Surveillance Risks in IoT Applied to Smart Cities*

Isadora Neroni Rezende [0000-0001-5476-3503]

PhD Candidate
Autonomous University of Barcelona, Catholic University of Leuven, University of Bologna
Law, Science and Technology, Rights of the Internet of Everything
Horizon 2020 - Marie Skłodowska-Curie ITN EJD
isadora.neroni@uab.cat

Abstract. With the advent of the IoT, proximity sensor devices are installed in many places in smart cities. Without any regulation or social policy, they could lead to a super-surveillance network managed by multi-agent systems in the future. Such networks may be able to reduce accidents, risks, damage and errors. However, they also pose high risk of surveillance and data breaches, including hacking attacks or malware intrusion. This research project is aimed at investigating the implications of IoT-driven surveillance in smart cities from privacy, data protection and ethical perspectives. The identification of the critical issues related to the extensive deployment of such sensing devices in the urban area will constitute a starting point for the development of a new regulatory framework for sensor-based surveillance in European Smart Cities. This new regulatory system shall be aimed at providing citizens with effective tools to exercise their rights to privacy and data protection when facing IoT-driven surveillance. Indeed, setting a clear set of rules governing big urban data processing shall be considered crucial to ensure a fair, democratic, human-centric development of smart cities in Europe.

Keywords: Smart Cities · Internet of Things · Surveillance · Sensors · Privacy · Data Protection · Big Urban Data

1 State of the Art

Research literature has not yet provided a universally agreed definition of the term "smart cities", despite its ever-growing popularity in public discourse. Generally speaking, this expression conveys the fuzzy idea of the "city of the future", characterised by the widespread digitization of services. While many scholars and stakeholders have focused on the conceptualization of the notion of smart cities [1], others preferred to give up on the challenge of defining what a smart city precisely is. For instance, researchers from the Vienna University of Technology

suggested a totally different approach, indicating that smart cities could simply be identified by referring to six key features: smart economy, smart mobility, smart environment, smart people, smart living, smart governance [11].

With the advent of the Internet of Things (IoT) [9], smart cities infrastructure is increasingly embedded with proximity sensors and actuator nodes capturing a plethora of real-time data on people, places and activities [16]. Urban data is also generated by mobile IoT devices, such as smartphones, or provided voluntarily by citizens by means of crowdsourcing apps. Although fundamental for acquiring a comprehensive and integrated view of the urban agenda [17], such ubiquitous surveillance systems can have worrisome implications for the rights to privacy and data protection of urban dwellers [5, 6, 18].

First of all, the identification of a legal basis legitimizing personal data processing still appears to be problematic in IoT environments, especially when data collection is based on consent [6, 26]. Indeed, consent-based gathering of IoT data poses a two-fold risk: on the one hand, people may not always know where or when data generated by their IoT devices will be gathered by smart city sensors; on the other, many users may wish not to be monitored, but they often lack the tools or any real alternative to actually escape IoT-driven surveillance [29].

Furthermore, systematic repurposing of big urban data significantly undermines citizens' possibilities to exercise an effective control on the information concerning them. Firstly, data generated within the city infrastructure is very likely to be combined with data stored in private companies' databases and processed with the use of big data technologies [6]. The criteria governing the algorithmic processing of big data are often lacking in transparency and may lead to discriminatory results [3, 13, 23]. When dealing with smart cities, these issues are likely to be magnified as the results of automated processing of urban data are employed systematically in public authorities' decision-making processes.

From a criminal justice perspective, for instance, sensor-based collection of data is likely to considerably affect the activities of law enforcement agencies operating in the urban area. Smart data trails may be employed either in predictive policing programs, or in the framework of ongoing criminal proceedings. In these cases, repurposing of big urban data needs to be grounded on a solid legal basis, as required by the European human rights framework on privacy and data protection[1]. Nonetheless, the growing convergence of private and public databases [8] significantly complicates the identification of the legal regime

[1] Cf. Articles 7, 8, and 52(1) of the Charter of Fundamental Rights of the European Union (hereinafter: CFREU) and Article 8 of the European Convention of Human Rights (hereinafter: ECHR). Moreover, it should be noted that in its leading case Digital Rights Ireland, the European Court of Justice (hereinafter: ECJ) has considered law enforcement's access and re-use of metadata on communications as constituting an interference on the rights enshrined at Articles 7 and 8 of the CFREU, cf.

laying down the exact conditions for law enforcement's access of users' personal data. In fact, the legal requirements for repurposing collected IoT data may vary depending on the public or private nature of the database in which such data has been stored. In the former case, smart data may be lawfully re-used for law enforcement purposes without any prior authorisation, pursuant to the general principle of re-use of documents held by public sector bodies[2]. In the latter, on the contrary, law enforcement officers shall obtain ex ante authorisation from an independent body in order to access data gathered by private companies[3].

