of surveillance cameras that stood in addition to the general data protection law. The legislative proposal noted, among other things, that general data protection legislation is based on general principles. The lack of concrete standards for cameras ultimately impacts the principle of legal certainty, as well as the legitimacy of surveillance.[55] By listing the objectives for which images may be recorded and used, setting retention periods and requiring the display of a pictogram indicating that camera surveillance takes place, the law essentially limits controllers' discretion in determining the necessity and proportionality of the processing.

Unlike video-surveillance, there are no *leges speciales* to guide smart city processing in public spaces via sensors, trackers and facial detection technologies. Regulators are nevertheless not indifferent to these developments. The French data protection authority

---

demonstrated that a percentage of 50% of respondents were *'not OK at all'* with any form of automated emotion detection using facial coding. See: McStay, A (2016) 'Empathetic media and advertising: industry, policy, legal and citizen perspectives (the case for intimacy)', Big Data & Society.

[54] A detailed discussion on the concept of public spaces, the values attached to them and how these are challenged by smart city surveillance can be found in the doctoral thesis of Maša Galič entitled 'Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space' (Doctoral dissertation Tilburg University) <https://pure.uvt.nl/ws/portalfiles/portal/31748824/Galic_Surveillance_19_11_2019.pdf>.

[55] Belgische Senaat, Wetsvoorstel tot regeling van de plaatsing en het gebruik van bewakingscamera's, 31 mei 2006, Parlementair document nr. 3-1734/1, https://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=3&NR=1734&VOLGNR=1&LANG=nl >; See also the Opinion of the Belgian Data Protection Authority on the proposal: Advies van de Commissie voor de bescherming van de persoonlijke levenssfeer Parlementair document nr. 3-1734/3, https://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=3&NR=1734&VOLGNR=3&LANG=nl.

issued in February 2020 guidelines on how to measure the audience of billboards or the number of visitors in spaces accessible to the public. According to the French authority, *'legitimate interests'* can only be relied on for the processing if data are anonymised within minutes of collection, or if they are immediately pseudonymised and subsequently anonymised within 24 hours.

Moreover, controllers must put in place additional procedural safeguards.[56] In its guidance on Wi-Fi and Bluetooth tracking, the Dutch authority opined that the ability of private entities to rely on '*legitimate interests'* differs depending on whether tracking takes place in a public space or a semi-public one.[57] It considers that private entities have no authority over public spaces, thus, only public authorities would normally be entitled to process personal data from such spaces. In semi-public spaces that are privately owned there is more scope to rely on *'legitimate interests'*, even though the authority still suggests that this is possible only when the objective of the tracking system is to ensure the safety of passers-by, and not a commercial goal.[58]

These stricter approaches towards data processing in public spaces may hinder the harmonisation objective at the heart of the GDPR. Harmonisation is crucial for processing activities that pertain to the *'private realm'* because businesses ought to benefit from a level-playing field and legal certainty in the EU internal market. Restricting the application of the *'legitimate interests'* does not sit comfortably with CJEU case-law on that legal basis either and will be discussed in Section 4.

3.3 Sensitive data processing

Lawfulness of processing of sensitive personal data becomes increasingly relevant to discuss in the smart city context when one witnesses the trialling and use of facial recognition technology across many different contexts. Local (police) authorities have been experimenting with facial recognition and its potential to instantly locate and track people walking in a monitored area. Public schools have sought to use this technology to improve security in the school and to optimally measure students' attendance. Moreover, in the retail context, facial recognition is promoted as a tool to facilitate the operation of loyalty programmes, offer frictionless shopping experiences and even detect known shoplifters as they enter a store.

The GDPR has placed the processing of *'biometric data for the purpose of uniquely identifying a natural person'* to the sensitive data category, thereby making facial

[56] CNIL (2020), 'Dispositifs de mesure d'audience et de fréquentation dans des espaces accessibles au public : la CNIL rappelle les règles' <https://www.cnil.fr/fr/dispositifs-de-mesure-daudience-et-de-frequentation-dans-des-espaces-accessibles-au-public-la-cnil>.
[57] Dutch Data Protection Authority, 'Questions about Wi-Fi and Bluetooth tracking' <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq>.
[58] Dutch Data Protection Authority, 'Questions about Wi-Fi and Bluetooth tracking' <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq>.

recognition technologies in many cases subject to the stricter legal regime applicable to sensitive data. Article 9(1) prohibits the processing of sensitive data, a prohibition that can only be lifted if one of the exceptions listed in Article 9(2) applies. We consider the following exceptions to be most relevant in a smart city context:

- Processing based on the explicit consent of the data subject (Article 9(2)(a))
- Processing necessary for reasons of substantial public interest (Article 9(2)(g))
- Processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 9(2)(i))

3.3.1 The limitations of explicit consent

Explicit consent is the only ground that may legitimise sensitive data processing for commercial interests like marketing, advertising, and optimisation of shopping experiences, and the protection of private property. The other exceptions listed in Article 9(2) are tailored around public interests (e.g. the protection of public health), or other interests that are construed narrowly (e.g. the establishment, exercise or defence of legal claims). Indeed, in the context of sensitive data, there is no concept like the broad *'legitimate interests'* legal basis of Article 6(1)(f).

