

# Smart City as Safe City: From False Social Promises to True Surveillance and Discrimination\*

Céline Castets-Renard

(Professor, University of Ottawa, Civil Law Faculty, Canadian Research Chair Holder on International and Comparative AI Law)

---

**ABSTRACT:** Dubai, Singapore, Sydney, Amsterdam, Barcelona, and Toronto all exemplify the trend of developing into "smart cities" - urban areas that leverage information and communication technologies to improve quality of life and promote sustainable development. While definitions vary, smart cities are generally seen as combining technological, human, and institutional dimensions to address urban challenges through innovation, efficiency, and citizen participation. However, after an initial wave of enthusiasm in the early 2010s, interest in smart city projects has waned due to high costs, limited effectiveness, and implementation difficulties, often falling short of citizens' expectations. As a result, many initiatives have been scaled back or abandoned. Meanwhile, surveillance and security technologies have become the dominant - though narrower - application of smart city tools, shifting the focus toward "safe cities" and prompting critical reflections on the social impacts of such technologies, particularly on vulnerable populations.

---

**KEYWORDS:** Smart city, safe city - AI and surveillance - Surveillance in public space - Women and Surveillance

---

**TABLE OF CONTENTS:** 1. Introduction. – 2. Paradigm Shift: from the Concept of Smart City to Safe City. – 2.1. Smart Cities as Data Cities and Infrastructure Cities. – 2.2. Smart city as Surveillance City. – 2.3. Inherent Potential of Surveillance. – 2.4. Safe City as Smart City: Marketing for a Better Social Acceptability. – 3. Impact on Citizens: A Need for Transparency and Inclusivity of the "Smart Safe City". – 3.1. Impact on Citizens: Challenges to Democracy and Human Rights. – 3.2. A Need for More Policies, Transparency and Inclusivity. – 3.3. Impact on Women: Gendering the Smart city. – 4. Conclusion: Lessons Learned.

---

## 1. Introduction

What do Dubai,<sup>1</sup> Singapore,<sup>2</sup> Sydney,<sup>3</sup> Amsterdam,<sup>4</sup> Barcelona,<sup>5</sup> Toronto<sup>6</sup> have in

---

\* Article submitted to double-blind peer review.

<sup>1</sup> F. Salem, *A Smart City for Public Value: Digital Transformation Through Agile Governance - The Case of 'Smart Dubai'*, World Government Summit Publications, 2016. Available at SSRN: <https://ssrn.com/abstract=2733632>.

<sup>2</sup> Singapore developed Virtual Singapore, a dynamic 3D city model and collaborative platform supporting city stakeholders in driving innovation.

<sup>3</sup> R. Dowling, P. McGuirk, S. Maalsen and J. Sadowski, *How smart cities are made: A priori, ad hoc and post hoc drivers of smart city implementation in Sydney, Australia*, in *Urban Studies*, vol. 58, n. 16, 2021, 3299.

<sup>4</sup> L. Taylor, C. Richter, S. Jameson and C. Perez del Pulgar, *Customers, users or citizens? Inclusion, spatial data and governance in the smart city*, Report, University of Amsterdam, 2016.

<sup>5</sup> I. Capdevila and M. Zarlenga, *Smart City or Smart Citizens? The Barcelona Case*, in *Journal of Strategy and Management*, vol. 8, n. 3, 2015, 266.

<sup>6</sup> T. Scassa, *Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto*, in *Technology & Regulation*, vol. 2, 2020, 44; T. Scassa, *Innovation ahead of Legal Change: The Case of Sidewalk Toronto*, in C. Castets-Renard and J. Eynard (eds.), *Artificial Intelligence Law: Between Sectoral Rules and Comprehensive Regime Comparative Law*, Bruylant, 2023, 533; E. Goodman and J. Powles, *Urbanism Under Google: Lessons from Sidewalk Toronto*, in *Fordham Law Review* vol. 88, Issue 2, 2019, 457.

common? In different ways, all these cities are or have been engaged in the process of becoming "smart cities". For several years now, many urban policies have focused on "smart city" projects. While there is no single definition of a "smart city" is,<sup>7</sup> it is generally understood that 'smart' urban policies involve local government initiatives that leverage information and communication technologies to improve residents' quality of life while promoting sustainable development.<sup>8</sup> Enhancing quality of life and fostering sustainability<sup>9</sup> are the core objectives of these projects. Other scholars<sup>10</sup> define a smart city

---

<sup>7</sup> For some authors, this is an "unsettled debate": M. Ziosi, B. Hewitt, and P. Juneja, M. Taddeo and L. Floridi, *Smart Cities: Reviewing the Debate about their Ethical Implications*, in *AI & Society*, vol. 39, 2024, 1185.

