smart cities

MDPI

Article

Privacy and Security Concerns in the Smart City

Brian F. G. Fabrègue [1,*] and Andrea Bogoni [2]

[1] Faculty of Law, University of Zurich, 8006 Zürich, Switzerland
[2] Department of Management, University of Bergamo, 24127 Bergamo, Italy
* Correspondence: brianfranco.fabregue@uzh.ch

Abstract: This article will highlight negative personal privacy and informational security outcomes that may arise from development programs currently pursued in smart cities. It aims to illustrate the ways in which the remedies proposed so far appear insufficient from a legal or practical standpoint, and to set forth a number of tactical approaches that could be used to improve them. Cities require spatial efficiency to address rising complexities, which can only be attained through an adequately efficient exchange of information among its citizens and administrators. Unprecedented volumes of private, public, and business data can now be collected, processed, and transmitted thanks to present technology. According to the authors' analysis of current trends in technology, data collection, legislation, and the related public acceptance in Italy and Switzerland, governments, corporations, employers, and individuals will increasingly experience hazard and damage given the ease at which tracking technologies can be abused. The study clarifies how significant data privacy and information protection are in the making of a successful smart urban community and provides insights on local Italian and Swiss policy makers' interest about digital innovation tied to the development of data protection.

Keywords: public administration reform; e-government; computer and society

Citation: Fabrègue, B.F.G.; Bogoni, A. Privacy and Security Concerns in the Smart City. *Smart Cities* **2023**, *6*, 586–613. https://doi.org/10.3390/smartcities6010027

Academic Editors: Catalin Vrabie, Teodora I. Bițoiu, Diana-Camelia Iancu and Pierluigi Siano

Received: 24 December 2022
Revised: 24 January 2023
Accepted: 8 February 2023
Published: 10 February 2023

1. Introduction

The traditional smart city development process adheres to the "god-dominant" paradigm, wherein both public and private strong organizations or individuals have complete control over the design of urban context sensing and actuation [1]. This is a top down method, structuring the discourse and practices. However, in the last few years, the dynamic underpinning of smart cities has undergone a drastic shift [2,3].

The emergence of private or associated stakeholders who position themselves between citizens and traditional stakeholders in the city's administration has caused the original smart city planning paradigm to evolve. This organizational make-up tends to move away from centralizing rationales and aim to reach an inventive balance between top-down and bottom-up approaches on the basis of field observations. The smart urban context is now more institutionally diverse and more iterative than planned.

The transport industry exemplifies it well: the use of data may optimize transit by eliminating journey connections and streamlining multi-mode transportation. Fundamentally, it is now possible to include the transport dimension as part of a broader perspective accounting for the interaction between the public transport offering, the use of other public services (e.g., childcare facilities, schools, hospitals) and people's professional and private lives. A district with a significant concentration of shift workers, for instance, may now receive transport solutions more suited to its needs [4].

The relationship between bottom-up agenda-setting and public policy takes centre stage in the sense that the information that communities are willing to share and political will on the part of authorities are powerful contributors to a city's smartness.

However, the quantification of human life through digital information is still dominated by economic actors for marketing or management purposes that can clash with

policy objectives. This use of data for profit can arguably objectivize neighbourhoods and infrastructure with adverse social ramifications and problematics [5–7]. The new institutional dynamic in smart cities can harness "datafication" to offset or regulate this effect; but overall, the flow of data modifies the policy vision of stakeholders.

Developing a smart city after this shift of dynamics means to multiply synergies and this implies a high level of organicity to multiply synergies. We believe that the current literature on privacy in smart cities lacks more of a pragmatic drive, which could become of great significance to both increase public awareness and directly influence policy makers, especially on a local scale. This can be achieved combining ethical and theoretical aspects with practical solutions and scenarios. Therefore, our research aims to be a tool for public policy enhancing by depicting the state of the art of smart city privacy both practically and philosophically, comparing current scenarios on a local scale and providing constructive suggestions.

This study highlights the negative impact that smart programmes have on personal privacy and information security. The collection, processing and transmission of large amounts of data in smart cities can lead to trade-offs between policy efficiency, business profitability, consumer convenience and personal privacy: this element has mostly been set aside by smart cities program designers. Our analysis of trends in technology, data collection, legislation and public acceptance in Italy and Switzerland shows how concern for users' privacy is not central to the smart city initiatives. Our analysis also provides insights for local policymakers on how to balance digital innovation and privacy. We aim to fill a research gap by highlighting the shortcomings of current solutions and proposing new approaches to improve them. Overall, the study highlights the importance of privacy and information protection for the success of smart and digital urban communities.

2. Urban Big Data and Smart Cities

Ever since data have been generated about cities, several types of data-informed urbanism have existed. Data have been utilized as the evidentiary base for establishing urban policies, programs and plans, tracking their performance and simulating future growth. The employed data are often sampled, generated ad hoc or occasionally and have a limited scope. Censuses, household, transport, environment and mapping surveys, as well as commissioned interviews and focus groups, are examples of such data, which are supplemented by various types of public administration records.

These databases are increasingly complemented by new forms of urban big data. Big data are fundamentally different from typical 'small' datasets in that they are generated and processed in real time, are exhaustive in scope, and have high resolution and granularity [8], for instance, collecting all the tap-ins and tap-outs of subscription cards on the underground, using automatic number plate recognition (ANPR)-enabled cameras to track all vehicles, and using sensors to monitor the mobile phone MAC addresses to track all pedestrians with a phone. It is easy to see how easy it is to collect large amounts of data on individuals in a smart city setting, and how these data can be used to track individuals' movements and locations.

This transition from slow and sampled data to fast and extensive data was made possible by the rollout of a slew of new, networked digital technologies implanted in the fabric of urban environments, which form the basis of the effort to construct smart cities. These technologies include digital cameras, sensors, transponders, meters, actuators, GPS and transduction loops that continuously monitor various phenomena and send data to a variety of control and management systems, such as city operating systems, centralized control rooms, intelligent transport systems, logistics management systems, smart energy grids and building management systems that can process and respond to the data flow in real time [9]. In addition, numerous smartphone applications and platforms for the sharing economy create a variety of real-time location, movement and activity data. In other words, there has been a considerable increase in what has been termed 'datafication' [10], that is, a substantial expansion in the volume, breadth and granularity of the data collected about

people and places [11]. Due to the fact that the data are digital, organized and stored in digital databases, they can be easily combined, shared and analysed utilizing data analytics.

The final result is a torrent of real-time, granular, contextual and actionable data created frequently by a variety of public and private organizations concerning cities and their residents.

As a consequence of the emerging data deluge, data-informed urbanism is being increasingly supplemented and replaced by data-driven urbanism (the mode of production of smart cities), and this is altering how we understand, plan and govern cities, both within and across specific domains (e.g., transport, environment, lighting, waste management) [12,13]. In fact, one of the effects of data-driven urbanism is that city systems and infrastructures are becoming significantly more interconnected and integrated. Urban operating systems, for instance, explicitly link several smart city technologies to provide improved coordination of municipal processes.

Similarly, urban operational centres and urban dashboards seek to aggregate and interconnect urban big data in order to provide synoptic smart city intelligence [14]. A locally relevant example is the Smart Control Room project in Venice, inaugurated in September 2020 in collaboration between the city council, the local police TIM and Venis SpA. It aims to improve mobility and security in the city by creating a model of urban intelligence through the use of sensors, information technology, telecommunications and, of course, 5G in particular [15].

TIM's Smart City Control Room solution allows local administrators to manage various city services in an integrated manner, including the intelligent management of lighting and waste collection, as well as mobility and security. Additionally, if necessary, data from the Control Room can be used and analysed to make decisions and intervene in real time.

While it is undeniable that the project is at the forefront of smart urban innovation and that it will most likely be an ingenious tool for trying to manage Venice's overwhelming tourist crowds, we would like to point out some of the unfavourable implications that characterise the "Control Tower" [16], as others have also already begun to note [17]. One of the first elements we would like to emphasise is the process of conceiving, studying and implementing this smart innovation. In particular, each of these steps was characterised by the traditional "god-dominant" paradigm [1]. In fact, the entire project was carried out only by large partners such as the city administration and the largest Italian telecommunications service provider, TIM. Despite the fact that regulating tourism is a need particularly felt by locals, many of the demands made by intermediate stakeholder groups did not penetrate the decision-making processes [18] and, to this day, there is still perplexity and uncertainty about privacy guarantees for citizens and tourists [19,20]. Another aspect of the story is directly linked to the progressive social and urban transformation of Venice, mainly due to economic drivers. Tourism is undoubtedly the main source of wealth for the city, but it has gradually changed its appearance: phenomena known as tourist monoculture and cosmopolitan consumption have turned the city into a giant hotel with annexed leisure activities [21]. Evidence of this systematic gentrification include, for example, the 500% increase in the number of hotel beds available between 2008 and 2019 [22]. To further control and limit access to the city in accordance with the Smart City Control Room, the Venice Pass will be introduced in 2023. It will be used to book and pay in advance for a special ticket to pass through the turnstiles that will be placed at main intersections [23].

In such a context, by adhering to a highly data-driven urban model and without appropriate clear privacy policies, Venice risks becoming more of a mechanical city, rather than an intelligent one.

2.1. Science/Informatics in the Smart City

There is a strong recursive relationship between data-driven urbanism and urban science/informatics, with the former supplying the raw material and applied domain and the latter offering the fundamental concepts and important tools for implementing smart city analytics and data-driven decision-making. Both urban science and urban

informatics advance knowledge on (i) how to handle and make sense of millions or billions of observations that are being generated dynamically [24] and (ii) how to translate the insight gained into new urban theory (fundamental knowledge) and actionable outcomes (applied knowledge) [25,26]. It is hypothesized that urban science/informatics has the possibility to reach for urban knowledge with higher breadth, depth, scale, and timeliness, and that is intrinsically longitudinal, in contrast to that acquired from older, more traditional urban research [24,27].

The urban science/informatics praxis adheres to a realist epistemology that assumes the existence of an external reality that functions independently of the observer and that can be objectively and accurately measured, monitored, statistically analysed and modelled. In other words, urban data can be unproblematically abstracted from the world in a neutral, value-free and objective manner, and are understood to be essential in nature, that is, they are fully representative of what is being measured (they faithfully capture its essence and are independent of the measurement process) [28].

This praxis promotes an instrumental logic that reinforces the assumption that cities can be steered and directed by a set of data levers and analytics, and urban concerns may be resolved via a variety of technology solutions [14,29,30]. Such a framing led to initial spatial and urban science being criticized for its alignment with positivist thinking and reductionism [31]. In addition, these theories neglected the relevance of politics, ideology, social structures, capital and culture in defining urban interactions, governance and development [32].

Urban science and urban informatics fail to recognize that cities are complex, multi-faceted, contingent, relational systems and full of contestation and wicked problems that are not easily captured or directed, and that urban issues are frequently best addressed through political/social solutions and citizen-centred deliberative democracy, as opposed to technocratic forms of governance [14,33].