The requirements for valid consent are more stringent compared to consent under Article 6(1)(a) as consent for sensitive data processing needs to be *'explicit'*. The European Data Protection Board (EDPB) has attempted to clarify this point arguing that the term explicit *'refers to the way consent is expressed by the data subject'*.[59] However, considering the increased risks this processing entails, it can be questioned the extent to which such emphasis on the process of getting consent gives true meaning to the intention of the Regulation. In their commentary on Article 9 GDPR, Georgieva and Kuner link explicit consent with a requirement for *'a high degree of precision and definiteness in the declaration of consent, as well as a precise description of the purposes of the processing'*.[60]

It is suggested that this high threshold for valid explicit consent is difficult to meet in practice. For instance, in terms of technologies capturing and processing sensitive data in public or semi-public spaces, controllers must implement opt-in mechanisms rather than adopt tacit or hypothetical ones. Indeed, one does not agree to the processing merely by passing close to a camera.[61] Moreover, consent entails a right for the data subject to

---

[59] EDPB (2020) 'Guidelines 05/2020 on consent under Regulation 2016/679' Adopted on 4 May 2020, 20-21.

[60] Georgieva, L and Kuner, C (2020) 'Article 9. Processing of special categories of personal data' in Kuner, Bygrave and Docksey (eds) The EU General Data Protection Regulation (GDPR): A Commentary (Oxford: Oxford University Press), 377.

[61] On this point, it is worth clarifying that the EDPB considers that Article 9(2)(e), which allows processing that relates to personal data that are *'manifestly made public by the data subject'*, cannot be relied on to legitimise the processing. Entering within a camera's range does not mean that an individual intends to make sensitive data relating to him or her public. See: EDPB (2020) 'Guidelines 3/2019 on processing of personal data through video devices' Version 2.0 Adopted on 29 January 2020, 15.

withdraw his or her consent at any time. This right is particularly challenging to exercise in ambient environments as in smart cities.

3.3.2 Substantial public interest, scientific research and the need for additional legal basis in EU or national law

Article 9(2) GDPR enables the processing of sensitive data where it is necessary for reasons of substantial public interest and for scientific research purposes. In both cases, it is understood that this is to be done on the basis of (additional) EU or national law. It is thus relevant here to refer back to the discussion on the requirements for additional legal bases, which was considered in Section 3.1.2, and particularly the need for *'foreseeability'*.

The EU legislator has been more wary in the case of these Article 9 exceptions to stipulate that such laws must respect the essence of the right to data protection, be proportionate to the aim pursued and provide suitable and specific measures to safeguard fundamental rights. Moreover, as Article 9(2) GDPR provides exceptions to the principle that sensitive data should not be processed, a meaningful protection of fundamental rights requires these exceptions to be interpreted strictly.[62] [63]

Consequently, while in the case of the *'public task'* legal basis a general law mandating an authority to perform public interest tasks could sometimes be enough to ground a processing activity, broad legal empowerments to process sensitive data are most likely inadequate. Proportionality, respect of essence and suitable legal safeguards can only be achieved where narrowly defined *'substantial public interest'* or *'scientific research'* objectives are weighed against the impact of the intended processing on the rights and freedoms of the individuals concerned.

Without such additional legal bases, the exceptions in Article 9(2) GDPR that require further EU or national law are *'empty shell'*. Yet, the question remains as to whether these laws already exist in all Member States. The issue of lawfulness of sensitive data processing gained prominence during the covid-19 pandemic. Health related data is considered sensitive data. The EDPB issued guidelines on this matter, which note that in the absence

---

[62] Georgieva, L and Kuner, C (2020) 'Article 9. Processing of special categories of personal data' in Kuner, Bygrave and Docksey (eds) The EU General Data Protection Regulation (GDPR): A Commentary (Oxford: Oxford University Press), 375.

[63] The attempt of a school in Sweden to use facial recognition to record student attendance, in an experimental project, provides useful insights on the strict interpretation of Article 9(2) exceptions. The Swedish data protection authority was called to examine the lawfulness of the processing. The authority considered that students' sensitive data could not be processed on the basis of explicit consent because of the power imbalance between the controller (school) and the data subjects (students). The question then arose whether the exception for reasons of *'substantial public interest'* could be relied on. The authority stressed the need for a basis in EU or national law and noted that the implementing provisions established in Sweden have a narrow scope and are not meant to apply to day-to-day, fundamental rights-intrusive processing, as the one envisaged to manage school attendance. See: Swedish Data Protection Authority, 'Supervision in accordance with the EU Data Protection Regulation 2016/679 - facial recognition for attendance control of students' Decision of 20 August 2019 [in Swedish] https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf.

of data subject consent, specific laws by the EU or Member States must provide a legal basis for the processing.

Moreover, proportionality, respect of essence and suitable and specific protective measures are also mentioned as requirements for those legal bases.[64] However, even though the EDPB consists of representatives of all EU Member States that have knowledge of each national context, no further guidance or concrete examples of such laws are included in the guidelines. One could argue that these guidelines were a missed opportunity to clarify what constitutes a valid legal basis and the EDPB could have given some specific examples. Indeed, research stakeholders have been asking for such clarification in terms of processing for scientific research well before the pandemic.[65]

The pandemic did eventually see some legislative activity to legitimise the processing of health data for research and public health purposes, at least in Belgium.[66] At the same time, there is no specific legal framework on other forms of sensitive data processing relevant for smart cities, such as the use of facial recognition for reasons of substantial public interest or research.