<sup>8</sup> I. Capdevila and M.I. Zarlenga, *Smart City or smart citizens? The Barcelona case*, in *Journal of Strategy and Management*, vol. 8, Issue 3, 2015.

<sup>9</sup> D. McLaren and J. Agyeman, *Sharing Cities: A Case for Truly Smart and Sustainable Cities*, MA, MIT Press, 2015.

<sup>10</sup> T. Nam and T.A. Pardo, *Conceptualizing smart city with dimensions of technology, people, and institutions*, in *Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times\_dg.o '11*, 2011, 282.

based on three dimensions: technologic, human and institutional. A more specific definition describes a smart city as “an urban area that uses digital technology to collect data and to operate/provide services.”<sup>11</sup>

Smart cities hold great promise, offering solutions to many urban challenges. By leveraging technology, cities can prioritize interactions and establish dynamic relationships, enabling the continuous identification and resolution of issues. Ultimately, smart technologies aim to make cities more efficient, sustainable, and beneficial for their residents.<sup>12</sup> Especially, urbanization’s growing trend is causing challenges in managing basic amenities and resources in urban areas, necessitating innovative solutions to ensure efficient functioning and improved quality of life for citizens.<sup>13</sup> According to the *International Telecommunication Union (ITU)*, a smart city “uses ICTs to improve people’s quality of life, make urban operations and services more efficient, and boost its competitiveness, while ensuring that it meets the economic, social, environmental, and cultural needs of present and future generations.”<sup>14</sup> However, the priorities of smart cities vary based on each country’s specific context. These priorities may include: “boosting energy efficiency, enhancing competitiveness, developing innovation technology, promoting open data solutions, and encouraging citizen participation.”<sup>15</sup>

In the early 2010s, both academic literature and public policies on smart cities were largely optimistic. However, interest began to decline toward the end of the decade and has continued to wane since. Many reasons can be raised to explain this decline, especially regarding the cost and the (in)efficiency of

such tools. The reality and the literature have shown that many expectations, probably too numerous and too high, have not been met, because the tools turned out to be “unintelligent”,<sup>16</sup> too costly or even not so easy to implement.<sup>17</sup> Moreover, the promises of digital innovation in smart cities have not been fully kept, especially from the perspective of citizens’ needs.<sup>18</sup> This has led to widespread discouragement in many cities around the world, some of which have abandoned their projects due to the difficulties of implementation or the lack of proper preparation.<sup>19</sup> However, amid this downturn, surveillance tools have emerged as the most prominent yet narrow application of smart city initiatives, primarily centered on security. This paradigm shift marks a transition from the concept of a “smart city” to a “safe city,” prompting a reevaluation of these frameworks (section 2). Additionally, the rise of safe cities raises important questions about the social impact of technology on citizens, particularly on vulnerable populations (section 3).

## 2. Paradigm Shift: from the Concept of Smart City to Safe City

### 2.1. Smart Cities as Data Cities and Infrastructure Cities

Smart cities are defined by how their local governments monitor, analyze, plan, and manage urban spaces. At the core of this approach is data. Data is collected from a variety of sources, including from citizens (mostly personal data), devices, buildings, and surveillance cameras. Moreover, the applications of smart city technologies are extensive, spanning areas such as traffic and transportation systems, utilities, urban forestry, water supply networks, waste management, education, healthcare, public services, criminal investigations, and

<sup>11</sup> P. James, R. Astoria, T. Castor, Ch. Hudspeth, D. Olstinske and J. Ward, *Smart Cities: Fundamental Concepts*, in *Handbook of Smart Cities*, New York, Springer International Publishing, 2020, 1.

<sup>12</sup> O. Oladeji Olaniyi, O.J. Okunleye and S.O. Olabanji, *Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature*, in *Current Journal of Applied Science and Technology*, vol. 42, Issue 25, 2023, 10.

<sup>13</sup> O. Oladeji Olaniyi *et al.*, see note 12.