As a result, computational and scientific approaches to smart cities produce a limited and limiting understanding of how cities function (limiting what kinds of questions can be asked and how they can be answered) and how they should be managed (limiting other forms of urban governance and other forms of knowledge, such as phronesis, experience-based knowledge and knowledge derived from practice and deliberation) [34]. The proponents of computational social and urban science counter that, in the era of big data, the variety, exhaustivity, resolution and relationality of data, as well as the growing power of computation and new data analytics, address some of the criticism, particularly those of reductionism and universalism, by providing more fine-grained, sensitive and nuanced analysis that can take context and contingency into account [8]. While contemporary urban science undoubtedly draws on positivist ideas [35,36], it is argued that data-driven science will become the new dominant mode of the scientific method in the age of big data because its epistemology is suited to exploring, extracting value and making sense of massive, interconnected data sets; it extracts additional, valuable insights that traditional knowledge-driven science would not be able to generate; and it generates more holistic and comprehensive models and theories of whole complex systems, rather than elements [37,38]. Both approaches are present in urban science/informatics, although the latter is preferred in the smart city context.

2.2. Datafication and Privacy

The critical perspective of urban sciences and informatics has, however, seldom attacked one core aspect of this self-feeding evolution. As more and more aspects of people's daily life are captured as data, they are now susceptible to considerably greater levels of heightened scrutiny. The pervasiveness of digitally mediated transactions and surveillance, along with the increasing use of unique identifiers and personally identifiable information (PII) to access services (e.g., names, usernames, passwords, account numbers, addresses, emails, phone numbers, credit card numbers, smart card ID, license plates, and

faces), makes it nearly impossible to live daily lives without leaving digital footprints and shadows.

Privacy—the ability to selectively expose oneself to the world—is regarded as a fundamental human right in many jurisdictions (especially democratic regimes) and is protected in various ways by national and supranational legislation. Nevertheless, cultures and circumstances vary in their everyday and legal understandings of privacy. Privacy debates, in general, concern the acceptable access to and disclosure of personal and sensitive information about an individual [39].

2.3. Dataveillance and Geo-Surveillance

We shall make a clear example regarding the datafication process. As a result of pervasive data urbanism, dataveillance and, in the case of smart cities, geo-surveillance is intensified [40,41].

Dataveillance is the monitoring, collecting and analysis of data and metadata on a personal or collective scale mainly through online platforms and social media. Roger Clarke, a surveillance theorist, coined the term dataveillance as a means of describing the impact of data processing and information technology systems on personal or mass surveillance [40]. It is directly related to the practice of "profiling" [42], which does not require the monitoring of an identified individual for a specific purpose, but rather focuses on the identification of individuals of interest who can later be subjected to personalized and targeted surveillance.

Geo-surveillance is the monitoring of a spatial location and movement of people, vehicles, objects and services, as well as their interactions [43]. For instance, many cities are flooded with digital CCTV cameras that can zoom, move and follow individual people and can be controlled remotely. Additionally, vast portions of the road network and vehicle movement are monitored by traffic, red-light, congestion and toll cameras. The analysis and interpretation of CCTV data are being supported by facial, gait and ANPR algorithms that utilize machine vision.

As the types of data that can be collected rise in tandem with the sophistication of sensory technologies, so does the capacity for discrimination. This has consequently generated worries about "social sorting", which is the potential of monitoring to assist or develop new types of categorisations, as described by David Lyon [44].

In many cases, simplistic socio-political drives misunderstand security for excessive and pervasive surveillance on citizens. For instance, without any national legal basis, in 2020, the Swiss-bordering Italian city of Como attempted to equip itself with technologies that enable the recognition of an individual through the capture of biometric data [45], despite the fact that, in the end, the administration actually mistook 'face detection' for 'face recognition' devices, intending to implement the latter functionality in its 2019 budget document for 2020 [46]. The history of Como's facial recognition technology is strongly tied to the summer 2016 incidents that affected the area where said CCTVs were installed; that year, Como became a node of the migration routes to Northern Europe and, at the height of the crisis, housed up to 500 migrants stranded in the city by the closing of the Swiss border [47].

Nevertheless, the cameras—if correctly purchased—would have theoretically been illegally tracking, recognizing and gathering information of all people passing by, including (and mostly) Italian citizens.

The Italian National Data Protection Authority promptly requested the city administration to inform the public of the presence or absence of such technology, its purposes, the manner in which the personal data of citizens would be processed and the impact assessment required to anticipate risks associated with the use of a highly vulnerable system. In its late February 2020 opinion, delivered to the municipality of Como, the Italian National Data Protection Authority was unequivocal: the system installed by the municipality could not be utilized, since it lacked a legal foundation in Italy [48].

Although the Como scenario did not see the intended 'face recognition' project coming into existence due to an administrative error—which, in any case, would have been blocked by the GPDP [49]—these events are a good example for the implementation of smart technology in an urban context through precautionary, regulatory and user-oriented principles. It is important to analyse each contingent situation to avoid episodes of misuse or political bias.

In fact, facial recognition can pose significant risks to privacy. In this regard, the execution of these types of programs poses a clear risk of citizens losing some of their liberties. As for the transportation sector of Sao Paulo, J. Novaes [50] demonstrates how biometric data might be collected with dubious transparency methods and for questionable ends.

3. Risks around Data Usage

Datafication has obvious consequences: issues arise when one realises that the link between the private and public spheres is only made possible by a flow of data that is growing in dimension and volume by the day. This concentration of data, coming from multiple actors, is becoming increasingly precise and detailed. This flow of data must therefore be designed to be fluid and efficient, but at the same time, well guided by the values of privacy and individual freedom, in a harmonious balance between efficiency and respect for the individual.

To illustrate this concept of balance, we could take the example of smart meters: they are an undeniable technological advance, simplifying billing and pricing for the service provider by tracking usage.

However, if the high frequency with which consumption (of water, energy, etc.) is monitored ultimately makes it possible to reconstruct the intimacies of people's lives (i.e., to know if they have had guests, if they wake up frequently at night, etc.), then this invention poses a clear threat to respect for individual freedom.

3.1. Answering Data Surveillance

In a smart city context, we have already explained that the main switch between private and not private is mostly linked to the method of data collection. This can be governed by three simple rules, in a cooperative method:

1. Firstly, it is necessary to adjust the default parameters of the system so that they are as well-balanced as they are feasible. Using the smart meter as an example once more, the goal is to adjust the default read frequency to a certain interval of minutes which satisfies both the information gathering needs of the operator and the user's privacy.
2. The second principle is the individual's permission to modify the system's default settings. With the user's permission, the frequency of readings can be increased for smart meters. Similarly, data may be stored locally for six months without the corporation having access to it. Users may consent to the accessing of their data if they wish to have their consumption analysed in order to be provided other, more suitable plans.
3. The third and final principle, following balanced default settings and personal consent, is aggregate data processing. The objective here is to guarantee data anonymity. Open data rationales, which permit the exchange of data between services, must not compromise the privacy of end users. In other words, if data exchange is required, the online data must not be detrimental to citizens.

These principles have little effect on innovation [51–53]. To use a driving metaphor, they are a seatbelt in the system, not a brake pedal. Without the preservation of individual liberty, the city would be merely mechanical, and not smart/sensible.

This is certainly a first step, but remains a limited goal. Legal and legislative arguments on privacy in smart cities and similar programs are currently dominated by a debate centred on data and, consequently, data protection law for individuals, such as GDPR or the California Consumer Privacy Act [54]. However, the majority of the data is collected in public settings and frequently refers to (algorithmic) groups of people (rather than

identifying individuals), making it appear non-personal, and hence, exempt from data protection rules. In this context, the topic of 'privacy' primarily focuses on personal versus non-personal data, data ownership and technological solutions such as data protection (or privacy) by design [54].

A different image emerges when the question of privacy in a public space is seen from a larger viewpoint. Critical debates on smart cities and living labs in a number of disciplines, including urban geography, surveillance studies and privacy theory (distinct from the more specialized field of data protection law), have demonstrated that privacy issues are much broader and more diverse than only *personal* data-related issues, not only because privacy should be viewed as comprising multiple types (including associational, behavioural and bodily privacy, on top of which lies a layer of informational privacy) [55], but also because smart cities and living labs shape the public space of cities and the behaviour of citizens there, with far-reaching social and political implications [56].

Thus, the smart city debate—at least, one that takes privacy seriously—should take a broader approach to the issue, incorporating the perspectives of surveillance studies, privacy theory and urban geography, and the insights that these perspectives provide. We need to counter the tendency to focus only on information privacy and data protection (controlling the collection, storage and processing of personal data), which ignores other dimensions and types of privacy that are nonetheless worth protecting in a digital environment.

There are often unanswered questions about what exactly this means and under what circumstances these issues arise: how and for whom. Indeed, many experts and the media either fail to define surveillance (as if it were a simple concept) or use the outdated panopticon or the vague image of Big Brother to describe surveillance in smart cities [56].

3.2. Safety and Deceptive Urging: "Nudging" in Smart Cities

The primary privacy danger associated with monitoring as a form of security relates to the issue of manipulative nudging and its influence on autonomy, one of the primary reasons why humans value privacy.

Smart cities are transforming cities into huge labs, where the central concern is how to make the behaviour of individuals predictable and externally controllable. In this way, technology can be considered as controlling the environment to discover and affect visitor behaviour in order to make the location safer and more appealing. This form of development is frequently referred to as nudging [57].

Commonly, a nudge is defined as any feature of the choice architecture that modifies people's behaviour in a predictable manner without restricting their options or substantially altering their economic incentives [58].

The concept of nudging is founded on the observation that the majority of individual decision making is subconscious, passive, and unreflective as opposed to deliberate and active [58]. Thus, the environment can be created with the purpose of systematically influencing human decision making in particular directions. As a result, nudges are frequently criticized in the literature for their manipulative effects that circumvent autonomous decision making, posing a threat to our autonomy [59].

However, there are various types of nudges, some of which are manipulative and others that are not. Some nudges are direct and intend to appeal to individuals' deliberative abilities. For instance, basic disclosures (a type of "informational nudge"), such as nutritional labels on food, aim to influence individuals' capacity for deliberation. In contrast, nudges can be defined as manipulative if they employ a hidden effect by secretly manipulating a person's decision-making capacity by using the person's cognitive (or affective) limitations and vulnerabilities [60]. Manipulation is typically targeted; to exploit one's weaknesses, one must be aware of them and how to exploit them [60]. However, the majority of nudges are not tailored to specific individuals; rather, they are administered uniformly to everyone. A road speed bump, for example, impacts everyone who passes it. ICTs are ideally suited to promote nudging that enables 'fine-grained microtargeting', transforming manipulative nudging into what Yeung refers to as 'hypernudging' [59].

Additionally, surveillance within smart city and living lab programs alters the texture of public spaces in functionally defined ways that may be damaging to both formal and informal community life. In particular, it accomplishes this by silencing public places that can be used for a variety of reasons and in a variety of ways for certain patterns of use [61].