4. The Different regime for 'public' and 'private' interests

4.1 Consequences of data protection's recognition as a fundamental right

Section 3 revealed a key difference in the treatment of processing for private interests, on the one hand, and public interest processing, on the other. Regarding the latter, to ensure lawfulness, the GDPR provisions, which establish legal bases (Article 6(1)) or legal grounds exceptionally enabling the processing of sensitive data (Article 9(2)) are not enough. Additional legal bases are needed. This entails that contrary to private interest processing, where the responsibility to balance interests lies with the individual controller, for public

[64] EDPB (2020) 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak', Adopted on 21 April 2020.
[65] 'The Application of GDPR to Biomedical Research: Stakeholder Advisory Opinions to Assist Regulators', Input Paper prepared for the ISC seminar on challenges for health research arising from the GDPR, Brussels 19 November 2019, 8.
[66] See for instance: Federal level: Koninklijk besluit nr. 44, 26 June 2020 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano, http://www.ejustice.just.fgov.be/eli/besluit/2020/06/26/2020041950/staatsblad; Flanders: Decreet van 29 May 2020 tot organisatie van de meldingsplicht en het contactonderzoek in het kader van COVID-19, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2020052904&table_name=wet; Brussels: Besluit van bijzondere machten van het Verenigd College van de Gemeenschappelijke Gemeenschapscommissie n° 2020/006 van 18 June 2020 tot het organiseren van het gezondheidskundig contactonderzoek in het kader van de strijd tegen de COVID-19-pandemie, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2020061838&table_name=wet.

interest processing it is the responsibility of the legislator to determine public interests and how those interests should be weighed against the rights of the individuals.

The Data Protection Directive did not contain similar provisions on the need for additional legal bases. Moreover, the provisions on additional legal bases in the GDPR often employ language that mirrors the language found in Article 52(1) of the Charter, including the respect of essence and the proportionality principle. A question arises as to whether the increased importance of additional legal bases could be due to the recognition of a fundamental right to data protection in the Charter. It is suggested that the development of a right to data protection in Article 8 of the Charter reflects a rather unusual trajectory. [67] This is because the right was preceded by detailed secondary law regulating data processing. Faced with a CJEU that failed to thoroughly engage in discussions on the normative elements of the right,[68] academic scholarship has taken up the challenge of elucidating its role and meaning.

Academic debate has discussed whether the right should be understood as prohibitive or permissive,[69] substantive or procedural,[70] or as a tool for transparency. [71] While this debate remains, the CJEU held in Digital Rights Ireland that the measure *'constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data'*.[72] This statement suggests that the Court views data protection as a prohibitive right, equating any processing to an interference with the right that needs justification. Viewing the right as prohibitive indeed brings it closer to the functioning of other fundamental rights, such as the right to privacy.

Recognising data protection as a fundamental right in the EU Charter has legal consequences, specifically regarding how the relationship between the right and the EU

---

[67] Clifford, D (2019) The legal limits to the monetisation of online emotions (Doctoral dissertation KU Leuven Centre for IT & IP Law), Chapter 3.2.

[68] For a detailed and critical discussion of this case law, see: González Fuster, G (2014) The emergence of personal data protection as a fundamental right of the EU (Switzerland: Springer International Publishing), Chapter 7.

[69] See, notably: González Fuster, G and Gutwirth, S (2013) 'Opening up Personal Data Protection: A Conceptual Controversy', 29 Computer Law & Security Review 531, 532-533; Hijmans, H (2016) The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU Springer, Issues in Privacy and Data Protection, 55; Clifford, D (2019) The legal limits to the monetisation of online emotions (Doctoral dissertation KU Leuven Centre for IT & IP Law), Chapter 3.2.1.

[70] See, notably: Ausloos, J (2020) The right to erasure: Safeguard for informational self-determination in a digital society? (Oxford: Oxford University Press); Dalla Corte, L (2020) 'A right to a rule: On the substance and essence of the fundamental right to personal data protection' in Hallinan, D, Leenes, R, Gutwirth, S & De Hert, P (eds), Data protection and privacy: Data protection and democracy (Oxford: Hart Publishing), 27-58.

[71] Gutwirth, S and De Hert, P (2006) 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Claes, E, Duff, A & Gutwirth, S (eds) Privacy and the criminal law (Antwerp/Oxford: Intersentia), 61-104.

[72] Judgment in Digital Rights Ireland, C-293/12 and C-594/12 ECLI:EU:C:2014:238, para. 126.

secondary legal framework on data protection should now be understood.[73] At the outset, it should be noted that fundamental rights traditionally aim to protect citizens against states. For instance, the ECHR initially recognises negative obligations for states to refrain from unjustifiable interferences with fundamental rights. Alternatively, positive obligations may also exist for some rights, requiring states to take action to ensure that individuals effectively enjoy their rights. EU Treaties arguably activate such positive obligation concerning data protection as Article 16 TFEU requires the EU legislator to *'lay down the rules'* in terms of the protection of personal data.

Secondly, most fundamental rights including the right to data protection are not absolute but may be limited on the grounds of general interest of the public or protecting the rights of others. The conditions on limitations of fundamental rights can be found in Article 52(1) of the Charter and include the need to respect the essence of the right, necessity and proportionality. To a large extent, those reflect the conditions on justified limitations, which are also found in the ECHR.