<sup>14</sup> International Telecommunication Union (ITU), available at: [www.itu.int/en/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx](http://www.itu.int/en/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx).

<sup>15</sup> K. Sungjin, *The Development of Smart Cities and the Korean Smart City Model*, in *KIET Industrial Economic Review*, vol. 23, n. 2, 2018, 35.

<sup>16</sup> S. Goldsmith, *As the Chorus of Dumb City Advocates Increases, How Do we Define the Truly Smart City?*, in [datasmart.ash.harvard.edu](http://datasmart.ash.harvard.edu), 2022.

<sup>17</sup> O. Oladeji Olaniyi *et al.*, see note 12.

<sup>18</sup> M.E. Cortés-Cediel *et al.*, *Analyzing Citizen Participation and Engagement in European Smart Cities*, in *Social Science Computer Review*, vol. 39, n. 4, 2021, 592.

<sup>19</sup> Sidewalk Toronto is one of the most famous failures of a smart city. This urban development project was proposed in 2017 by Sidewalk Labs (involving Alphabet) at Quayside in Toronto (Canada) and was cancelled in 2020. The project drew criticism, particularly over data privacy issues regarding the huge data collection from the community.

information systems. Therefore, the primary and most significant concern related to the deployment of smart cities lies in the collection of vast amounts of personal data and the potential risk to privacy.<sup>20</sup> In most cases, the data subjects are neither informed nor asked for their consent. In European Law, under the General Data Protection Regulation (GDPR),<sup>21</sup> the legal basis is more likely to rely on “the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller” (GDPR, art. 6(1)(e)). The basis for this processing shall be laid down by Union law or Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR, art. 6(3)). These provisions refer to the core principles governing the processing of personal data, including the principles of lawfulness, fairness, and transparency, as well as purpose limitation and data minimization (GDPR, art. 5). However, the information and transparency of legislative measures taken at the national or European level on these legal bases are most of the time neither well known nor clearly communicated to citizens

Furthermore, in a smart city, data sharing extends to businesses, citizens, and other third parties who can benefit from accessing and using this information.<sup>22</sup> As a result, one of the defining features of smart cities is the unprecedented volume and variety of data generated and collected through digital technologies.<sup>23</sup> Many cities rely on information and communication technologies (ICTs), for example, to improve areas such as energy efficiency, waste management,

housing, healthcare, traffic flow and safety, air quality monitoring, crime prevention, and the delivery of clean water and sanitation services.<sup>24</sup> The Internet of Things (IoT)<sup>25</sup> connects billions of devices and objects equipped with smart sensors, allowing them to communicate, collect real-time data, and transmit this information via wireless networks to centralized control systems.<sup>26</sup> Artificial intelligence (AI) makes it possible to analyze massive datasets, identifying patterns and trends, while big data analytics plays a key role in processing the vast amounts of information generated by smart city infrastructures, supporting the efficient management and successful implementation of smart city projects.<sup>27</sup> The European AI Regulation (AI Act)<sup>28</sup> governs the use of artificial intelligence based on a risk classification system. However, the use of AI for analyzing and processing data collected as part of smart city operations is not considered high-risk and therefore does not fall within the scope of this regulation.

## **2.2. Smart city as Surveillance City**

Among the many objectives attributed to smart cities, functions such as alerting police to crimes in real time, predictive policing, and surveillance of public spaces through cameras are not typically the most emphasized. While enhancing safety can certainly contribute to improving residents’ quality of life - a core aim of smart cities - other priorities have generally taken precedence, such as optimizing traffic management, overseeing water and energy use, and improving waste collection. Given the wide range of possibilities and goals associated with smart cities, there was little reason to assume that security and surveillance would become primary focuses. The shift from smart city to safe city was neither a necessity nor a matter

<sup>20</sup> L. Edwards, *Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective*, in *European Data Protection Law Review*, vol. 2, Issue 1, 2016, 28; K. Finch and O. Tene, *Smart Cities: Privacy, Transparency, and Community*, in E. Selinger, J. Polonetsky and O. Tene (eds.), *Cambridge Handbook of Consumer Privacy*, 2018, 125.

<sup>21</sup> Regulation (EU) No. 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, OJ L 119, 4.5.2016, 1-88.

<sup>22</sup> S. Paiho, P. Tuominen, J. Rökman, M. Ylikerälä, J. Pajula and H. Siikavirta, *Opportunities of collected city data for smart cities*, in *IET Smart Cities*, vol. 4, n. 4, 2022, 275.