This nudging has a very practical impact. It is sometimes believed that safeguarding privacy in public spaces does not take into account the social and cultural relevance of public spaces, which serve as a foundation for informal sociality and civic life [61].

This claim, however, is founded on a restricted understanding of privacy as the right to be left alone, so removing the individual from their public and social roles. Privacy is a prerequisite for the full exercise of other rights and freedoms, particularly those pertaining to public space, such as the right to access, the right to representation and the freedoms of assembly and association [62]. For example, masking and other methods of preserving anonymity may be necessary to ensure that protesting citizens can act as political agents: "Public space is not only a political area; it is also a space produced in and through privacy" [63].

For individuals to evolve into autonomous beings, both individually and politically, they must leave their private spaces and interact with others in public areas. In other words, individuals must create a variety of social relationships with strangers and near-strangers and engage politically in the public sphere [64]. The right to form and sustain social and political relationships has value not only for the individual, but also for society and democracy as a whole. In the context of privacy in the public space, it is not the case that private and public are exclusive opposites (e.g., a space or an activity can only be public or private, with nothing in between).

Consequently, the protection of privacy in the public space serves to safeguard those features of public space associated with political involvement and sociability.

The tightening of social control in which de-escalation (or exclusion) and nudging is the norm is likewise opposed to the practice of critical citizenship. Liberal citizenship necessitates a certain amount of 'discomfort', sufficient to inspire citizens to strive towards advances in the achievement of political and social objectives. This modified citizenry such as the one illustrated above lacks the resources and perhaps even the motivation to engage in such an environment [65]. In a carefully scripted public arena where difference is discouraged or excluded, there is no place for discomfort or the formation of various publics with divergent viewpoints. In the end, the objective of pervasive networked surveillance that profiles and categorizes individuals is to eliminate the diversity and serendipity essential in forming strong communal bonds.

Thus, the public spaces of contemporary (smart) cities may be favourable to consumption, but detrimental to social and political engagement. As a result, it is essential to safeguard the public space as a shared place with reciprocal rights and obligations, as opposed to a world where privacy and other individual rights are susceptible to the whims of others, particularly governments and businesses.

4. Ethical Aspects

Information and communication technologies (ICTs) present society with numerous new challenges. Due to their extensive use and growing presence in people's daily lives, it is important to recognize the role ICTs play in the urban environment.

It seems worthwhile to evaluate how such a pervasive presence of ICTs could, in some instances, influence the information flow that supports decisions and policies, with negative social consequences if an unethical selection of the information generated and collected leads to biased political decisions that exacerbate inequality and discrimination.

As smart cities are implemented across the globe, such scenarios become more probable and potentially hazardous.

4.1. Threefold Taxonomy of Cultures and Technology

The basic function of technology in modern cultures merits discussion. Postman [66] provides a threefold taxonomy of cultures and their technologies.

In the first scenario, cultures use technology solely as a fundamental tool, subject to the authority of social values and religious systems, in a culturally integrated manner that does not impose inconsistencies in the worldviews of those societies. In a second type, cultures act as technocracies in which adopted technologies alter cultural reality and contradict or threaten societal conventions, myths, politics and religion. A third type consists of the technopoly, which derives from the realization that social growth is contingent on the human capacity to apply knowledge to the creation of inventions.

We find ourselves in a clearly cut technopoly: telecommunications entered our social and economic lives throughout the twentieth century, initially as something useful but not essential; nowadays, the benefits they bring became inextricably woven into the fabric of our societies, to the extent that everything depends on its presence today.

The telecommunications revolution in all its forms (television, radio, telephone and data communication networks) unites the world's many civilizations. Its presence enabled a progressive shift towards a technocracy, bringing about the so-called "global village" through causing changes in many societies and cultures. Together with the computer, an additional great invention, these two technologies regenerated and strengthened one another. Rapidly, the digital world was incorporated into the telecommunications infrastructure, erasing the inherent disparities between legacy systems and establishing the fundamental premise of the digitization and convergence of various communication structures.

Thus, ICTs have become a societal criterion. In addition, Postman [66] argues that the technopoly's goals are reductionist, restricting discussion to efficiency and effectiveness, ultimately resulting in a loss of attention on the social reality that developed these informational structures.

4.2. Smart Cities Datafication: A Non-Neutral Phenonmenon

As cities transform into platforms for economic development from a technopolistic perspective, the converging role of ICTs in the daily lives of citizens, businesses and governments assumes greater significance.

For instance, a crucial concern is the privacy of the information monitored by Wireless Sensor Networks (WSN) and the effects that a breach of this principle can have on the routines and habits of citizens in the event of deliberate or accidental data leakage. In this regard, the International Telecommunication Union (ITU) [67] identified data protection and privacy as one of the greatest obstacles to implementing developing technologies in smart cities.

Although there are many potential benefits, it is necessary to consider the conditions for the adoption of such new technologies and the issues related to their acceptance by the population, such as data privacy, information security, availability, interoperability, the provision of the necessary infrastructure and efficient and effective management.

In addition, when examining the good or negative contributions of ICTs to efficiency and production or their environmental implications, it is not sufficient to examine equipment, structures and systems [68]. The role of specific types of power and authority should also be considered. Ultimately, technology is linked to political decisions and has the capacity to manipulate reality and favour specific social classes.

Kuchenbuch [69] illustrated such a dilemma by referencing the historical usage of architecture to implement social control. Another well-documented case is the New York Long Island bridges in the 1920: some of these bridges were purposefully constructed below the standard height to prevent the passage of buses. This step was an attempt to influence society, as it would prohibit poor people from entering so-called sophisticated regions, hence preserving their exclusivity for middle- and upper-class individuals. In this manner, technology provided certain social groups advantages over others.

Consequently, when it comes to the building of smart cities, it is crucial to comprehend their underlying architecture and the functions of their sensors. When city officials obtain data via a sensor system, the fundamental question is what criteria were used, who is coordinating the data acquisition and what is being conducted to prevent manipulations.

4.3. The Matter of Power and Authority

An analogy may be drawn: what if 'information packets' were compared to buses and cars that originate from multiple origins (sources), are handled along their routes by 'bridges' and are then subject to routing criteria that are not always transparent to society? The 'bridges' may decide pre-emption, queueing and processing speed based on the source address and operate as strategically placed filters. In addition, the rhetoric of managers implies that all judgments are based on open and socially accepted parameters, supported by data derived from informational systems operating at maximum technical efficiency. However, we contend that this reasoning does not reveal the complexities of various invisible aspects that untrained eyes cannot perceive, ranging from the entire process to the manipulations designed to serve specific objectives.

It is necessary to focus on the building of smart cities, since they can impact the rights of their residents. A risk identified by Postman [66] is the gap between the information and its human purpose that the technopoly creates. If systems lack a human purpose, information becomes an aim in and of itself, which can distort reality.

A situation of even greater gravity would be the deliberate manipulation of reality, which can occur through manoeuvres that direct the implementation stages to serve the objectives of select organizations.

This invisibility allows decision makers to prioritize the treatment of higher-class areas above those of lower-class places.

As early as 2016, a large leak of confidential information revealed that national security agencies were not only examining the telecommunication data of their own residents, but were also violating the privacy of telecom and Internet users abroad [70].

Some of these surveillance operations, such as the secret PRISM program, gathered the private information of Americans who were not even suspected of terrorism or criminal activity. The NSA and the FBI, as shown in a top-secret document obtained by The Washington Post, tapped straight into the central servers of nine prominent Internet companies, gathering audio and video chats, images, e-mails and documents that enabled analysts to also monitor foreign targets [71].

The "technopoly" as presented above assumes complete power, which is uncontested because the decisions were ostensibly "technical options" designed to foster progress and general welfare.

ICTs and communication highways, deployed by governments and businesses with diverse interests, play a crucial role in a society that is constructing digital smart cities. However, if society determines that progress must be led by an ethical commitment to the social good, who will ensure that all decisions adhere to this commitment, and who would face the challenge of continually reinforcing and making it transparent?

In a smart city context, the function of ethics is to define boundaries through codes, ordinances, rules and laws that convey social ideals and guide decisions [72]. When correctly scaled, values guarantee safety in times of crisis, robust social structures and effective political institutions.

In the context of actions related to the deployment of smart cities at a cooperative institutional level, we need a new role for IT Governance: the addition of an ethical dimension to the realm of responsibilities that arise in response to this new reality. One should allocate rights and responsibilities to enable audit mechanisms and security measures, supported by supervisory committees that can analyse IT activities and operations to identify and mitigate ethical issues and assure comprehensive transparency.

This mimics a general sectorial trend: G. Soós [73] shows how, in recent years, cyber-libertarianism waves of entrepreneurs, advocates and experts attempted to offer solutions

that transcend nation states, restoring individual liberty and government-free cooperation through the decentralization of technology and power.

4.4. A Possible Praxis to Implement Ethics

We advocate for the construction of technical procedures aimed at widening the bounds of IT governance practices.

In order to keep policymakers accountable for their decisions—not just during deployment phases, but also during operation—it is necessary to incorporate an ethical dimension into each level of the decision making by defining responsibilities. Transparency at all levels of decision making is the only way to prevent distortions created by biased information from overshadowing the benefits of smart cities.

The issues stated in the UNESCO Earth Charter [74] that call for better democratic institutions at all levels and for more transparency and publicity in the exercise of power, including involvement in decision making and access to justice, can enrich the considerations in this article.

During our research, we found that some smart cities have already taken steps toward these goals. As a matter of transparency, the "Open by Default" policy has been obligatory for OGD (Open Government Data) in the city of Zurich, starting in September 1, 2021, per City Council Resolution 741/2021 [75]. In compliance with this internationally acknowledged OGD policy, existing data sets are made freely accessible to the public by default if they do not contain any protected content.

The city of Zurich is also undertaking a trial project to increase the visibility of data collecting in public spaces. This is achieved specifically by clearly marking sensors using pictograms. Moreover, the most recent available data from the relevant sensors are processed on the city of Zurich's website and made accessible by a QR code on-site. Only open and accessible data from current sensors are utilized for this purpose [76].

5. Understanding Privacy Techniques in the Smart City

To implement the abovementioned ethnical aspects, information technology advancements permit improved data collection and the development of apps tailored to utilize these data. By deploying solutions leveraging these applications, smart city operations can be enhanced. Nonetheless, the potential of privacy infractions rises as a result of the combination of enhanced data availability and robust analytical tools. Smart city solutions must be executed meticulously to ensure compliance with regulatory limits and social expectations. Sections 5 and 6 examine the current state of smart cities around the world, presenting some examples of actual solutions, and then investigate how the privacy of individuals could be compromised and how this vulnerability could be reduced through the use of multiple privacy-enhancing technologies.

While privacy can be simply stated as the right of an individual to not be viewed or bothered [77], this definition becomes inadequate with the advent of new and developing technology. There are numerous methods for seeing a person beyond the physical sense. For instance, if information about a person is recorded and then disclosed, certain parts of that person's existence have been observed, which might be considered an invasion of privacy. Given that smart cities are information-driven, we will examine privacy from the standpoint of equating the information characterizing a person with their actual, physical characteristics.