Thirdly, judicial review to verify compliance with fundamental rights' obligations is, at least in the context of the ECHR, not identical in cases concerning negative or positive obligations.[74] While for both types of obligations the aim is to strike a fair balance between competing interests, in terms of negative obligations, there is a stricter scrutiny of the conditions on justifiable limitations, and the extent to which a fair balance has been struck. A wider margin of appreciation is given when it comes to positive obligations as courts may be reluctant to replace their own judgment with the balancing made by legislators. There, the ECtHR seemingly proceeds *'with a degree of circumspection that is rarely found in the framework of a review of negative obligations'*.[75]

In light of the above, the GDPR could be seen as reflecting the positive obligation to ensure that the right to data protection is protected. In fact, as Ausloos notes, while the right to data protection is to be protected *'in particular'*, the GDPR aims to protect all fundamental rights and freedoms of natural persons that may engage in the context of personal data processing.[76] To ensure such protection, the GDPR sets an infrastructure for fair balancing, which taken as a whole provides a detailed materialisation of the conditions for justifiable limitations found in Article 52(1) of the Charter.[77] This system of fair balancing though, mainly determines how the balance is to be struck, rather than conclusively striking the

---

[73] See: Lynskey, O (2015), The Foundations of EU Data Protection Law (Oxford: Oxford University Press), discussion in Chapter 8 'Conclusions and Future Prospects'.
[74] For an in-depth discussion see: Klatt, M (2011) 'Positive obligations under the European Convention on Human Rights', 71 Heidelberg Journal of International Law 691.
[75] Akandji-Kombe, JF (2007) 'Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights', Council of Europe Human rights handbooks, No. 7, 18.
[76] Article 1(2) GDPR; Ausloos, J (2020) The right to erasure: Safeguard for informational self-determination in a digital society? (Oxford: Oxford University Press), 82.
[77] Ausloos, J (2020) The right to erasure: Safeguard for informational self-determination in a digital society? (Oxford: Oxford University Press), 289.

balance between the competing rights and interests itself.[78] Questions such as to what extent a processing operation is fair, legitimate, or proportionate are open, and for the controller to decide. Controllers have significant discretion and decision-making power when it comes to such decisions.[79]

This discretion given to controllers is understandable, especially for processing that relates to private interests. There is a *'legitimate economic concern'* that *'private enterprise should not be overly burdened by data protection obligations'*.[80] Moreover, private entities are not the addressees of fundamental rights obligations. Though the exercise of positive obligations may require states to intervene and govern horizontal relations between private parties to ensure that individuals are protected from violations of their rights from private entities, States have discretion in terms of achieving such protection. The GDPR arguably reflects the EU legislator's choice to add responsibility to the controller by providing a system of checks and balances that should ultimately guide the latter towards fair balancing.

Yet, such degree of discretion could be more problematic for public authorities, which process data for public interest objectives. What might be at stake there is not only the positive obligation to protect, but the negative duty for public authorities not to interfere with the rights in question. Considering the CJEU's view that the right to data protection is interfered with whenever personal data is being processed, it could be argued that, by definition, by processing personal data authorities breach their duty not to interfere with the right. Such interference may be justified through recourse to Article 52(1) and Article 8(2) and (3)[81] of the Charter.

However, the fair balancing exercise is stricter in the context of negative obligations. It is unclear how the broad fair balancing guidance set out by the GDPR can meet the stricter demands, which normally apply to state actors in fundamental rights law. In fact, by making additional legal bases necessary for public interest processing, the GDPR suggests the opposite. To put differently, the legislator should predetermine and strike a fair balance in those cases, paying due regard to the conditions on limitations of fundamental rights established not only in the Charter and the ECHR, but also the CJEU and ECtHR case-law.

---

[78] Quelle, C (2017) 'Privacy, Proceduralism and Self-Regulation in Data Protection Law', Teoria Critica della Regolazione Sociale.

[79] Quelle, C (2018) 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach', 9 European Journal of Risk Regulation 502.

[80] Blume, P (2015) 'The Public Sector and the Forthcoming EU Data Protection Regulation', 1 European Data Protection Law Review 32, 32.

[81] According to the CJEU in Digital Rights Ireland, paras. 47 & 49 *'Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied. […] Moreover, Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set forth in Articles […] and 8 of the Charter, as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.'* This indicates an understanding of Article 8(2), and possibly Article 8(3) as well, as detailing specific conditions that legitimise the processing, which co-exist with the general limitations clause in Article 52(1) of the Charter.

Finally, it should also be noted that stricter legitimacy requirements for processing taking place in a vertical (state-citizen) scenario, can also be mandated by legal orders of Member States. For example, in terms of the right to informational self-determination, the German Constitutional Court recognises that the legislator must specify the purpose of the processing, which must be narrower than the public task of a public agency.[82]

4.2 Smart cities, legitimacy and legal certainty

The requirement for additional, foreseeable legal bases to ground public interest processing in smart cities inevitably stresses the need to create laws to supplement the GDPR. In the absence of such laws, questions remain regarding the legitimacy of smart city processing. At the same time, to create this new type of laws may not be an easy task. Smart city projects are innovative, experimental and adaptive. These characteristics are in sharp contrast with the rigidity of legal rules. From a factual standpoint, even for controllers it can be challenging in innovative projects to anticipate and specify the purposes of the processing, as well as balancing the benefits against the risks. Incorporating these considerations into legislation, enabling both foreseeability and flexibility, remains a herculean task. Some of the challenges to overcome include the variety of projects, technologies and purposes within the smart city, or the level at which legislation needs to be created, be it international, regional or domestic.