<sup>23</sup> James *et al.*, see note 11.

<sup>24</sup> ITU, see note 14.

<sup>25</sup> ITU, see note 14. IoT referring to the network of rapidly growing computing devices with built-in sensors and software to connect with each other and share data.

<sup>26</sup> ITU, see note 14.

<sup>27</sup> O. Oladeji Olaniyi *et al.*, see note 12.

<sup>28</sup> Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) No. 2018/858, (EU) No. 2018/1139 and (EU) No. 2019/2144 and Directives No. 2014/90/EU, (EU) No. 2016/797 and (EU) No. 2020/1828, OJ L, 2024/1689, 12 July 2024.

of course. Yet, *International Data Corporation* (IDC)<sup>29</sup> published the type of tools that have been implemented the most. The three largest sources of spending associated with smart cities as of 2022 were visual surveillance (Closed-circuit television (CCTV)), also known as video surveillance, public transit,<sup>30</sup> and outdoor lighting.<sup>31</sup> More broadly, scholars like Murakami Wood and Mackinnon have described smart cities as “urban surveillance platforms,”<sup>32</sup> highlighting how surveillance infrastructure increasingly underpins their operation.

In some cases, the trajectory has been reversed, with cities evolving from a focus on safety toward broader smart city functions. Johannesburg, for example, has pursued a model where authorities first establish a safe city framework and then expand its capabilities to develop into a smart city.<sup>33</sup> In this view, safety is treated as the foundation of the smart city, with surveillance data serving multiple administrative purposes beyond security.

### 2.3. Inherent Potential of Surveillance

Some scholars have identified four key ethical concerns arising from the development of smart cities: (1) network infrastructure, raising issues of control, surveillance, data privacy and ownership; (2) post-political governance, reflecting tensions between public and private decision-making and the depoliticization of urban management; (3) social exclusion, inequality and discrimination; and (4) sustainability, focusing

<sup>29</sup> Business wire, *IDC Forecasts Smart Cities Spending to Reach \$158 Billion in 2022, with Singapore, Tokyo, and New York City Among Top Spenders*, available at: [www.businesswire.com](http://www.businesswire.com).

<sup>30</sup> M. Kumar, N. Kumari, S. Tomar and T. Kumar, *Smart Public Transportation for Smart Cities*, in *International Conference on Advances in Engineering Science Management & Technology (ICAESMT)*, Uttaranchal University, Dehradun, India, 2019, available at SSRN: <https://ssrn.com/abstract=3404487>.

<sup>31</sup> L. Nethravathy, K. Harshitha, S. Khan R.S., N. Vishal, M.R. Pooja and M. Meghana, *Intelligent Street Lighting System for Smart City*, in *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*, 2021, available at SSRN: <https://ssrn.com/abstract=3833878>.

<sup>32</sup> D. Murakami Wood and D. Mackinnon, *Partial Platforms and Oligoptic Surveillance in the Smart City*, in *Surveillance & Society*, vol. 17, n. 1/2, 2019, 176.

<sup>33</sup> M. Kwet, *City Surveillance State: Inside Johannesburg's Safe City Initiative*, in *South African Institute of International Affairs*, 2022, 3.

not only on protecting the environment but also on its strategic role in the future.”<sup>34</sup> Beyond the well-known privacy risks, the potential for surveillance is closely tied to the very foundation of smart cities - their network infrastructure and the constant collection of data. In this context, the rise of surveillance practices is not unexpected, as the technological framework enabling such monitoring has been embedded in smart city systems from the outset.

“Safe cities are a new trend that often form part of a wider effort to transform urban areas into ‘smart cities.’”<sup>35</sup> According to PWC (PriceWaterhouse Coopers), “a safe city could be defined as a system in place that ensures that citizens, business and properties, organisations and institutions are safe from both external and internal threats to their well-being.”<sup>36</sup> The concept of safe cities has historical roots in innovations like CompStat (Comparative Statistics) a police management system introduced by the New York City Police Department (NYPD) in 1994.<sup>37</sup> CompStat relies on continuously updated digital crime records to track and respond to incidents in real time. As Sadowski and Pasquale note, “when urban infrastructures are rigged with networks of surveillance, sensors, and algorithms, the ability for police forces to monitor city spaces and mobilize action is enhanced.”<sup>38</sup> In many cases, the infrastructure and data systems needed to support these safety functions are already embedded within smart city technologies, making the transition to safety-focused applications both seamless and readily available. Elizabeth Joh takes the analysis a step further, considering that: “policing is inherent to the smart city”.<sup>39</sup>

### 2.4. Safe City as Smart City: Marketing for a Better Social Acceptability

While the political dimensions of smart

<sup>34</sup> M. Ziosi *et al.*, see note 7.