To comprehend privacy in smart cities, we must go beyond the criterion of not being viewed or disturbed.

5.1. The Right to Be Left Alone

Finn et al. [78] outline seven forms of privacy that could be compromised by new technologies: privacy of the person, privacy of behaviour and habits, privacy of communication, privacy of data and image, privacy of ideas and feelings, privacy of location and space and privacy of affiliation. According to the aforementioned definitions, the term

'personal privacy' relates to body functions. 'Behavioural and habitual privacy' encompasses a variety of personal pursuits, including religion and politics. 'Communication privacy' includes electronic messages, phone calls and postal mail. 'Data and image privacy' refers to the requirement that individuals have total control over their gathered personal information. The expression 'thoughts and sentiments in private' alludes to individual viewpoints. 'Location and space privacy' refers to the seclusion of a place or an area.

Finally, the term 'metadata' refers to information that surrounds data but does not pertain to the data's exact contents [79]. It includes, among other things, the timing of searches against a database, the source and destination of an electronic message and the size of an email message in bytes.

The implementation of any strategy must take into account both the requirements of each application and technological advancements. Individual solutions will necessitate unique cryptographic primitives or design techniques, but the smart city's general privacy policy should be pervasive.

Depending on the type of data, various privacy measures may be applicable. We can have categorically descriptive or quantitatively numerical information; on a 'micro' scale, this information may pertain directly to a person, whereas on a 'macro' scale, it may pertain to a group of people.

5.2. Attackers and Information Sources

In smart cities, privacy safeguards must be conceived and executed with different types of attackers in mind. Metrics for measuring the privacy enjoyed by users of a system depend substantially on the type (and capabilities) of an attacker [80,81].

Attackers can be categorized by orthogonal dimension [82,83]: they can be internal or external, passive or aggressive, global or local and static or adaptive. Their capabilities can vary in terms of resources (e.g., network coverage, processing power), algorithms (e.g., restriction to algorithms with probabilistic polynomial time) and prior knowledge and available data (e.g., information from a side channel or scenario-specific knowledge). This classification is beneficial when analysing a specific attack or when measuring privacy attributes such as anonymity [82], but it is unnecessarily detailed when considering generic privacy issues for a wide area such as the smart city. Therefore, we focus on the function of the attacker in the smart city and distinguish between service providers, involved parties and third parties service suppliers.

In addition, four sources of data can be used by attackers in smart city scenarios to compromise privacy: observable data, repurposed data, published data and leaked data.

Based on observable data attacks, information can be obtained by intercepting wireless and wired transmission; the attacker is passive, but must be physically present where the transmission can be eavesdropped.

In addition, data can have been repurposed have been acquired for one cause, but are then used for another. The attacker may be a service provider, such as for location-based services, who not only uses user data to perform the service, but also to profile users. According to contextual integrity [84], data repurposing without user agreement is always a violation of privacy.

Finally, the data could include leaked information that was intended to remain confidential, but the attacker has gained them by means such as software faults, security vulnerabilities, misuse of permitted access or social engineering. These leaks have been frequent in the past [85,86]; thus, they should be anticipated [87]. Nonetheless, if these data are not safeguarded, the repercussions for privacy can be serious, and data keepers may face hefty fines and a loss of reputation. Although perfect security is improbable, the privacy technologies presented in Section 6 can significantly reduce the impact and risk of a data breach.

5.3. No Security without Privacy

There is a direct relationship between security and privacy, and comprehensive privacy protection is nearly impossible without security. For instance, a public camera positioned to record and transmit photos of individuals is a privacy issue by design; however, failing to secure the camera's communication with a back-end server is a security issue that results in a privacy issue. The distinction between conceptual and security-related privacy concerns is hazy; thus, it is short-sighted to discuss privacy protection without discussing the security challenges posed by smart city technologies.

The extensive set of recommendations and principles for designing safe computer systems is beyond the scope of this essay.

Privacy protection in the smart city is frequently contingent upon the security of its systems and subsystems, therefore comprising a need for access management. If attackers are able to compromise smart home devices, for instance, they can spy on the inhabitants or even gain physical access to the home (see Komninos et al. [88] for a review of the security issues of the smart home and smart grid).

This issue can be noticed in numerous smart city technologies, such as Internet of Things devices, wearable devices, sensor networks, autonomous systems and intelligent cars, particularly when these devices support a wide variety of protocols and contain a large number of software components. This is obviously the case for mobile phones, which, when compromised, can result in a complete invasion of user privacy.

The sensory interfaces of numerous intelligent devices pose a security risk. It has been demonstrated that the sensory channel of cyber–physical systems can be exploited to infect devices with malware [89], which can then be used to violate privacy.

For autonomous systems with an Internet connection through which equipment might be compromised and remotely controlled, access control is of particular importance to avoid property and person harm.

A second security issue is related to side channels, such as time or power consumption, which can leak data even if a system is cryptographically protected. When analysing the communication of smart meters [90], IoT devices [91] or intelligent vehicles [92], for instance, these side-channel attacks can lead to privacy violations. To determine the location of a device or user, location inference attacks may also employ side channels (e.g., smartphone accelerators [93] or radio frequency fingerprinting [94]). In the context of smart city technology, the problem of a system releasing more information than intended must be carefully studied, as every piece of information may be utilized by an attacker to breach the system's security and privacy.

A third and final condition for privacy implementation is through security of protocols and networks. For example, cryptographic protocols utilize cryptographic primitives, such as cryptographic hash functions or encryption algorithms, to establish a secure, confidential communication channel.

The only way to limit the impact is to design the system with privacy in mind; even in the absence of security issues, flaws in communication protocols can result in privacy concerns. Each system based on defective protocols may leak information beyond its intended purpose. Developers of smart city applications should always verify that the entire protocol stack supports the desired privacy objectives.

6. Privacy Strengthening

There are inherent weaknesses in data collecting, processing, storage and dissemination that can be exploited to violate the privacy of people.

In smart cities, efforts have been made to mimic privacy that is respecting of situations. Martinez-Balleste et al. [95] present an example and describe identity, query, location, footprint and owner privacy. This paradigm is useful for implementing privacy-enhancing technologies in smart cities.

In addition, attention being paid to the ENISA principles [96] is crucial to minimize the danger of unintentional exposure. Based on these guidelines, we can address two main different strategies: process-based privacy security and data-oriented privacy defence.

6.1. Process-Based Privacy Security

Process-based privacy security focuses on the processes surrounding the responsible handling of personal data. Therefore, they deal with the organizational aspects and the procedures.

Privacy, by design, encompasses seven guiding principles [97]: (i) proactive privacy protection, rather than remedial action after privacy violations have occurred; (ii) privacy as the default setting; (iii) privacy embedded into the design; iv) full functionality with full privacy protection; (v) privacy protection throughout the entire data lifecycle; (vi) visibility and transparency; and (vii) respect for user privacy. Nevertheless, this formulation of the privacy by design principles is unclear and occasionally circular [87]. Moreover, S. Spiekermann [98] contends that privacy by design—in the form of privacy impact assessments—must be legally compelled (rather than depending on voluntary compliance) in order to "defend the essential values of our Western liberal democracies and constitutions".

Attempts have been made to incorporate these concepts into the design of new systems. For instance, D. Preuveneers and W. Joosen [99] employ two principles—proactivity and end-to-end security—to drive the design of a remote health monitoring solution, whereas A. Kung et al. [100] apply the idea of transparency to intelligent transport systems. Although not expressly stated in the seven principles, Gürses et al. [87] suggest that data minimization should be the foundation of privacy by design. In the following part, we address data minimization as a method of data-centric privacy protection, taking a smart cities perspective.

To systematically apply privacy by design to the smart city, the principles must be included into a privacy engineering procedure. For instance, the method proposed in Gürses et al. [87] begins with functional requirements analysis and data minimization; then analyses attackers, threats and additional security requirements; and concludes with the design's implementation and testing. J. Hoepman [101] provides eight privacy design solutions for integrating privacy needs into a conventional software engineering process. Four tactics pertain to data-oriented privacy defence (minimize, hide, segregate and aggregate), whereas four strategies pertain to process-based privacy security (inform, control, enforce and demonstrate).

Security architectures privacy architectures are required to connect various defences and ensure that no privacy leaks occur at any time. For instance, the architecture described by H. Choi et al. [102] utilizes trusted distant data stores and a broker to arbitrate access to the users' data stores. This is similar to [103,104], which combine many cryptographic approaches to provide privacy assurances.

6.2. Data-Oriented Privacy Defence

Data-oriented privacy defence focuses on the privacy-friendly processing of the data itself. It is a strategy that is more technical in nature.

As stated previously, data minimization can be inferred from the concepts of privacy by design.

In smart cities, data minimization has been utilized to formally examine architectural options for electronic toll pricing [105] and generate privacy-preserving strategies for large data analysis [106].

Modern smart system sensors naturally collect more sensor data than required for the intended activity, presenting a special challenge to data minimization. We refer to these as supplementary data. To prevent their exploitation, the system should be built to limit the amount of captured data for the intended use case.

Moreover, a tool pertaining to the 'hiding' tactic of data-oriented privacy defence is offered by anonymity and unlikability; k-anonymity is a popular strategy for protecting the privacy of people in public releases of statistical databases. The central concept is that databases, such as those containing medical information, contain both identifying information (such as names) and sensitive information (such as medical problems). Hence, k-anonymity—which we analyse in detail later—divides database rows into equivalence classes with at least k rows that are indistinguishable based on their quasi-identifiers [107,108].

However, it has been demonstrated that k-anonymity, as with many other types of anonymisation, presents flaws that allow the re-identification of people and/or their sensitive information in a variety of contexts.

For instance, the Zurich Handelsgericht had determined that pseudonymized or effectively anonymized bank information is no longer covered by banking secrecy. In particular, the court was tasked with determining whether supposedly pseudonymised consumer data could be forwarded to the Department of Justice (DoJ) as part of the US program. The court determined that pseudonymisation was ineffective since the Department of Justice could, with reasonable efforts, re-identify the bank data subjects. Unfortunately, the DOJ was able, thanks to third party information, to de-anonymize the data completely [109].

Differential privacy is a more contemporary method to database privacy that offers unobservability and, unlike k-anonymity, can provide privacy guarantees: any disclosure is equally probable (within a tiny multiplicative factor), regardless of whether an item is in the database or not [110]. For instance, the outcome of a database query should be comparable regardless of whether or not the database contains a particular individual's record. This assurance is typically met by adding a small amount of random noise to database query results.

In terms of 'hiding' and 'segregating' techniques, encryption safeguards privacy by ensuring the secrecy of messages and other data. Traditionally, symmetric encryption requires two parties to exchange an encryption/decryption key, whereas public-key encryption allows messages to be encrypted using a public key, and only the private key may decrypt the contents.

Identity-based encryption is a form of public-key encryption in which the public key can be any string, such as a user's name or email address [111]. This enables the encryption of messages for a recipient who has not produced a public/private key combination. Private service discovery can be implemented using identity-based encryption [112].