The need for additional legal bases also stresses the harmonisation objective of EU data protection law. This objective can be found in both, Article 16(2) TFEU and Article 1(1) of the GDPR. Both provisions note that the aim of EU data protection legislation is to lay down rules to protect personal data and ensure their free movement. At the same time, it should be recalled that, when it comes to referring to additional legal bases, the GDPR stipulates that those may not only come from EU law, but also national law. This calls for reflection as to whether in some instances EU-wide legal instruments are more appropriate than national ones. For example, the need for additional legal bases to ground the exception to the prohibition of sensitive data for scientific research reasons might be a case in point. Given the increasingly international character of modern research, variations in the legal bases for processing adopted across different Member States would challenge the conduct of research that spans multiple states.[83]

For smart city processing serving private interests, it is argued that preserving the data protection's harmonisation objective is even more crucial. A harmonised framework provides a level-playing field for private actors in an era where personal data processing is key to the exercise of economic activity. The CJEU has stressed the importance of harmonisation in its case-law regarding the application of the *'legitimate interests'* legal

[82] von Grafenstein, M (2020) 'How to build data-driven innovation projects at large with data protection by design: A scientific-legal Data Protection Impact Assessment with respect to a hypothetical Smart City scenario in Berlin', HIIG Discussion Paper Series, 2020(3), 46.
[83] 'The Application of GDPR to Biomedical Research: Stakeholder Advisory Opinions to Assist Regulators', Input Paper prepared for the ISC seminar on challenges for health research arising from the GDPR, Brussels 19 November 2019, 8.

basis, in cases where Member States introduced additional conditions to the application of the legal basis. According to the Court in Breyer, national law *'cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case'*[84]. This suggests that the outcome of the balancing should be reached by the controller. Yet, in the smart city context we have seen that data protection authorities have attempted to place limits on the ability of private entities to process personal data from public and semi-public spaces based on the *'legitimate interests'* legal basis.

Different national approaches emerging in Member States challenge the CJEU case-law which suggests that the outcome of the balancing exercise cannot be defined by the legislator. However, it should be noted that, the famous Google Spain[85] judgment on the right to be forgotten, also suggests that the CJEU itself may guide such balancing. The Court there noted that the rights of the data subject overruled the economic interest of the operator.[86] This suggests that some margin of appreciation is given to the CJEU, and arguably even Member States, so that a more structured framework can be adopted for the balancing exercise in certain scenarios. The Breyer judgment nevertheless highlights the importance of retaining some flexibility for the controller.

The use of facial recognition technologies in horizontal relations - that is, for private interests - has the potential to make diverse national legal approaches imminent. In the Netherlands, for example, a report commissioned by the government to explore facial recognition's risks in horizontal relationships has put on the table a series of regulatory options to be discussed.[87] The latter include a total ban on the use of the technology, requesting prior approval by the Data Protection Authority, a specifically targeted legal framework to govern facial recognition, codes of conduct and certification, as well as raising citizen awareness of the technology related risks. In view of potential economic benefits linked to the commercial use of this technology, one could wonder whether action at EU level aimed to regulate risks would be more appropriate to safeguard the importance of harmonisation in the economic area.

5. Legal bases for law enforcement related processing

While previous sections revolved around the legal framework for general processing, smart city initiatives often serve objectives linked to security and the prevention, investigation and detection of crime. For instance, notable examples include intelligent cameras for

[84] Judgment in Breyer, C-582/14 ECLI:EU:C:2016:779, para. 62.
[85] Judgment in Google Spain, C-131/12 ECLI:EU:C:2014:317.
[86] Judgment in Google Spain, para. 97.
[87] Keymolen, E, Noorman, M, van der Sloot, B, Cuijpers, C, Koops, BJ and Zhao, B (2020) 'Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties', WODC / Ministerie van Justitie.
<https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/04/20/tk-bijlage-wodc-rapport-op-het-eerste-gezicht/tk-bijlage-wodc-rapport-op-het-eerste-gezicht.pdf>.

facial recognition and automatic number plate recognition. As processing for law enforcement purposes is governed by the LED, it is also relevant here to discuss the specificities of that legal framework. Additional laws are central to the lawfulness of such processing. Under the LED, the processing is lawful when it is necessary for the performance of a task carried out by a competent authority and it is based on EU or Member State law.[88] In addition, it is required that such laws specify the objectives and purposes of the processing, as well as the personal data at stake.

An important number of decisions from the ECtHR regarding interferences with privacy due to personal data processing took place in the police context.[89] Similarly, seminal CJEU judgments on the rights to privacy and data protection concerned EU or national measures considering data processing for a law enforcement-related purpose.[90] Although not specifically referring to the LED, this case-law is relevant in terms of discussing the lawfulness of police surveillance measures. Such case law has established criteria for the legality, necessity and proportionality of the laws that enable such processing.

Courts have particularly insisted on the *'quality of the law'* requirement and scrutinised laws on the necessity and proportionality of the interference. Indeed, laws regulating law enforcement processing should be lengthy and meticulous.[91] This is particularly the case as law enforcement can be considered a sensitive area, which may well lead to complaints regarding their compliance with fundamental rights. The challenges that new technologies and innovative processing methods raise, bring into question the issue of whether existing laws provide sufficient safeguards to protect against new risks. In this context, the ECtHR quality of the law requirement, which stresses the foreseeability and predictability of legislation in legitimising personal data processing, becomes difficult to satisfy.

Moreover, with police authorities increasingly eager to experiment, test and pilot new technologies, questions arise as to whether the applicable legal framework to cover such tests is the law enforcement data processing one, or the general GDPR framework. This question is not trivial because the legal bases that may ground a processing operation are markedly different in the two frameworks. On the one hand, the scope of the LED is well-defined as the Directive applies to processing for the purposes of prevention, investigation, detection or prosecution of criminal offences including public security issues.