<sup>35</sup> M. Kwet, see note no. 33.

<sup>36</sup> PriceWaterhouse Coopers (PWC), *Safe Cities: The India Story*, in *The Associated Chambers of Commerce and Industry of India (ASSOCHAM)/PWC*, New Delhi, India, 2013.

<sup>37</sup> A.G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race and The Future of Law Enforcement*, New York, NYU Press, 2017, 29.

<sup>38</sup> J. Sadowski and F. Pasquale, *The spectrum of control: A social theory of the smart city*, in *First Monday*, vol. 20, n. 7, 2015.

<sup>39</sup> E.E. Joh, *Policing the Smart City*, in *International Journal of Law in Context*, vol. 15, n. 2, 2019, 177.

cities often remain overlooked,<sup>40</sup> the optimistic and utopian narrative surrounding the “smart city” is increasingly being leveraged to promote the concept of the “safe city,” using similar language that can be misleading. Rather than emphasizing *surveillance technologies* directly, the focus shifts to the notion of the *safe city*, presented as a natural extension of the smart city. With the implementation of smart cities, adopting the safe city concept becomes seamless, as the elements that contribute to ‘smartness’ also play a crucial role in achieving the desired safety objectives.<sup>41</sup> In this way, the safe city benefits from the broad social acceptance and positive image already associated with smart cities. Although the idea of a safe city more accurately reflects the reality of surveillance-driven technologies, its language remains deliberately positive, drawing on shared values like innovation, efficiency, and public well-being, much like the smart city itself. While the term “safe city” may lack a precise or robust definition, it serves as an effective tool to promote and legitimize the expansion of technology-driven policing and security measures.

As a result, the expansion of surveillance systems within ‘smart’ initiatives, further amplified by advanced analytics, alters the political and economic landscape of urban life.<sup>42</sup> The rise of safe cities, either as a replacement for or an extension of smart cities, profoundly shifts the promises made to citizens.

### **3. Impact on Citizens: A Need for Transparency and Inclusivity of the “Smart Safe City”**

#### **3.1. Impact on Citizens: Challenges to Democracy and Human Rights**

Akbari highlights the growing need to scrutinize the influence of socio-political structures in shaping urban technologies and policies, criticizing the rise of the “authoritarian smart city”.<sup>43</sup> One notable development is the increasing role of closed-circuit television (CCTV), which is now

emerging as a kind of “fifth utility” alongside gas, electricity, water, and telecommunications.<sup>44</sup> As Akbari points out, once CCTV systems are in place, their expansion becomes almost inevitable due to the strong economies of scale involved.<sup>45</sup> While CCTV and data analytics are considered “nonviolent” and often perceived as subtle, benign, or unobtrusive,<sup>46</sup> their impacts are far from negligible. Sadowski and Pasquale observe that while smart city technologies may reduce the physical violence of controlling protests, they make the suppression of collective action more precise, effective, and potentially more coercive.<sup>47</sup>

Clearly, the technology employed for surveillance in safe cities undermines fundamental rights and freedoms, including the right to privacy (art. 7 of the Charter of Fundamental Rights of the EU), the right to data protection (art. 8 of the Charter), the freedom of expression and information (art. 11 of the Charter), freedom of speech, freedom of assembly and of association (art. 12 of the Charter),<sup>48</sup> even if the right to security of person (art. 6 of the Charter) should also be protected. According to Allam, the contemporary concept of smart cities, combined with the idea of safe cities, raises concerns about privacy and good governance.<sup>49</sup> Data protection, low citizen engagement, and the disproportionate influence of private companies are also critical issues,<sup>50</sup> that can weaken democratic governance.<sup>51</sup>

A safe city project can be perceived as a government strategy to capture private data

<sup>40</sup> A. Akbari, *Authoritarian Smart City: A Research Agenda*, in *Surveillance & Society*, vol. 20, n. 4, 2022, 441.