Individuals can use anonymous digital credentials to confirm information about themselves, such as whether they are a valid sender or possess a specified attribute such as age or nationality, without revealing their identify. Anonymous and pseudonymous credentials provide anonymity, pseudonymity and unlinkability, respectively. Both techniques prevent authorities from de-anonymizing users, simultaneously facilitating proof of certification.

6.3. Privacy-Enhancing Technologies

Both strategies and techniques are founded upon a variety of privacy-protecting methods, ranging from the removal of identifying information to more complex solutions such as random relay networks. There are two key categories of approaches used to accomplish privacy protection: anonymisation and security. Both are essential for the future of privacy in the smart cities.

Anonymization procedures modify the condition of a data set so that no original source can be identified. Typically, this would involve the total de-identification and the preservation of pseudo-identifiers in some fashion. In most cases, anonymization strategies include masking and altering sensitive data.

A well-protected system is ensured by the well-known trio of security features: these characteristics are confidentiality, availability and integrity. Since it can be demonstrated

that each of these properties can be abused to violate privacy, it is possible to claim that strengthening these properties is a privacy protection activity.

Listed below are some of the main technologies that might be used to better protect privacy through technology security, divided between the three main areas of functionality they are applied to: anonymisation, perturbation and encryption.

6.3.1. Anonymizing Tactics

Masking applies a whole, partial or formatted substitution to any attribute. For instance, specific digits of phone numbers or credit card numbers can be disguised to display only those digits in precise spots.

Nulling out is a substitution technique in which all the values of an attribute are eliminated [113,114]. This may be an identifying characteristic, an unrelated sensitive characteristic or a pseudo-identifier.

Micro-aggregation is the grouping of entries in a data set based on how similar their protected attribute values are. The average attribute value throughout the group is used to generalize the value of each entry inside the group. Solé et al. [115] provide algorithms for accomplishing micro-aggregation.

Substitution can prepare data for consumption by an end user or at the sensor layer's source. It is a data anonymization method suited to categorical information.

K-anonymity aids in avoiding re-identification via quasi-identifiers by ensuring that all data entries share the values of their quasi-identifiers with k 1 other entries [108]. Even if an attacker has some previous knowledge, k-anonymity prevents them from identifying their target among k 1 other items in the data. L-anonymity uses micro-aggregation in a particular, meticulously planned approach to generate groupings that provide anonymization and disruption.

K-anonymity is closely related to the following two other technologies:

1. L-diversity extends k-anonymity in situations when the sensitive attribute does not vary across a set of individuals having k-anonymized quasi-identifiers [114]. If all k entries in the group have identical sensitive properties, then the application of k-anonymity is irrelevant, as the attacker will still be able to determine their exact attribute. L-diversity increases k-anonymity such that there are l well-represented values inside each set of k-anonymized tuples [116].
2. T-closeness is an extension of k-anonymity that enhances l-diversity. T-closeness also seeks to increase the distribution of values in the sensitive attribute of anonymized data, but instead of focusing on well-represented values, it prioritizes a distribution that is typical of the genuine worldwide distributions for the sensitive attribute [114].

6.3.2. Perturbation Tactics

Shuffling is the reassignment of values in columns in a manner that eliminates the relationships between characteristics [113,114]. The objective of shuffling is to eliminate linkages between sensitive features and identifying attributes without modifying the entries in any other way. As demonstrated by Li et al. [117], shuffling is a valid method for protecting privacy in data publications. This technology could be used by smart city systems that disclose data through open data initiatives.

Variance alters numerical data that are either correlated or uncorrelated to the number distribution in all data, achieving the goal of protecting the anonymity of people represented in a data set by fully deleting their data while preserving certain statistical properties [113,114].

Generalization diminishes the granularity of a data attribute [114]. It can be applied to continuous or categorical data, and is useful for anonymizing the sensor and application layers.

Sampling is the release of only a subset of the total data set. Some data are withheld, while the data that are made public should be indicative of the entire collection. Clearly,

it is not intended to be used to modify data in any way; rather, it is used to safeguard the identities of people omitted from the data set.

Differential privacy protects aggregated statistical data against attackers who manipulate a sequence of inquiries to derive an individual's private information. The presence or absence of an individual in a data set is naturally concealed by employing a method that totally conceals that individual's contribution to the aggregate data. Typically, this is accomplished by deliberately adding noise into the results [118].

6.3.3. Encryption Tactics

Encryption comprises techniques for concealing information to a degree proportional to the strength of the algorithm and cryptographic key employed. It is a broadly applicable technology that can be utilized at each tier of a smart city's architecture. There are numerous implementations of encryption and other technologies that enhance privacy based on encryption:

Private and public key encryption implementations may employ the same or separate keys for encryption and decryption techniques. The same key is used for both the encryption and decryption with secret key encryption, whereas public key infrastructures employ distinct keys.

Biometric encryption is a unique encryption implementation. The key for encryption and decryption is generated using human input, such as a fingerprint, eye scan, facial structure or any other measurable and distinguishable attribute. Sethi [119] provides a list of regularly utilized biometric traits, which includes the iris, face, fingerprints, hand geometry, retina, voice, signatures and key dynamics.

Homomorphic encryption is a type of encryption that enables users to perform computations on encrypted material without decrypting it first. These resulting computations are stored in an encrypted format that, when decrypted, produce the same results as if they had been conducted on unencrypted data. Homomorphic encryption can therefore be used to protect the privacy of outsourced data storage and processing. This enables encrypted data to be outsourced to commercial cloud environments for processing while remaining encrypted.

7. Switzerland

How is privacy considered in a smart city context today? The comprehension of the complexity of public administration reforms in various countries is influenced by the fundamentals of their institutional and political systems. In the Swiss context, ties to the past and the historical background of the nation's founding are especially strong.

The common depiction of Switzerland as a "Sonderfall" (unique case) of a nation that built its prosperity on political neutrality and consensus decision making is highly important. The Swiss policymaking process is influenced by the institution and political system's defining characteristics: direct democracy, consensual form of government and federalism. This trio reinforces the rigidity and stability of Switzerland's political institutions. Even though none of the three qualities is remarkable on its own, their combination generates a unique institutional framework that explains Swiss policy responses in social and economic spheres [120]. In the past, the Swiss decision-making process has been characterized as ponderous and resistant to significant improvements. When a suggested policy succeeded in a decision, the resulting adjustments were likely modest and minimal. Due to the consensus-based political structure, compromise solutions agreed by all parties have tended to be similar to the status quo, and innovations have been limited [121]. Nonetheless, various changes have been seen over time. As policy challenges have become more complicated, it has become increasingly challenging to find solutions within the conventional federalist model of power distribution. As a result, coordinated reactions became more important [122].

Switzerland is a federalist nation characterized by the extensive autonomy of its 26 regions ("cantons") and 2202 municipalities in policymaking. The allocation of competencies

among the three levels of government is founded on the idea of subsidiarity; policy choices are made at the lowest level of government capable of addressing the subject adequately. Historically, cantons and municipalities have delegated authority to the central government, typically because it was more efficient for the central government to carry out these activities [123]. However, local authorities (especially cantons) retain great power, going as far as deciding their own civil law procedure (e.g., Basel, Vaud) and implementing social policies. For instance, out of the total tax paid by one citizen, local taxes can make up to 85%. In a smart city context, this gives large local means and powers.

This does not result in the Swiss Federal Government having no power whatsoever; there are multiple initiatives at the federal level in a smart cities context. However, unlike other countries, these are made through consensus and collaboration processes. One such example is the e-government, the implementation of which in Switzerland is governed by a variety of both federal and local documents [124].

The most important document is the "eGovernment Strategy Switzerland", which was developed jointly by the three levels of government (federal, local and municipal) [125]. In addition to the federal strategy, the majority of Swiss cantons have developed their own eGovernment policies with distinct objectives and priorities.

The regularly published national eGovernment study [126] is an important publication that examines the evolution of eGovernment in Switzerland and summarizes the viewpoints of many actors.

Another example of collaboration is found in the realm of mobility integration policies, for the purposes of which every moderately large city in Switzerland can qualify as smart. While public transportation authorities, the railways and car/bike sharing are all run by different companies, either public or private, they all feature some level of integration, such as the possibility to use your railway pass on local subways and buses, or the possibility to use the same identifiers.

The results of the Swiss case study indicate the degree to which adherence to the "conventional" concept of the public administration is characterized by hierarchical relationships between the public administration and citizens. Some view legal limits and hierarchical structures as impediments to innovation, but others view them as anchors of continuity and stability against the external environment's unpredictability.

7.1. Practices in Transformational Government

On the basis of our empirical findings from the examination of the strategies of Swiss regional governments, some best practices for the development of transformational smart city government may be identified:

- Standardisation of service provision across departments: The uniform "look and feel" of the government one-stop-shop is necessary for the convenience of electronic access to public services. Swiss cantonal governments strive to create electronic platforms offering a variety of products, intuitive search functions and traceability of processes, as their users are typically unconcerned with the department responsible for the required service and more likely to value prompt and user-friendly service delivery. Similar initiatives are being launched at the federal level in an effort to ease the communication between the federal government and private businesses. The preferred strategy of Swiss cantonal governments to increase the loyalty of their public departments appears to be to emphasize the positive effects that the provision of cross-cutting public services has on residents and the activities of public departments. An obligation-based approach to the construction of one-stop-shops has also been identified, but due to the consensus-based character of Swiss policymaking, it is not the preferred method of federal and regional governments. In general, governments appear to construct their unified electronic presences in a pragmatic manner; first, they focus on the departments that stand to gain the most from the new platform.
- Incremental approach to digitalisation: The success of the Swiss public administration's gradual implementation of eGovernment is a solution for its previous financial

losses in the field. During the first decade of the twenty-first century, the failures of excessively ambitious programs slowed down the deployment of eGovernment in the country. In recent years, a cautious acceleration has been noticed alongside a shift in mindset. According to a member of the federal parliament, Swiss governments manage public digitalization projects exceptionally poorly. I believe that legislators are cautious to launch another initiative, since there have been so many failures with software that cost millions of dollars but never worked.

- Lack of central authority and consensus model: The free market approach, but more than anything, the consensus method, has shown a practical advantage in the Swiss construction of smart cities. Instead of falling in the usual pitfalls of centralised authority, the consensus method relies on a multiple feedback system, with a dense web of local stakeholders. This allows the deciders to make relevant decisions actually requested by the local inhabitants.

In Switzerland, the (neo)institutionalist paradigm dominates the digitization of the public sector. As a result of the various characteristics of the public and private sectors, the drivers of innovation in each differ. In general, the public sector is characterized by a number of constraints relating to its institutional, political and legal frameworks, as well as the culture of public organisations.

Even though the answer to more widespread public invention is complicated and public innovation does occur [127], rankings reveal a significant gap between the innovativeness of the commercial and public sectors in Switzerland.