In the context of smart cities, the expanding privatisation of infrastructure implies that venues traditionally considered as public (e.g. town squares, roads) are now laden with privately operated sensors. Likewise, services such as public transportation, policing, management of utilities and public health systems are extensively delegated to private companies on the grounds of public-private partnerships (hereinafter: PPP or P3). In these situations, it may not always be easy to know if sensor data will be stored directly in public databases, or in those held by the private companies delivering the service [19]. Any lack of clearness on the legal framework applicable to IoT data collected in smart cities is thus likely to benefit disproportionally the activities of law enforcement agencies, which may easily get access to citizens' data by circumventing privacy and data protection safeguards.

Legal issues related to the processing of smart data go largely beyond the field of (algorithmic) criminal justice. Thanks to big data analytics, troves of personal data gleaned from different small sensors in the urban area can now reveal powerful inferences about citizens and consumers, which could occasionally result in denial of insurance, discrimination in recruitment procedures or in price policies [25]. When dealing with smart cities, economic sorting of the population can also lead to unfair practices in the management of public services, which may be partially or poorly delivered in disadvantaged neighbourhoods [29]. In this respect, it should be noted that the policies drawing on the algorithmic processing of smart data not only give rise to discrimination issues, but also put into question the accountability of public authorities, as well as citizens' possibility of exercising a democratic control over historic State functions [27].

IoT data collected by smart city sensors will be probably outsourced to the cloud. In this case, automated software is likely to copy the data and re-direct it to other data centres – possibly falling under a different jurisdiction – in order to spare resources and boost performance rates. In practice, however, such pro-

---

ECJ, 8 April 2014, *Digital Rights Ireland Ltd*, joint cases C-293/12 and C-594/12, §35.

[2] Article 3 of the Directive 2019/1024/EC of the European Parliament and of the Council, of 20 June 2019, on on open data and the re-use of public sector information (recast) (Official Journal L 172, 26/06/2019 pp. 56 – 83).

[3] Cf. ECJ, *Digital Rights Ireland Ltd*, cit., §62.

cessing operations are hardly transparent and raise important privacy concerns, as data is very likely to be outsourced to countries having lower data protection standards [7]. Moreover, when access to stored IoT data is required by foreign law enforcement authorities, cross-border cooperation between States may be necessary [14].

2 Research questions

This research project aims to tackle the following research questions and sub-questions:

1. How can citizens effectively exercise their rights to privacy and data protection in the context of smart cities IoT-driven surveillance?

- Is the traditional notion of individual privacy apt to tackle the challenges of big urban data processing?
- When required, how can end users provide for meaningful consent to data processing operations in IoT urban environments?
- Which conditions should govern law enforcement agencies' access and use of publicly and privately stored IoT urban data?
- What kind of remedies should be available to smart cities citizens against fully automated processing of big urban data performed by public authorities?
- Which mechanisms can ensure smart cities public bodies' accountability for privacy and data protection violations?
- Which are the implications of smart cities open data initiatives for citizens' rights to privacy and data protection?
- Which principles should govern a privacy-oriented implementation of the smart city infrastructure?
- Which technological solutions can safeguard data sovereignty for cloud-stored IoT urban data?

2. Can individuals claim to have a reasonable expectation of privacy in smart cities IoT public environments?

- Is the traditional distinction between private and public places still viable in the context of IoT urban environments?
- Can the distinction between private and public places still be considered as a proxy to distinguish major and minor private life intrusions in smart cities IoT environments?
- From a criminal justice perspective, which procedural safeguards should be granted to individuals against investigatory acts performed on IoT devices by law enforcement officers in public places?