<sup>41</sup> P. Doyle, *Making Smart Cities into Safe Cities*, available at: <https://gcn.com/articles/2016/10/11/safesm-art-cities.aspx>.

<sup>42</sup> J. Sadowski and F. Pasquale, see note no. 38.

<sup>43</sup> A. Akbari, see note no. 40.

<sup>44</sup> S. Graham, *CCTV: The stealthy emergence of a fifth utility?*, in *Planning Theory & Practice*, vol. 3, n. 2, 2002, 237.

<sup>45</sup> J. Sadowski and F. Pasquale, see note no. 38.

<sup>46</sup> D. Murakami Wood, W.C. William and R. Webster, *Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain’s Bad Example*, in *Journal of Contemporary European Research*, vol. 5, n. 2, 2009, 259.

<sup>47</sup> J. Sadowski and F. Pasquale, see note no. 38.

<sup>48</sup> M. Kwet, see note no. 33.

<sup>49</sup> A. Zaheer, *The Emergence of Anti-Privacy and Control at the Nexus between the Concepts of Safe City and Smart City*, in *Smart Cities (Basel)*, vol. 2, n. 1, 2019, 96.

<sup>50</sup> J. Sadowski and R. Bendor, *Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary*, in *Science, Technology, & Human Values*, vol. 44, n. 3, 2019, 540.

<sup>51</sup> E.P. Goodman, *Smart City Ethics: The Challenge to Democratic Governance*, in M.D. Dubber, F. Pasquale, and S. Das (eds.), *The Oxford Handbook of Ethics of AI*, 2020, 823.

and impose control.<sup>52</sup> It can also be seen as a means of managing risks by implementing pre-emptive practices in law enforcement and public surveillance, such as in the areas of mental health and addiction care.<sup>53</sup> Therefore, “the ‘precautionary culture’ itself risks encroaching on the freedoms of citizens, ultimately making cities less safe.”<sup>54</sup> In this perspective, the anticipating offenses can pose a significant threat to the respect of the presumption of innocence and right of defence, in violation of Article 48 of the Charter of Fundamental Rights of the EU.

### 3.2. A Need for More Policies, Transparency and Inclusivity

Until appropriate policies, standards and governance frameworks are established for both smart and safe cities, urban well-being will remain compromised.<sup>55</sup> Unsurprisingly, there is a growing demand for stronger data policies and state oversight regarding how private corporations use data and how personal data is shared across agencies and companies.<sup>56</sup> While initiatives are being taken to regulate data sharing and enable responsible data governance, such as the European Data Governance Act,<sup>57</sup> there is still a lack of concrete measures in place to protect and safeguard the aforementioned fundamental rights.

Furthermore, the United Nations Sustainable Development Goals (SDG) 11<sup>58</sup> advocates for making cities inclusive, safe, resilient and sustainable with a particular emphasis for the need to “provide access to safe and inclusive green and public spaces by 2030, provide universal access to safe,

inclusive and accessible, green and public spaces, in particular for women and children, older persons and persons with disabilities (Target 11.7)”. This goal means “ensuring that citizens, organisations, institutions, properties and shared identities and cultures are secured from any forms of threats.”<sup>59</sup> This call for increased inclusivity is particularly relevant, as surveillance tools have historically been used to target oppressed and marginalised communities.<sup>60</sup> The tendency of smart cities to exacerbate existing inequalities and social polarization have been widely criticized.<sup>61</sup>

### 3.3. Impact on Women: Gendering the Smart city

Women have historically been overlooked in the design of urban environments, as cities were primarily designed for and by men.<sup>62</sup> Saegert’s early studies in urban theory highlight the implicit principle of “masculine cities and feminine suburbs.”<sup>63</sup> As a result, women’s movements have often been confined to the domestic sphere, with barriers to accessing better-paying jobs due to inadequate public transportation, limited childcare services, and concerns about crime and harassment in public spaces.<sup>64</sup>

While more gender-sensitive urban planning policies are being implemented, cities grow ‘smarter’ with urban infrastructure and services and technology itself is gendered.<sup>65</sup> However, discussions concerning innovations of smart city solutions have been gender-neutral and there is little research on whether gender differences exist in how the smart city is planned and experienced.<sup>66</sup> Moreover, gendered studies of the smart city have narrowly focused on women’s safety. It

<sup>52</sup> A.S. Elmaghaby and M.M. Losavio, *Cyber security challenges in smart cities: Safety, security and privacy*, in *Journal of Advanced Research*, vol. 5, Issue 4, 2014, 491.