7.2. Case Study

The main objective of this survey is to evaluate smart projects supported and financed or co-financed by public authorities, notably local administrative ones, and their relation to privacy. For each one, we looked in particular if a project existed (Y) or not (N/A), and if specific privacy initiatives were taken in each one of them (Y) or not (N/A). Lastly, we checked if a privacy policy, specifically for the smart cities initiatives, had been adopted (Y) or if the local authority relied on state-level legislation (N/A).

We looked for projects in three smart areas: mobility policies (regarding technology aimed at integrating the means of transportation, controlling the traffic and offering a sustainable sharing alternative to private transportation); health policies (such as digital medicine and digital health integration of data) and eGovernment policies (with reference to official communication and active participation of citizens).

The results of the Swiss case study indicate that the degree of adherence to the 'conventional' concept of public administration differs between public departments.

There is a great deal of interest throughout Switzerland in everything related to smart travel and mobility, which is directly linked to the sustainable travel industry. The aforementioned integration between local public transport authorities and the national railways has shown a very good outcome. However, it is noticeable that Zurich is the only one of those surveyed that has specific privacy policies for each of its mobility projects.

Zurich has also made extraordinary efforts to promote a series of smart projects along with specific privacy policies, demonstrating not only a very high level of interest in implementing smart policies, but also a concrete will to protect citizen's right to privacy in regard to sector-specific challenges. Other administrations of well-recognised smart cities such as Geneva and Lausanne have not yet acted in the direction of data privacy with sector-specific policies: despite this, both are considered to be worldwide references for smart cities.

Smart health initiatives show a much more inconsistent solution: the small Tessin Canton has implemented, in collaboration with a private initiative, a "patient folder" that can be exported everywhere, which provides all of their cities an actual implementation of digital health integration. On the other hand, the Canton and Republic of Geneva, renown smart city with a much higher population, is yet to take any measures. This is perplexing to say the least: in Switzerland, most Healthcare initiatives are supported by private insurers

on a Danish model (private insurers manage the healthcare system within a regulated framework), and the integration of a smart city within this framework—as Zurich did—is much more feasible than in a centralised model.

Zurich and Luzern aside, in the process of implementing eGovernment, the lag in public innovativeness manifests itself in the inability of public agencies to incorporate the consequences and dangers of innovative processes into their organizational culture. In other words, it would appear that the Swiss administrative culture is frequently incompatible with the consequences that eGovernment generates, even if, in other context, it is well aware of said dangers.

As shown in Table 1, Swiss administrative independence has paved the way for the heterogeneous development of smart and privacy policies across the country.

Table 1. Switzerland.

City	Population	Smart Mobility Policies						Smart Health Policies				Smart Local eGovernment				Local Privacy Policies
		Integration Grid		Traffic Control		Biking/Car Sharing		Digital Health Integration		Digital Medicine		Open Data		Active Citizen		
		Program	Data protection	Program	Data protection	Program	Data protection	Program	Data protection	Program	Data protection	Program	Data protection	Program	Data protection	
Zurich	341,730	Y	Y	Y	Y	Y	Y	Y	N/A	Y	N/A	Y	Y	Y	Y	Y
Geneva	183,981	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	N/A	N/A	Y	N/A	Y	N/A	N/A
Basel	164,488	Y	N/A	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A
Lausanne	139,111	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y	Y	Y	Y	N/A
Bern	121,631	Y	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Y	N/A	N/A
Wintherthur	91,908	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	Y	N/A	Y	N/A	Y	N/A	N/A
Luzern	81,691	Y	Y	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y
Lugano **	63,000	Y	N/A	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	Y	N/A	Y	N/A	N/A
Bellinzona **	16,572	Y	N/A	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	Y	N/A	Y	N/A	N/A

Source: Institutional Websites and Sources. ** Lugano and Bellinzona both work within the larger "Ticino Smart City" initiative.

8. Italy

Unlike Switzerland, where smart cities have their place in the landscape and there is a major interest in the smart cities solution, Italy lacks a local smart city ecosystem. Other than Milan, medium-sized Italian cities such as Bergamo, Trento, Parma, Modena and Reggio Emilia answer the call for a proper smart city consideration. They rate well in terms of environmental protection, economic stability, sustainable mobility and digital transformation, while cities in the south remain at the bottom of the list. Florence rates well due to its high quality of life, digital transformation and strong position in terms of government competency, environmental protection and sustainable transportation. Governance, digital transformation, economic solidity, environmental protection and quality of life all rank highly for Bologna [128].

The IMD rating [129] emphasizes the well-known divide between northern and southern cities, with southern cities occupying the bottom spots. The absence of infrastructure and the community's reluctance to utilize the services are unquestionably among the leading causes of the gap. For instance, the car-sharing program has failed in most southern Italian cities.

In general, it is simpler to achieve sustainability in transit, the environment, the economy, construction and the management of the territory's natural resources in medium-sized cities, since they are more operational and organized.

Compared to prior years, the number of smart city projects and programs is increasing, with initiatives that are more consistent and innovative. Despite this, the widespread growth of smart cities in Italy still faces a number of hurdles.

Thirty-six percent of the main Italian municipalities have initiated at least one smart city project between 2018 and 2021, the majority of which are still in the experimental

phase, according to the Internet of Things Observatory survey [130]. In addition, the trials frequently occur separately and without coordination.

Despite the numerous tests conducted, the initiatives are still inadequately linked and frequently lack a defined strategy for territorial growth. The lack of appropriate economic resources and adequate skills, as well as the prevalence of ambiguous governance frameworks, are impediments to their development.

These are the primary reasons why the majority of ventures fail after the initial experimental phase. A coordinated national plan is necessary to resolve the issue. Municipalities must define commitments and priorities, and the correct compromise must be reached to avoid the excessive centralisation that already exists.

A suitable model for project analysis depends on four variables: the maturity of the towns, the maturity of the offer, the utilization of the obtained data, and the public–private partnership. The investigation reveals that the maturity level of the municipalities is significantly lower than that of the offer. In summary, towns are unprepared for the task, and the number of public–private partnerships is still insufficient.

Several municipal governments initiated E-government programs as experimental communication tools with citizens, businesses and other local and national administrations. Some progressive local governments have built community ICT networks that include all stakeholders, in addition to internal networks for the management of public institutions. They have been attempting to enhance their decision-making process by leveraging networks and related ICT solutions. New databases and networks, data processing and dissemination, electronic filing systems, document exchange systems, decision-making support tools, electronic procurement, electronic declaration and application systems and other tools have been implemented to facilitate a more effective, cost-conscious, performance-based, user-friendly and transparent public administration. However, many years after the initial experiments, a very limited number of municipalities are still exploring with ICT technologies. Additionally, in municipalities with ICT networks, network usage is frequently restricted to e-mail exchange and one-way information dissemination. Few individuals are successful at establishing two-way and/or multi-way communication, executing transactions and utilizing ICT networks for management. The government has been encouraging and supporting municipal projects. However, budgetary and personnel constraints have prevented local governments from conducting potentially useful trials. Local political interests typically oppose the use of ICT, and few residents are enthusiastic about this innovation. Theoretically, the benefits that eGovernment projects and the related tools should bring should change not just the administrative aspect of public institutions, but also their communication with stakeholders.

Case Study

In order to compare the Swiss findings with the Italian ones, we chose nine Italian cities with the same methodology as implemented in Table 1. Particularly, we analysed and surveyed the three most populous cities from three main areas of the Italian peninsula: north, centre and south. As for Switzerland, the objective of this survey is to evaluate smart projects supported and financed or co-financed by public authorities, notably, local administrative ones.

The following table, Table 2, shows that the three main cities from northern, central and southern Italy are all undergoing smart innovation processes with a few differences to each other. Notably, the health area is the one that is developed the least, whereas the smart mobility has the greatest focus and financing. We assume that the great interest regarding mobility is related to the implementation of efficient and sustainable tourism policies, a crucial sector in Italy, such as the one of Venice that we examined earlier [8].

Table 2. Italy.

City	Population	Smart Mobility Policies						Smart Health Policies				Smart Local eGovernment				Local Privacy Policies
		Integration Grid		Traffic Control		Biking/Car Sharing		Digital Health Integration		Digital Medicine		Open Data		Active Citizen		
		Program	Data protection	Program	Data protection	Program	Data protection	Program	Data protection	Program	Data protection	Program	Data protection	Program	Data protection	
Milan	1,397,715	Y	N/A	Y	Y	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y	Y	N/A
Turin	848,196	Y	N/A	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	Y	N/A	Y	N/A	Y
Genoa	558,930	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y	N/A	Y	Y	N/A
Rome	2,783,809	Y	Y	Y	Y	Y	N/A	N/A	N/A	Y	N/A	Y	N/A	Y	Y	N/A
Bologna	394,463	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	Y	N/A	Y	N/A	Y	N/A	N/A
Florence	359,755	Y	N/A	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	Y	N/A	Y	Y	Y
Naples	940,940	N/A	N/A	Y	N/A	Y	N/A	Y	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A
Palermo	640,720	N/A	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A	N/A	Y	N/A	N/A	N/A	N/A
Bari	313,003	N/A	N/A	N/A	N/A	Y	N/A	N/A	N/A	Y	N/A	Y	N/A	N/A	N/A	N/A

Source: Institutional websites and sources.

Despite the political drive towards smart innovation, we feel the need to stress the lack of interest in data protection, which, for instance, is totally absent in biking/car sharing projects. In addition, the known divide between north and south in innovation basis is herein evident.

Finally, only a few administrations have adopted an autonomous local privacy policy (the rest are only in accordance with European or national legislation); we are yet to see a significant effort in implementing specific privacy defensive tools and clear data protection principles according to each segment of the smart development process.

There are several aspects of Italian culture and society that can be considered when looking for a reason for the lack of significant efforts to protect privacy in the context of smart cities.

Indeed, there is a very low level of systemic trust, especially in institutions, while there is a high sense of perceived risk and a discreet valorisation of one's own data among digitised people [131,132]. This is exacerbated by a below-European-average knowledge of their rights in this area: for instance, while Italians reach the average in their awareness of online terms and conditions, only 51% are aware of the existence of GDPR, compared to the European average of 70% [133].

This paradoxical ambivalence risks leading to a progressive separation between the administrations and partners responsible for innovation policies and civil society. In the absence of a participatory smart city, public policies themselves risk failing to (i) meet the real needs of citizens; (ii) listen to the demands of different stakeholders; and (iii) spend digital-policy budgets efficiently.

In this context, the PNRR (Piano Nazionale di Ripresa e Resilienza) funding—which is the Italian governmental expenditure plan of NextGeneration EU—aims at restoring the country's economy through six essential missions: (i) digitalisation, innovation, competitivity, culture and tourism; (ii) green transition; (iii) sustainable mobility; (iv) education and research; (v) cohesion and inclusion; and (vi) health. Funds are being allocated to local administrations across the peninsula to undertake innovative projects, therefore transferring high-level responsibilities to peripheral authorities.

Among the funds of PNRR Mission 1, for instance, 40 million Euros are designated for mobility as a service, a new integrated form of transportation that is being tested in metropolitan areas. Currently, the Maas4Italy initiative envisions three pilot cities (Milan, Rome and Naples), with the possibility of spreading best practices to seven more cities.