3 Objectives

The first research question aims to identify privacy, data protection and security issues arising from the systematic deployment of sensor-driven surveillance in smart cities. In this respect, a particular attention will be dedicated to the conditions enabling smart cities dwellers to give meaningful consent to the collection of their personal data in IoT public environments. The creation of a trust-based relationship between citizens and smart cities public bodies heavily relies on the development of a clear, organic set of rules governing the collection and processing of sensor data in the particular context of smart cities. That is why the final objective of this research project will be the proposition of a specific regulatory framework for sensorveillance (i.e. sensor-based surveillance) in European Smart Cities. Such new legal framework shall be inspired to the following guidelines:

- In its scope, it shall be applicable indiscriminately to public and private entities participating to the management of the smart city;
- It shall aim at overcoming traditional privacy legal tools inapt to tackle the new reality of sensor fusion [15] in smart cities;
- It shall draw on the systematic implementation of the principles of privacy by design[4] and data protection impact assessments[5] in the design of smart cities infrastructure;
- From a criminal justice perspective, it shall provide for homogeneous safeguards for access and re-use of IoT-generated data, regardless of the private or public nature of the storing database;
- It shall provide for effective remedies against the dangers of fully automated processing of big urban data, thus enabling citizens to exercise a control over the decisions of smart cities public bodies.

As a starting point, we have acknowledged that the current EU data protection framework remains unclear on which legal ground may lawfully serve as viable basis for data processing operations in smart urban environments. In these instances, anchoring data collection to users' consent may be problematic, as city authorities may have a legitimate interest in not revealing the exact positioning of the sensors embedded in the infrastructure (e.g. for security reasons, or due to potential re-use of sensor data in the law enforcement sector). Also, urban data collection may not be grounded on a legitimate interest of the data controller[6], since this particular legal basis is not applicable to data collection performed by public authorities. On the other hand, the wording of art. 5(3) the Direc-

[4] Article 25 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) (Official Journal L 119, 4.5.2016, pp. 1 – 88).

[5] Article 35 of the GDPR.

[6] Art. 6(1)(f) of the GDPR.

tive 2002/58/EC[7] – which constitutes a lex specialis in relation to the GDPR – appears to be too obsolete to include in its scope the wide variety of sensors embedded in smart city infrastructure [6]. Arguably, the approval of the new e-Privacy regulation will further change the legal landscape for data processing operations in IoT environments. Against this background, this research project will aim at identifying the legal grounds that – nowadays or in the foreseeable future – may provide for practicable solutions to legitimise data processing in smart urban environments.

Furthermore, this project will seek to address the issues stemming from the growing re-use of publicly and privately-held data in the law enforcement context. Our analysis will follow the guidelines of the recent European strategy for data[8], which submits data transfers from the private sector to law enforcement agencies to general privacy and data protection norms (i.e. prior authorisation by a judge or other independent authority). On the other hand, when re-purposed data was initially stored by other public bodies, the Open Data Directive applies. In this case, however, access to data may be granted to law enforcement only when necessary and proportionate. Taking all of this into consideration, the prospective regulatory framework will lay out appropriate rules to align, as much as possible, data protection safeguards surrounding law enforcement's access of both privately and publicly-held data.

The prospective regulatory framework will seek to provide the best practices and mechanisms that can ensure the accountability of public authorities relying on algorithmic processing of big urban data. Accountability of public authorities should be fostered in three key moments. Firstly, we will focus on the ex ante approaches which may facilitate a prospective legal review of the decisions taken by automated systems operating in the city. When feasible, proposed solutions may involve transparency in technological processes and services (e.g. in the case of open technologies and software). Secondly, we will centre our analysis on ex post remedies which shall be made available to citizens against fully automated processing of their personal data carried out by public authorities. Thirdly, on a more general level, we will advocate the establishment of an audit commission which shall periodically review the performance of automated systems that are at the core of the smart projects implemented throughout the city. Due to the wide variety of the issues concerned, this regulatory body should be multidisciplinary in its composition, involving ethicists, legal experts, political and

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal L 201, 31.7.2002, p. 37–47.

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 19th Feb. 2020, *A European Strategy for data*, COM(2020)66.

citizens' representatives, technicians.

A new regulatory framework for sensorveillance in European Smart Cities should also be anchored to a thorough rethinking of the historic distinction between private dwellings and public venues [21]. To this purpose, the second research question aims at investigating the possibility of creating a new legal categorisation for private-public (IoT) places in smart cities. The theorisation of a new legal framework for smart cities IoT environments shall be focused on the parameter of the reasonable expectation of privacy of urban dwellers, rather than on the public or private nature of the venue in question.

4 Methodology

In order to attain the proposed objectives, this research will combine an interdisciplinary [2] and a comparative approach.