<sup>53</sup> W. de Jong and S. Litska, *Controlling Risks in the Safe City: The Rise of Pre-Emptive Practices in Law Enforcement, Public Surveillance and Mental Health and Addiction Care (1970–2020)*, in *Urban Studies*, vol. 58, n. 12, 2021, 2514.

<sup>54</sup> W. de Jong and S. Litska, see note no. 53.

<sup>55</sup> C. Maple, *Security and privacy in the internet of things*, in *Journal of Cyber Policy*, vol. 2, Issue 2, 2017, 155.

<sup>56</sup> A. Zaheer, see note no. 49.

<sup>57</sup> Regulation (EU) No. 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724, OJ L 152, 3.6.2022, 1- 44.

<sup>58</sup> UN Global sustainable development report, Retrieved from: <https://sustainabledevelopment.un.org/globalsdrep> or, 2015.

<sup>59</sup> A. Zaheer, see note no. 49.

<sup>60</sup> R. Benjamin, *Race After Technology Abolitionist Tools for the New Jim Code*, Cambridge, Polity, 2019.

<sup>61</sup> R. Holland, *Will the real smart city please stand up?* in *City*, vol. 12, n. 3, 2008, 303.

<sup>62</sup> Ch. Ji-in, Ch. Jeongsun, A. Hyunjin and Ch. Hye-Young, *Gendering the smart city: A case study of Sejong City, Korea*, in *Cities*, vol. 120, 2022, 103422; L. McDowell, *Towards an understanding of the gender division of urban space Environment and Planning, in D: Society and Space*, vol. 1, n. 1, 1983, 59.

<sup>63</sup> S. Saegert, *Masculine cities and feminine suburbs: Polarized ideas, contradictory realities*, in *Signs*, vol. 5, n. 3, 1980, S96.

<sup>64</sup> J. Beebejaun, *Gender, urban space, and the right to the everyday life*, in *Journal of Urban Affairs*, vol. 39, n. 3, 2017, 323.

<sup>65</sup> J. Wacjman, *Feminism confronts technology*, Polity, 1991.

<sup>66</sup> Ch. Ji-in *et al.*, see note no. 62.

is also necessary to question what a safe technological tool would be. CCTV cameras are the tools most frequently and easily used. It's a low-cost, low-complexity technology that can enhance a sense of security. For instance, according to a survey of South Korean citizens, CCTV cameras are the most-preferred measure for crime prevention in communities.<sup>67</sup> However, empirical studies on CCTV have yielded inconsistent results, and its effectiveness in preventing crime remains uncertain.<sup>68</sup> Another study conducted in the U.K. revealed that women are skeptical about the effectiveness of CCTV and favor the presence of security officers over cameras, while men tend to prefer CCTV over other forms of security.<sup>69</sup>

While a safer environment for women can be created through smart solutions (CCTV, safety bell, connection to the city integrated operation center, brighter lighting, etc.) that specifically target female safety,<sup>70</sup> Yang emphasized the ambivalence towards technology, framing its use as a binary choice between privacy and safety.<sup>71</sup> For instance, in Seoul, the city collects vast amounts of data on gender-based crimes, including the locations of single-women households and the frequency and locations of gender-based violent crimes. However, there is no clear plan for taking meaningful action after an incident is reported to ensure victim safety and prevent the abuse of collected data.<sup>72</sup> Additionally, the use of CCTV is built on the assumptions that such tool empowers yet over-victimize women. Finally, the use of technologies, like CCTV, ignores critical aspects of safety that are not directly observable, such as domestic violence and workplace abuse. Therefore, a

contradictory phenomenon arises regarding women: on one hand, there is a risk of excessive invasion of privacy in public spaces, while on the other, serious violence may remain invisible outside of these spaces. As a result, the smart city also carries risks of exclusion and discrimination against women, which is not surprising considering that such discrimination is already present both in urban policies and in technologies, particularly digital technologies. Therefore, the principle of equality and non-discrimination established in Article 21 of the Charter of Fundamental Rights of the European Union is not upheld. This creates inequalities that are not always recognized when implementing smart city policies.