Yet, facial recognition pilots may have broader purposes. Test phases may serve to assess the effectiveness and efficacy of facial recognition systems such as, rating false positives,

---

[88] Article 8 LED.

[89] See: European Court of Human Rights, 'Guide on Article 8 of the Convention – Right to respect for private and family life', 47 (last update: 31.8.2020) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>.

[90] Judgment in Digital Rights Ireland, C-293/12 and C-594/12 ECLI:EU:C:2014:238; Opinion 1/15 of the Court, ECLI:EU:C:2017:592; Judgment in Tele2 Sverige AB, Joined Cases C-203/15 and C-698/15 ECLI:EU:C:2016:970.

[91] In Belgium, for instance, the Law on the functions on the Police (Wet op het politieambt) provides detailed safeguards for the processing of personal data by the police, and sets the conditions on the creation and use of databases, including the *'technical databases'* created following the use of intelligent cameras and systems for ANPR.

rather than contributing towards arrests of suspects. If these systems run experimentally without a clear crime prevention and/or investigation purpose, they are likely to fall under the GDPR and not the LED.[92] At the same time, if the GDPR regime is applicable, it should be recalled that the lawfulness of the processing requires the existence of a legal basis, under Article 6(1) GDPR, as well as satisfying one of the exceptions to the prohibition to process sensitive data as per Article 9(2). As regards the latter, in the absence of an additional legal basis that may legitimise sensitive data processing for research or substantial public interest reasons, explicit consent would seem to be the only ground capable of ensuring lawfulness.

6. Conclusion

Our analysis in this paper has demonstrated two key challenges on the lawfulness of smart city processing. Firstly, in terms of public interest processing, both, the GDPR and LED may be insufficient to ensure the lawfulness of processing. Such pieces of legislation include provisions on legal bases for public interest processing which require further operationalisation at the EU or national law level. It is therefore arguable that additional legal bases should be created.

However, when it comes to adopting the foreseeability principle, it is questionable if intrusive smart city processing should be undertaken by local authorities based on broad laws stipulating their tasks. To enable smart city development, it is therefore important to reflect on the additional laws needed to supplement the EU data protection acts. Secondly, regarding private interest processing, if the harmonisation objective is considered, this objective may be eroded when diverging national practices emerge as a result of regulators' desire to offer citizens increased protection in public spaces.

At the same time, it should be noted that even though the lawfulness principle unfolds differently depending on whether a processing operation serves public, private, or law enforcement interests, in practice, it is difficult to ascertain this distinction. This is due to the blurring lines between, on the one hand, public, and, on the other, private, in the smart city context. Smart city initiatives are often implemented as Public-Private-Partnerships, which involve both, public and private actors. In her analysis of the Stratumseind Living Lab in the city of Eindhoven, Galič has argued that *'commercial goals are inseparable from the maintenance of the public order and safety part of the goals and they are attempted to be achieved through the same means and actors'*.[93] Thus, a case can be made that the clarity

[92] Peeters, B (2020) 'Facial recognition at Brussels Airport: face down in the mud' (CiTiP Blog 17 March 2020) <https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/> (accessed 5 February 2021).

[93] Galič, M (2019) 'Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space' (Doctoral dissertation Tilburg University) <https://pure.uvt.nl/ws/portalfiles/portal/31748824/Galic_Surveillance_19_11_2019.pdf, 349>.

that the lawfulness principle demands over the actors and interests pursued by a processing operation is put under considerable pressure by smart cities' Public-Private-Partnership model.

Bibliography

Advies van de Commissie voor de bescherming van de persoonlijke levenssfeer Parlementair document nr. 3-1734/3 <https://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=3&NR=1734&VOLGNR=3&LANG=nl>.

Akandji-Kombe, JF (2007) 'Positive obligations under the European Convention on Human Rights: A guide to the implementation of the European Convention on Human Rights', Council of Europe Human rights handbooks, No. 7.

Ausloos, J (2020) The right to erasure: Safeguard for informational self-determination in a digital society? (Oxford: Oxford University Press).

Belgian Constitutional Court, Judgment n° 27/2020 of 20 February 2020, Action for annulment of the Law of March 21, 2018 'amending the law on the police function, with a view to regulating the use of cameras by the police services, and amending the law of March 21, 2007 regulating the installation and the 'use of surveillance cameras, the law of 30 November 1998 on the intelligence and security services and the law of 2 October 2017 regulating private and specific security'.

Belgische Senaat, Wetsvoorstel tot regeling van de plaatsing en het gebruik van bewakingscamera's, 31 mei 2006, Parlementair document nr. 3-1734/1 <https://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=3&NR=1734&VOLGNR=1&LANG=nl>.

Besluit van bijzondere machten van het Verenigd College van de Gemeenschappelijke Gemeenschapscommissie n° 2020/006 van 18 June 2020 tot het organiseren van het gezondheidskundig contactonderzoek in het kader van de strijd tegen de COVID-19-pandemie <http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2020061838&table_name=wet>.

Blume, P (2015) 'The Public Sector and the Forthcoming EU Data Protection Regulation', 1 European Data Protection Law Review 32.

Butler, O (2018) 'Obligations imposed on private parties by the GDPR and the UK Data Protection Law: Blurring the public-private divide', 24(3) European Public Law 555.