First of all, we will rely on scholarly writings of different academic fields, e.g. ICT law, privacy and data protection law, criminal law, urban studies and surveillance studies. We will also embrace the traditional doctrinal legal method, by carrying out an integrated legal analysis of the EU privacy and data protection legislation, as well as of different regulatory instruments adopted by certain European smart cities (e.g. Barcelona). The review of the current positive law will be combined with an in-depth analysis of the European Court of Justice (ECJ) and the European Court of Human Rights (ECtHR)'s case law relevant for the fields of privacy and data protection. Throughout the lead-time of implementation of this project, a particular attention will be dedicated to the latest technological advancements offering the best privacy-enhancing solutions for IoT environments in smart cities. As highlighted by Gasser, contemporary approaches to privacy law need to rethink the role of technology, which should be no longer regarded as a threat to privacy, "but as a part of the solution space" [10].

When re-defining the framework for private and public places in smart cities, we will also draw on a comparative approach, taking into consideration the case-law of United States judicial bodies (in particular of the United States Supreme Court, USSC) and European supranational Courts, i.e. the European Court of Human Rights (ECtHR) and the ECJ. Indeed, the casuistic, empirical approach adopted by these courts is suitable to deal with the ever-changing legal issues emerging from the deployment of new surveillance technologies [28]. In particular, the USSC case-law concerning the scope of Fourth Amendment safeguards in the contemporary technological framework may be useful in analysing the concepts of consent and expectation of privacy in IoT environments[9] [12]. From

[9] *Carpenter v. United States*, U.S., No. 16-402 (2017).

a European perspective, we will investigate if the current state of the ECtHR's case-law provides for the need of a reasonable expectation of privacy even in smart cities public places[10].

From an evaluative standpoint, this research will adopt an abductive, case-based approach in assessing whether current smart cities policies and European legal standards are apt to the task of upholding privacy and data protection standards in IoT environments. On the one hand, the analysis of existing public policies in European and American smart cities will mainly rely on empirical qualitative research methods [4]. On the other, the review of the EU privacy and data protection framework will be primarily focused on the issues arising from the contextual and relational nature of algorithmic data processing techniques employed in big urban data environments. Because the importance of contexts has been highly stressed in privacy literature [24], we should thoroughly examine the features and dynamics of the urban settings where IoT surveillance practices take place.

Subsequently, the normative framework that will inspire the development of a regulatory system for sensorveillance in smart cities will take into account the criterion of proportionality – pivotal in European teleological legality [22] – as well as the ethical values of equality, security, social justice and trust between citizens, smart cities public authorities and IoT technologies deployed in the urban scenario. Those principles shall indeed be considered crucial in ensuring an anthropocentric development of the peculiar social setting of smart cities. On the whole, our normative approach will be grounded on the acknowledgment that the implementation of IoT solutions is deeply rooted in current policies for urban development, and it is only likely to be fostered in the future [20]. Therefore, our normative solutions shall focus on coherent, fair and humane approaches to emerging legal and ethical issues, without aiming at banning ground-breaking technologies that may contribute to the resilience and sustainability of the smart cities of the future.

5 Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD "Law, Science and Technology Rights of Internet of Everything" grant agreement No 814177.

[10] On the European side, a number of decisions of the ECtHR also deal with the issue of extending, on certain conditions, privacy protection in public places. Among most recent decisions, see inter alia ECtHR, 28 November 2017, *Antović and Mirković v. Montenegro*, Application no. 70838/13, §§41-43.