#### 4. Conclusion: Lessons Learned

Firstly, public opinion, policymakers and some experts<sup>73</sup> have been too naïve to understand the positive aspects of the smart city, without considering the infinite surveillance potential of these ecosystems combining infrastructures and massive data collection tools, including personal data. The vocabulary used to designate *sensors*<sup>74</sup> and objects for managing *flows* such as water or traffic has taken on the appearance of neutrality, whereas all activities in a city are linked to human activity, whether individual or collective. The technology embedded in smart city does not only manage *objects* nor achieves *neutral* management activity. Moreover, the technological systems “absorb and reproduce the dominant cultural values of the contemporary political economy.”<sup>75</sup> As Akbari highlighted it “the smart city’s conceptualisation, governance, and implementation is inherently political and embedded within political systems that pursue authoritarian objectives.”<sup>76</sup> In this context, surveillance is becoming “normal” in Europe,

<sup>67</sup> S.J. Kang, J.E. Park and K.H. Lee, *An analysis for effect of crime preventive CCTV in residential areas through public opinion survey*, in *Journal of the Architectural Institute of Korea Planning and Design*, vol. 25, n. 4, 2009, 235.

<sup>68</sup> Ch. Joon Tag and J. Park, *Exploring the Effects of CCTV upon Fear of Crime: A Multi-Level Approach in Seoul*, in *International Journal of Law, Crime and Justice*, vol. 49, 2017, 35.

<sup>69</sup> M. Carter, *Gender Differences in Experience with and Fear of Crime in Relation to Public Transport. Research on Women’s Issues in Transportation*, vol. 2, Transportation Research Board, Washington DC, 2005, 100.

<sup>70</sup> Ch. Ji-in *et al.*, see note no. 62.

<sup>71</sup> Ch. Yang, *The Techno-Optics of Safety: Surveillance and Women’s Ambivalent Experiences in South Korea’s ‘Smart Safe City*, in *Science, Technology, & Human Values*, 2024.

<sup>72</sup> Ch. Yang, see note no. 71.

<sup>73</sup> But not all of them: see J. Sadowski and F. Pasquale, note 38.

<sup>74</sup> R. Nitin, C. Saurabh and R. Jayesh, *Artificial Intelligence (AI) and Internet of Things (IoT) – Based Sensors for Monitoring and Controlling, in Architecture, Engineering, and Construction: Applications, Challenges, and Opportunities*, 2023, available at SSRN: <https://ssrn.com/abstract=4642197> or <http://dx.doi.org/10.2139/ssrn.4642197>.

<sup>75</sup> T. Monahan, *Surveillance as governance: Social inequality and the pursuit of democratic surveillance*, in K.D. Haggerty and M. Samatas (eds.), *Surveillance and democracy*, New York, Routledge, 2010, 91.

<sup>76</sup> A. Akbari, see note 40.

led by the Britain case.<sup>77</sup> It is a key mode of organisation in contemporary capitalist nation-states, designated as “surveillance societies.”<sup>78</sup> Security is largely driven by the “surveillance capitalism”<sup>79</sup> and security technology companies exert significant influence on public policy.<sup>80</sup>

Secondly, beyond the well-known risks of surveillance, as well as threats to privacy and personal data protection, the smart city is also a source of exclusion and discrimination against women - a reality that is less recognized and therefore less addressed. This lack of awareness further weakens the position of women. However, conversely, when gender-specific risk factors are considered, it often results in increased surveillance of women without necessarily providing them with better protection. Ultimately, it is important to call out the use of the positive and appealing vocabulary of the smart city, which is often used to justify the widespread deployment of surveillance tools and security policies that refuse to name themselves as such. This lack of transparency is particularly troubling for society and, even more so, for historically marginalized and disadvantaged groups. This analysis serves as a call to resist the smart city model when it reveals itself to be a security-driven city with discriminatory effects.

---

<sup>77</sup> D. Murakami Wood and W.R. Webster, see note no. 46.

<sup>78</sup> D. Lyon, *The Electronic Eye: The Rise of Surveillance Society*, Minneapolis, University of Minnesota Press, 1994.

<sup>79</sup> S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs, 2019.

<sup>80</sup> For instance, these include Cisco, IBM, Microsoft, SAP, and Amazon Web Services in the U.S., Huawei in China, Schneider Electric in Germany.