Charter of Fundamental Rights of the European Union, 2012/C 326/02.

CJEU, Heinz Huber v Bundesrepublik Deutschland, C-524/06 ECLI:EU:C:2008:724.

CJEU, Digital Rights Ireland, C-293/12 and C-594/12 ECLI:EU:C:2014:238.

CJEU, Tele2 Sverige AB, Joined Cases C-203/15 and C-698/15 ECLI:EU:C:2016:970.

CJEU, Smaranda Bara and Others, Case C-201/14 ECLI:EU:C:2015:638.

CJEU, Breyer, C-582/14 ECLI:EU:C:2016:779.

CJEU, Google Spain, C-131/12 ECLI:EU:C:2014:317.

Clifford, D (2019) The legal limits to the monetisation of online emotions (Doctoral dissertation KU Leuven Centre for IT & IP Law).

Clifford, D and Ausloos, J (2018), 'Data Protection and the Role of Fairness', Yearbook of European vol. 37.

CNIL (2015) '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/>.

CNIL (2020), 'Dispositifs de mesure d'audience et de fréquentation dans des espaces accessibles au public : la CNIL rappelle les règles' <https://www.cnil.fr/fr/dispositifs-de-mesure-daudience-et-de-frequentation-dans-des-espaces-accessibles-au-public-la-cnil>.

Dalla Corte, L (2020) Safeguarding data protection in an open data word: On the idea of balancing open data and data protection in the development of the smart city environment, (Doctoral dissertation Tilburg University) <https://research.tilburguniversity.edu/en/publications/safeguarding-data-protection-in-an-open-data-world-on-the-idea-of>.

Dalla Corte, L (2020) 'A right to a rule: On the substance and essence of the fundamental right to personal data protection' in Hallinan, D, Leenes, R, Gutwirth, S & De Hert, P (eds), Data protection and privacy: Data protection and democracy (Oxford: Hart Publishing).

Davis, P (2020) 'Facial detection and smart billboards: Analysing the 'identified' criterion of personal data in the GDPR', University of Oslo Legal Studies Research Paper Series No. 2020-01.

Decreet van 29 May 2020 tot organisatie van de meldingsplicht en het contactonderzoek in het kader van COVID-19 <http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2020052904&table_name=wet>.

De Hert, P and Malgieri, G (2020) 'Article 8 ECHR compliant and foreseeable surveillance: The ECHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law', Brussels Privacy Hub Working Paper Vol. 6 No. 21.

De Montjoye, YA, Hidalgo, C, Verleysen, M and Blondel, V (2013) 'Unique in the crowd: The privacy bounds of human mobility', 3 Scientific Reports.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281 (no longer in force).

Directive 2016/680/EU 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 L119.

Dutch Data Protection Authority, 'Questions about Wi-Fi and Bluetooth tracking' <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-en-telecom#faq>.

ECtHR, 'Guide on Article 8 of the Convention – Right to respect for private and family life', 47 (last update: 31.8.2020) https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

ECtHR, Roman Zakharov v Russia, Application no. 47143/06.

ECtHR, Huvig v France (ECtHR) Application no. 11105/84.

ECtHR, Uzun v Germany (ECtHR) Application no. 35623/05.

EDPB (2020), 'Guidelines 3/2019 on processing of personal data through video devices' Version 2.0 Adopted on 29 January 2020.

EDPB (2020) 'Guidelines 05/2020 on consent under Regulation 2016/679' Adopted on 4 May 2020.

EDPB (2020) 'Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak' Adopted on 21 April 2020.

EDPS (2017), 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf>.

Edwards, L (2016) 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective', 2 European Data Protection Law Review 18.

European Commission, Smart Cities <https://ec.europa.eu/info/eu-regional-and-urbandevelopment/topics/cities-and-urban-development/city-initiatives/smart-cities_en>.

Finch, K and Tene, O (2014) 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town', 41 Fordham Urban Law Journal 1581.

Galič, M (2019) Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space' (Doctoral dissertation Tilburg University)

<https://pure.uvt.nl/ws/portalfiles/portal/31748824/Galic_Surveillance_19_11_2019.pdf>.

Galič, M and Gellert, R (2021) 'Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab', 40 Computer Law & Security Review.

Garante per la protezione dei dati personali (2017) 'Installazione di apparati promozionali del tipo 'digital signage' (definiti anche Totem) presso una stazione ferroviaria - 21 dicembre 2017 [7496252].

Georgieva, L and Kuner, C (2020), 'Article 9. Processing of special categories of personal data' in Kuner, Bygrave and Docksey (eds) The EU General Data Protection Regulation (GDPR): A Commentary (Oxford: Oxford University Press).

González Fuster, G (2014) The emergence of personal data protection as a fundamental right of the EU (Switzerland: Springer International Publishing).

González Fuster, G and Gutwirth, S (2013) 'Opening up Personal Data Protection: A Conceptual Controversy', 29 Computer Law & Security Review 531.

Government of India, 'Smart Cities Mission' <http://smartcities.gov.in/content/>.

Greenfield, A (2013), Against the smart city (New York: Amazon Media - Kindle edition).

Gupta, P, Chauhan, S and Jaiswal, MP (2019) 'Classification of Smart City Research - a Descriptive Literature Review and Future Research Agenda', 21 Information Systems Frontiers 661.

Gutwirth, S and De Hert, P (2006) 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Claes, E, Duff, A & Gutwirth, S (eds) Privacy and the criminal law (Antwerp/Oxford: Intersentia).