References

1. Albino Vito, Berardi Umberto and Dangelico Rosa Maria. "Smart Cities: Definitions, Dimensions, Performance, and Initiatives." *Journal of Urban Technology* 22, no. 1 (2010):3-21.
2. Bibri, Simon Elias. *Smart Sustainable Cities of the Future: The Untapped Potential of Big Data Analytics and Context–Aware Computing for Advancing Sustainability.* Springer, 2018.
3. Bosco Francesca, Creemers Niklas, Ferraris Valeria, Guagnin Daniel and Koops Bert-Jaap. "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities." In *Reforming European Data Protection Law. Law, Governance and Technology Series*, edited by Gutwirth Serge, Leenes Ronald, De Hert Paul, 3-33. Springer, 2015.
4. Burton, Mandy. "Doing Empirical Research." In *Research Methods in Law*, edited by Watkins Dawn and Burton Mandy, 66-86. London: Routledge, 2013.
5. Calvo, Patrici. "The Ethics of Smart Cities (EoSC): Moral Implications of Hyperconnectivity, Algorithmization and the Datafication of Urban Digital Society." *Ethics Inf Technol* (2019) (https://doi.org/10.1007/s10676-019-09523-0).
6. Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." *Eur. Data Prot. L. Rev.* 2, no. 1 (2016):28-58.
7. Esposito Christian, Castiglione Aniello, Frattini Flavio et al. "On Data Sovereignty in Cloud-Based Computation Ofoading for Smart Cities Applications." *IEEE Internet of Things Journal*, 6, no. 3 (2019):4521-4535.
8. Ferguson, Andrew Guthrie. "Big Data Surveillance: The Convergence of Big Data and Law Enforcement." In *The Cambridge Handbook Of Surveillance Law*, edited by Gray David, Henderson E. Stephen, 171-197. Cambridge University Press, 2017.
9. Friedland, Steven I. "The Internet of Things and Self-Surveillance Systems." In *The Cambridge Handbook Of Surveillance Law*, edited by Gray David, Henderson E. Stephen, 198-224. Cambridge University Press, 2017.
10. Gasser, Urs. "Recoding Privacy Law: Reflections on the Future Relationships among Law, Technology and Privacy." *Harv. Law Rev.* 130, no. 2 (2016):61-70.
11. Gifnger Rudolf, Fertner Christian, Kramar Hans et al. "Smart Cities: Ranking of European Medium-sized Cities." Accessed 11 Oct 2019. http://www.smart-cities.eu/download/smart_cities_final_report.pdf.
12. Gray, David, eds. *The Fourth Amendment in the Age of Surveillance.* Cambridge University Press, 2018.
13. Gutwirth Serge and Hildebrandt Mireille. "Some Caveats on Profiling." In *Data Protection in a Profiled World*, edited by Gurtwirth Serge, Poullet Yves, de Hert Paul, 31-42. Springer, 2010.
14. De Hert Paul, Parlar Cihan, Thumfart Johannes. "Legal Arguments Used in Courts Regarding Territoriality and Cross-border Production Orders: From Yahoo Belgium to Microsoft Ireland." *NJECL* 9, no. 3 (2018):326-352.
15. Hiller Janine S. and Blanke Jordan M. "Smart Cities, Big Data, and the Resilience of Privacy." *Hastings L.J.* 68, no. 2 (2017):309-356, 312.
16. Jin Jiong, Gubbi Jayavardhana, Marusic Slaven et al. "An Information Framework for Creating a Smart City Through Internet of Things." *IEEE Internet of Things Journal* 1, no. 2 (2014):112-121.
17. Kitchin, Rob. "Data-Driven, Networked Urbanism." Accessed 30 Oct 2019. https://ssrn.com/abstract=2641802.

18. Kitchin, Rob. "The Ethics of Smart Cities and Urban Science." *Phil. Trans. R. Soc. A* 374:20160115.
19. Kitchin, Rob. "Data-driven urbanism." In *Data and the City*, edited by Kitchin Rob, Lauriault Tracey P., Mc Ardle Gavin, 44-56. Routledge, 2017.
20. Kitchin Rob and Dodge Martin. "The (In)security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention." *Journal of Urban Technology* 26, no. 2 (2019):47-65.
21. Koops, Bert-Japp. "On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy." *Politica e Società* 3, no. 2 (2014):247-264.
22. Kostoris, Roberto E. "European Law and Criminal Justice." In *Handbook of European Criminal Procedure*, edited by Kostoris E. Roberto, 3-66. Springer, 2018.
23. Kroll Joshua A., Huey Jordan, Barocas Solon et al. "Accountable Algorithms." *Univ. Pa. Law Rev* 165 (2017):633-699.
24. Nissenbaum, Helen. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford: Stanford Law Books, 2010.
25. Peppet, Scott R. "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent." *Tex. L. Rev.* 93 (2014):85-176.
26. Strous Leon and IFIP Domain Committee on IoT. "IoT: Do we have a Choice? Draft IFIP Position Paper." In *Internet of Things. Information Processing in an Increasingly Connected World. Proceedings of the First IFIP International Cross-Domain Conference, IFIPIoT 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18-19, 2018*, edited by Strous Leon and Cerf G Vinton, 50-56. Springer, 2018.
27. Vedder Anton and Naudts Laurens. "Accountability for the Use of Algorithms in a Big Data Environment." *International Review of Law, Computers and Technology* 31, no. 2 (2017):206-224.
28. Washington Micheal and Richards Neil. "Digital civil Liberties and the Translation Problem." In *The Oxford Handbook of Criminal Process*, edited by Brown Darryl K., Turner Jenia Iontcheva, Weisser Bettina. Oxford University Press, 2019. (doi: 10.1093/oxfordhb/9780190659837.013.20).
29. Woo, Jesse. "Smart Cities Pose Privacy Risks and Other Problems, But That Doesn't Mean We Shouldn't Build Them." *UMKC L. Rev.* 85, no. 4 (2017):953-972.