Despite all the good premises, the question of whether local administrators will be up to the task still remains. Finally, we emphasise how crucial data protection policies will ensure individual liberties, especially during such a quick innovation process in Italy.

9. Conclusions

The study highlights the negative personal privacy and informational security outcomes that may arise from the development programs currently pursued in smart cities and digital cities. The authors aim to illustrate the ways in which the remedies proposed so far appear insufficient from a legal or practical standpoint. The study is centred around two countries that while geographically nearby, but are, however, very distinct as smart cities development zones: in Switzerland, the smart city concept is well known and used, while in Italy, it is mostly set aside as a secondary concept, ignored or even treated as an annoyance. Smart city initiatives in those two countries navigate in very different contexts, legally, economically and culturally. This allows the study findings to be applicable in wildly in different contexts.

There are two obvious limitations to this study:

(1) As it is impossible to know the exact types of data collected by the sector actors, we were forced to look for typical data in three sectors. As the study entities are of different sizes (although still within a fairly limited range), larger cities may have faced problems more quickly than smaller cities. This study tends to show the opposite (no link between city size and privacy measures).

(2) Due to the difficulty of accessing direct data, we were forced to look for proxies, such as reports, laws and best practices presented by the public entities themselves. This serves the purpose of the study, but only opens the way for a different understanding of the subject.

We have shown that the development and deployment of smart city technologies, as well as the urban planning and IT science surrounding these processes, clearly raise a variety of ethical, legal and practical concerns. This state of affairs has previously elicited various critiques which reject the very concept, ethos and practices [13,29,33,134] of smart urbanism as a result. An adequate response to these critiques might be to advocate a fundamentally different approach to urban development and the way different official assessments are carried out in lieu of current "urban science".

Another common criticism is that smart cities and urban science need to be rethought, not recast. Rather than throwing the baby out with the bathwater, it is necessary to recognise the substantial and significant benefits that smart city technology brings to city governments and citizens. Intelligent transport systems effectively improve traffic flow throughout a city, and smartphone applications have been shown to provide useful services to residents [4]. Similarly, urban science and informatics bring fresh and valuable insights into the dynamic nature of cities. This does not mean, however, that one should be totally unaware of the effects of smart cities technology.

First, a reorientation of the concept of the city is needed. Cities should be seen as fluid, open, complex, multi-level, contingent and relational systems, full of cultural and political issues, competing interests and entrenched problems that tend to evolve erratically. They should not be seen as bounded, predictable and manageable systems that can be managed and controlled in a mechanical, linear way. The habit of reducing complexity through modelling, and then basing urban management on the results of models, is reductionist; it impoverishes our understanding of a city, while exacerbating technocratic forms of government. In other words, the instrumental logic of urban analysis should not be allowed to replace common sense and experience, or even other sources of knowledge such as 'small data' studies. These epistemes should be used contextually and in conjunction with each other.

Researchers should not only consider the ethical consequences of their work in terms of privacy risks, notification and consent, but also how their findings are applied. This is because they owe their fellow citizens a form of due diligence that goes beyond mere compliance with applicable laws and institutional research board regulations. Although it is often difficult to define what constitutes indirect harm, analysts need to reflect on the conditions under which their work can be conducted and presented responsibly. Meanwhile, their professional organisations should review and adapt their ethical guidelines in

light of the proliferation of big data. Decision makers must, of course, take into account the potential negative effects of using a new smart city tool, as well as the impossibility of informing and obtaining consent in many cases. They should play a proactive role in brokering privacy and security arrangements on behalf of residents, through their contracting processes and parameters. Accordingly, all providers should be required to comply with service level agreements on system operation, data generated and use and sharing of information, after having undergone privacy impact assessments.

In summary, we must strive to develop smart cities and urban science that follow a set of privacy principles. This adaptive paradigm shift is not an easy task, but immediate improvement is needed, and this article presents some ideas for a realistic roadmap, which requires researchers and decision makers to first acknowledge the number and seriousness of such challenges that surround intensive and far-reaching information sharing.

Author Contributions: Conceptualization, B.F.G.F. and A.B.; methodology, B.F.G.F.; validation, B.F.G.F.; formal analysis, B.F.G.F. and A.B.; investigation, B.F.G.F. and A.B.; data curation, B.F.G.F.; writing—original draft preparation, B.F.G.F. and A.B.; writing—review and editing, B.F.G.F. and A.B.; visualization, B.F.G.F. and A.B.; supervision, B.F.G.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data has been acquired from public institutions and official websites and should therefore be regarded as open access.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Portal, L.; Fabregue, B. Establishing Participative Smart Cities: Theory and Practice. *Smart Cities Reg. Dev. (SCRD) J.* **2022**, *6*, 43–62. [CrossRef]
2. Kitchin, R. Toward a Genuinely Humanizing Smart Urbanism. In *The Right to the Smart City*; Cardullo, P., Di Feliciantonio, C., Kitchin, R., Eds.; Emerald Publishing Limited: Bradford, UK, 2019; pp. 193–204, ISBN 978-1-78769-140-7.
3. McFarlane, C.; Söderström, O. On Alternative Smart Cities. *City* **2017**, *21*, 312–328. [CrossRef]
4. Fabregue, B.; Portal, L.; Cockshaw, C. Using Smart People to Build Smart Cities: How Smart Cities Attract High Skilled Workers, Retain Them, and Become Innovative (Belgium, Netherlands, Denmark, Poland). *Smart Cities Reg. Dev. (SCRD) J.* **2023**, *7*, *in press*.
5. Cardullo, P.; Kitchin, R. Smart Urbanism and Smart Citizenship: The Neoliberal Logic of 'Citizen-Focused' Smart Cities in Europe. *Environ. Plan. C: Politics Space* **2019**, *37*, 813–830. [CrossRef]
6. Isin, E.; Ruppert, E. *Being Digital Citizens*; Rowman & Littlefield International: London, UK, 2015; ISBN 978-1-78348-055-5.
7. Shelton, T.; Lodato, T. Actually Existing Smart Citizens. *City* **2019**, *23*, 35–52. [CrossRef]
8. Kitchin, R. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*; SAGE: Thousand Oaks, CA, USA, 2014; ISBN 978-1-4739-0826-0.
9. Graham, S.; Marvin, S. *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*; Routledge: London, UK, 2001; ISBN 978-0-203-45220-2.
10. Strandburg, K.J. *Privacy, Big Data, and the Public Good: Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context*; Lane, J., Stodden, V., Bender, S., Nissenbaum, H., Eds.; Cambridge University Press: Cambridge, UK, 2014; pp. 5–43.
11. Crawford, K.; Schultz, J. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *B.C. L. Rev.* **2014**, *55*, 93.
12. Townsend, A. Cities of Data: Examining the New Urban Science. *Public Cult.* **2015**, *27*, 201–212. [CrossRef]
13. Marvin, S.; Luque-Ayala, A.; McFarlane, C. *Smart Urbanism: Utopian Vision or False Dawn?* Marvin, S., Luque-Ayala, A., McFarlane, C., Eds.; Routledge: London, UK, 2015; ISBN 978-1-315-73055-4.
14. Kitchin, R.; Lauriault, T.P.; McArdle, G. Knowing and Governing Cities through Urban Indicators, City Benchmarking and Real-Time Dashboards. *Reg. Stud. Reg. Sci.* **2015**, *2*, 6–28. [CrossRef]
15. TIM. Venezia, un Esempio di Smart City. La città del 25 Redat è Sicura, Vivibile e Sostenibile. Available online: https://www.gruppotim.it/it/sostenibilita/news/Venezia-smart-control-room.html (accessed on 16 December 2022).
16. Buckley, J. Venice Is Watching Tourists' Every Move. Available online: https://www.cnn.com/travel/article/venice-control-room-tourism/index.html (accessed on 21 January 2023).
17. Bubola, E. Venice, Overwhelmed by Tourists, Tries Tracking Them. *The New York Times*. 4 October 2021. Available online: https://www.nytimes.com/2021/10/04/world/europe/venice-tourism-surveillance.html (accessed on 9 February 2023).
18. Saccà, S.; Arco, G. La resa alla monocultura turistica 25 redatorial. *Ytali*. 24 August 2022. Available online: https://ytali.com/2022/08/24/la-resa-alla-monocultura-turistica-predatoria/ (accessed on 9 February 2023).