Hijmans, H (2016) The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU Springer, Issues in Privacy and Data Protection.

ICO, 'Guide to RPSI/ What is re-use of public sector information?' <https://ico.org.uk/for-organisations/guide-to-rpsi/what-is-rpsi>.

ICO, 'Lawful basis for processing: Public task' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/>.

Input Paper prepared for the ISC seminar on challenges for health research arising from the GDPR (2019), 'The Application of GDPR to Biomedical Research: Stakeholder Advisory Opinions to Assist Regulators', Brussels 19 November 2019.

Ireland's Data Protection Commission, 'Guidance Note: Legal Bases for Processing Personal Data' December 2019.

Kamara, I and De Hert, P (2018) 'Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach', Brussels Privacy Hub Working Paper Vol. 4 No. 12.

Keymolen, E, Noorman, M, van der Sloot, B, Cuijpers, C, Koops, BJ and Zhao, B (2020) 'Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties', WODC / Ministerie van Justitie. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/04/20/tk-bijlage-wodc-rapport-op-het-eerste-gezicht/tk-bijlage-wodc-rapport-op-het-eerste-gezicht.pdf>.

Kitchin, R (2014) 'The real-time city? Big data and smart urbanism', 79 GeoJournal 1.

Kitchin, R (2015) 'Data-driven, networked urbanism', The Programmable City Working Paper 14.

Kitchin, R and Cardullo, P (2019) 'Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused' smart cities in Europe', 37(5) EPC: Politics and Space 813.

Klatt, M (2011) 'Positive obligations under the European Convention on Human Rights', 71 Heidelberg Journal of International Law 691.

Koninklijk besluit nr. 44, 26 June 2020 betreffende de gezamenlijke gegevensverwerking door Sciensano en de door de bevoegde regionale overheden of door de bevoegde agentschappen aangeduide contactcentra, gezondheidsinspecties en mobiele teams in het kader van een contactonderzoek bij personen die (vermoedelijk) met het coronavirus COVID-19 besmet zijn op basis van een gegevensbank bij Sciensano <http://www.ejustice.just.fgov.be/eli/besluit/2020/06/26/2020041950/staatsblad>.

Kotschy, W (2020), 'Article 6. Lawfulness of Processing' in Kuner, Bygrave and Docksey (eds) The EU General Data Protection Regulation (GDPR): A Commentary (Oxford: Oxford University Press).

Lynskey, O (2015), The Foundations of EU Data Protection Law (Oxford: Oxford University Press).

McStay, A (2016) 'Empathetic media and advertising: industry, policy, legal and citizen perspectives (the case for intimacy)', Big Data & Society.

McStay, A and Urquhart, L (2019) ''This time with feeling?' Assessing EU data governance implications of out of home appraisal based emotional AI', 24 First Monday 10 <https://doi.org/10.5210/fm.v24i10.9457>.

Peers, S and Prechal, S (2014), 'Scope and Interpretation of Rights and Principles' in Peers, S, Hervey, T, Kenner, J and Ward, A (eds), The EU Charter of Fundamental Rights: A Commentary (London: Hart Publishing).

Peeters, B (2020) 'Facial recognition at Brussels Airport: face down in the mud' (CiTiP Blog 17 March 2020) <https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/> (accessed 5 February 2021).

Privacy International, 'Smart cities: Utopian vision, dystopian reality' (2017) <https://privacyinternational.org/report/638/smart-cities-utopian-vision-dystopian-reality>.

Purtova, N (2018) 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law', 10 Law, Innovation and Technology 40.

Quelle, C (2017) 'Privacy, Proceduralism and Self-Regulation in Data Protection Law', Teoria Critica della Regolazione Sociale.

Quelle, C (2018) 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach', 9 European Journal of Risk Regulation 502.

Ranchordás, S (2020) 'Nudging citizens through technology in smart cities', 34(3) International Review of Law, Computers & Technology 254.

Regulation 2016/79/EU 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 L119.

Swedish Data Protection Authority, 'Supervision in accordance with the EU Data Protection Regulation 2016/679 - facial recognition for attendance control of students' Decision of 20 August 2019 [in Swedish] <https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-ansiktsigenkanning-for-narvarokontroll-av-elever-dnr-di-2019-2221.pdf>.

The White House Office of the Press Secretary, 'FACT SHEET: Administration Announces New 'Smart Cities' Initiative to Help Communities Tackle Local Challenges and Improve City Services' 14 September 2015 <https://obamawhitehouse.archives.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help>.

Valcke, P, Clifford D and Steponėnaitė VK (2020) 'Constitutional Challenges in the Emotional AI Era' in Giovanni S, Micklitz, HW, Longo E, Pollicino O, Reichman, A and Simoncini A (eds) Constitutional Challenges in the Algorithmic Society (Cambridge: Cambridge University Press, forthcoming).

Van den Eeckhout, P (2017), 'Hoofdstuk 3. De gemeenten en de lokale openbare instellingen' in Van den Eeckhout, P & Vanthemsche, G (eds) Bronnen voor de studie van het hedendaagse België, 19e-21e eeuw (Brussel: Koninklijke Commissie voor Geschiedenis).

Von Grafenstein, M (2020) 'How to build data-driven innovation projects at large with data protection by design: A scientific-legal Data Protection Impact Assessment with respect to a hypothetical Smart City scenario in Berlin', HIIG Discussion Paper Series, 2020(3).

WP29 (2014) 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', WP 217.

WP29 (2017) 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' WP 248 rev.01.