19. Palazzo, S. Smart Control Room o Grande Fratello?/Caso Venezia: Telecamere per "gestire" persone. *IlSussidiario.net*. 11 July 2022. Available online: https://www.ilsussidiario.net/news/smart-control-room-o-grande-fratello-caso-venezia-telecamere-per-gestire-persone/2373034/ (accessed on 9 February 2023).
20. Gabriele Gargantini La stanza dove si vede tutto quello che succede a Venezia. *Il Post*. 10 June 2022. Available online: https://www.ilpost.it/2022/06/10/venezia-smart-control-room/ (accessed on 9 February 2023).
21. Minoia, P. Venice Reshaped? Tourist Gentrification and Sense of Place. In *Tourism in the City: Towards an Integrative Agenda on Urban Tourism*; Bellini, N., Pasquinelli, C., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 261–274, ISBN 978-3-319-26877-4.
22. Bertocchi, D.; Visentin, F. "The Overwhelmed City": Physical and Social Over-Capacities of Global Tourism in Venice. *Sustainability* **2019**, *11*, 6937. [CrossRef]
23. Contributo di accesso e prenotazione della Città di Venezia. Available online: https://live.comune.venezia.it/it/2022/07/contributo-di-accesso-e-prenotazione-della-citt-di-venezia-si-parte-il-16-gennaio-2023 (accessed on 21 January 2023).
24. Batty, M.; Axhausen, K.W.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart Cities of the Future. *Eur. Phys. J. Spec. Top.* **2012**, *214*, 481–518. [CrossRef]
25. Foth, M. *Handbook of Research on Urban Informatics: The Practice and Promise of the Real-Time City*; IGI Global: Hershey, PA, USA; ISBN 978-1-60566-152-0.
26. Offenhuber, D.; Ratti, C. *Decoding the City: How Big Data Can Change Urbanism*; Birkhauser Verlag AG: Basel, Switzerland, 2014; ISBN 978-3-03821-392-5.
27. Lazer, D.; Pentland, A.; Adamic, L.; Aral, S.; Barabási, A.-L.; Brewer, D.; Christakis, N.; Contractor, N.; Fowler, J.; Gutmann, M.; et al. Computational Social Science. *Science* **2009**, *323*, 721–723. [CrossRef]
28. Desrosières, A. *The Politics of Large Numbers: A History of Statistical Reasoning*; Harvard University Press: Cambridge, MA, USA, 2002; ISBN 978-0-674-00969-1.
29. Mattern, S. Methodolatry and the Art of Measure. *Places J.* **2013**. [CrossRef] [PubMed]
30. Morozov, E. *To Save Everything, Click Here*; Public Affairs: New York, NY, USA, 2017; ISBN 978-1-61039-370-6.
31. Buttimer, A. Grasping the Dynamism of Lifeworld. *Ann. Assoc. Am. Geogr.* **1976**, *66*, 277–292. [CrossRef]
32. Harvey, D. *Social Justice and the City*; University of Georgia Press: Athens, GA, USA, 1973; (revised 2009), ISBN 978-0-8203-3403-5.
33. Greenfield, A. *Against the Smart City*; Do Projects: New York, NY, USA, 2013.
34. Parsons, W. Not Just Steering but Weaving: Relevant Knowledge and the Craft of Building Policy Capacity and Coherence. *Aust. J. Public Adm.* **2004**, *63*, 43–57. [CrossRef]
35. Bettencourt, L.M.A.; Lobo, J.; Helbing, D.; Kühnert, C.; West, G.B. Growth, Innovation, Scaling, and the Pace of Life in Cities. *Proc. Natl. Acad. Sci. USA* **2007**, *104*, 7301–7306. [CrossRef] [PubMed]
36. Pentland, A. *Social Physics: How Good Ideas Spread—The Lessons from a New Science*; Penguin Press: London, UK, 2014; ISBN 978-1-59420-565-1.
37. Miller, H.J. The Data Avalanche Is Here. Shouldn't We Be Digging? *J. Reg. Sci.* **2010**, *50*, 181–201. [CrossRef]
38. Kelling, S.; Hochachka, W.M.; Fink, D.; Riedewald, M.; Caruana, R.; Ballard, G.; Hooker, G. Data-Intensive Science: A New Paradigm for Biodiversity Studies. *BioScience* **2009**, *59*, 613–620. [CrossRef]
39. Elwood, S.; Leszczynski, A. Privacy, Reconsidered: New Representations, Data Practices, and the Geoweb. *Geoforum* **2011**, *42*, 6–15. [CrossRef]
40. Clarke, R. Information Technology and Dataveillance. *Commun. ACM* **1988**, *31*, 498–512. [CrossRef]
41. Gitelman, L. *"Raw Data" Is an Oxymoron*; The MIT Press: Cambridge, MA, USA, 2013; ISBN 978-0-262-31232-5.
42. Clarke, R. Profiling: A Hidden Challenge to the Regulation of Data Surveillance. *J.L. Inf. Sci.* **1993**, *4*, 403.
43. Crampton, J.W. Cartographic Rationality and the Politics of Geosurveillance and Security. *Cartogr. Geogr. Inf. Sci.* **2003**, *30*, 135–148. [CrossRef]
44. Lyon, D. Surveillance as Social Sorting. Lyon, D., Ed.; Routledge: London, UK, 2002; ISBN 978-0-203-99488-7.
45. Como, le telecamere ci riconoscono—Già in funzione ma nessuno lo sa. *La Provincia*. 21 August 2019. Available online: https://www.laprovinciadicomo.it/stories/como-citta/como-le-telecamere-ci-riconoscono-gia-in-funzione-ma-nessuno-lo-sa_1319403_11/ (accessed on 9 February 2023).
46. Documento Unico di Programmazione per il Triennio 2020/2022. *Comune di Como*. 2019, pp. 103–104. Available online: https://www.comune.como.it/export/sites/default/it/comune/bilanci-documenti-piani/documento-unico-programmazione/DUP-2020-2022.pdf (accessed on 9 February 2023).
47. Dazzi, Z. Migranti, emergenza alla stazione di Como: Svizzera chiude accesso di Chiasso. *La Repubblica*. 12 July 2016. Available online: https://milano.repubblica.it/cronaca/2016/07/12/news/profughi_svizzera_como_stazione-143891692/ (accessed on 9 February 2023).
48. Garante per la Protezione dei Dati Personali (GPDP) Provvedimento 9309458. Available online: https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9309458 (accessed on 16 December 2022).
49. Garante per la Protezione dei Dati Personali. Available online: https://www.garanteprivacy.it/ (accessed on 19 December 2022).
50. Novaes, J. Private Information in Public Spaces: Facial Recognition in the Times of Smart Urban Governance. *Smart Cities Reg. Dev. (SCRD) J.* **2021**, *5*, 31–43. [CrossRef]
51. Goldfarb, A.; Tucker, C. Privacy and Innovation. *Innov. Policy Econ.* **2012**, *12*, 65–90. [CrossRef]

52. The Economist America Should Borrow from Europe's Data-Privacy Law. Available online: https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law (accessed on 19 December 2022).
53. Thierer, A.D. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. *SSRN* **2015**. [CrossRef]
54. Dalla Corte, L.; van Loenen, B.; Cuijpers, C. Personal Data Protection as a Nonfunctional Requirement in the Smart City's Development. In Proceedings of the 13th International Conference on Internet, Law & Politics, Universitat Oberta de Catalunya, Barcelona, Spain, 29–30 June 2017; ISBN 978-84-697-4474-1.
55. Koops, B.-J.; Newell, B.C.; Timan, T.; Skorvanek, I.; Chokrevski, T.; Galic, M. A Typology of Privacy. *U. Pa. J. Int'l L.* **2016**, *38*, 483.
56. Finch, K.; Tene, O. Smart Cities: Privacy, Transparency, and Community. In *The Cambridge Handbook of Consumer Privacy*; Selinger, E., Polonetsky, J., Tene, O., Eds.; Cambridge Law Handbooks; Cambridge University Press: Cambridge, UK, 2018; pp. 125–148, ISBN 978-1-107-18110-6.
57. van Dijck, J.; Poell, T. Social Media and the Transformation of Public Space. *Soc. Media + Soc.* **2015**, *1*, 2056305115622482. [CrossRef]
58. Leonard, T.C.; Richard, H. Thaler, Cass, R. Sunstein, Nudge: Improving Decisions about Health, Wealth, and Happiness. *Const. Polit. Econ.* **2008**, *19*, 356–360. [CrossRef]
59. Yeung, K. 'Hypernudge': Big Data as a Mode of Regulation by Design. *Inf. Commun. Soc.* **2017**, *20*, 118–136. [CrossRef]
60. Susser, D.; Roessler, B.; Nissenbaum, H. Online Manipulation: Hidden Influences in a Digital World. *Geo. L. Tech. Rev.* **2019**, *4*, 1. [CrossRef]
61. Patton, J.W. Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places. *Ethics Inf. Technol.* **2000**, *2*, 181–187. [CrossRef]
62. Ruppert, E.S. Rights to Public Space: Regulatory Reconfigurations of Liberty. *Urban Geogr.* **2006**, *27*, 271–292. [CrossRef]
63. Koops, B.-J. Privacy Spaces. *W. Va. L. Rev.* **2018**, *121*, 611.
64. Staeheli, L.; Mitchell, D. Spaces of Public and Private: Locating Politics. In *Spaces of Democracy: Geographical Perspectives on Citizenship, Participation and Representation*; SAGE Publications Ltd.: London, UK, 2004; pp. 147–160, ISBN 978-0-7619-4734-9.
65. Cohen, J.E. Surveillance vs. Privacy: Effects and Implications. *SSRN* **2017**. Available online: https://ssrn.com/abstract=3212900 (accessed on 9 February 2023).
66. Postman, N. *Technopoly: The Surrender of Culture to Technology*; Vintage: New York, NY, USA, 1993.
67. ITU. Council Internet of Things Global Standards Initiative. Available online: https://www.itu.int:443/en/ITU-T/gsi/iot/Pages/default.aspx (accessed on 16 December 2022).
68. Syed, A.S.; Sierra-Sosa, D.; Kumar, A.; Elmaghraby, A. IoT in Smart Cities: A Survey of Technologies, Practices and Challenges. *Smart Cities* **2021**, *4*, 429–475. [CrossRef]
69. Kuchenbuch, D. Architecture and Urban Planning as Social Engineering: Selective Transfers between Germany and Sweden in the 1930s and 1940s. *J. Contemp. Hist.* **2016**, *51*, 22–39. [CrossRef]
70. Szoldra, P. This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks. Available online: https://www.businessinsider.com/snowden-leaks-timeline-2016-9 (accessed on 19 December 2022).
71. Gellman, B.; Poitras, L.U.S. British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program. *Washington Post*. 6 June 2013. Available online: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (accessed on 9 February 2023).
72. Tzafestas, S.G. Ethics and Law in the Internet of Things World. *Smart Cities* **2018**, *1*, 98–120. [CrossRef]
73. Soos, G. Smart Decentralization? The Radical Anti-Establishment Worldview of Blockchain Initiatives. *Smart Cities Reg. Dev. (SCRD) J.* **2018**, *2*, 35–49. [CrossRef]
74. UNESCO. Unesco. *Earth Charter. Earth Charter*. Available online: https://earthcharter.org/wp-content/uploads/2020/03/echarter_english.pdf?x53442 (accessed on 9 February 2023).
75. Stadt Zürich. *STRB Nr. 0743/2021*. 2021. Available online: https://www.stadt-zuerich.ch/portal/de/index/politik_u_recht/stadtrat/geschaefte-des-stadtrates/stadtratsbeschluesse/2021/Jul/StZH_STRB_2021_0743.html (accessed on 9 February 2023).
76. Digital Transparency in Public Spaces—City of Zurich. Available online: https://www.stadt-zuerich.ch/prd/en/index/urban-development/smart-city/transparency.html (accessed on 19 December 2022).
77. Camrbidge Dictionary Privacy. Available online: https://dictionary.cambridge.org/dictionary/english/privacy (accessed on 19 December 2022).
78. Finn, R.L.; Wright, D.; Friedewald, M. Seven Types of Privacy. In *European Data Protection: Coming of Age*; Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y., Eds.; Springer: Dordrecht, The Netherlands, 2013; pp. 3–32, ISBN 978-94-007-5170-5.
79. Staudemeyer, R.C.; Pöhls, H.C.; Watson, B.W. Security and Privacy for the Internet of Things Communication in the SmartCity. In *Designing, Developing, and Facilitating Smart Cities*; Springer International Publishing: Cham, Switzerland, 2017; pp. 109–137, ISBN 978-3-319-44924-1.
80. Wagner, I.; Eckhoff, D. Technical Privacy Metrics: A Systematic Survey. *ACM Comput. Surv.* **2018**, *51*, 1–38. [CrossRef]
81. Wagner, I. Evaluating the Strength of Genomic Privacy Metrics. *ACM Trans. Priv. Secur.* **2017**, *20*, 1–34. [CrossRef]
82. Diaz, C. Anonymity Metrics Revisited. In Proceedings of the Anonymous Communication and Its Applications; Schloss Dagstuhl—Leibniz-Zentrum für Informatik: Dagstuhl, Germany, 2006; Volume 5411, pp. 1–6.

83. Wagner, I.; Eckhoff, D. Privacy Assessment in Vehicular Networks Using Simulation. In Proceedings of the Winter Simulation Conference 2014, Savannah, GA, USA, 7–10 December 2014; pp. 3155–3166.
84. Nissenbaum, H. Privacy as Contextual Integrity. *Wash. L. Rev.* **2004**, *79*, 119.
85. Hackers Claim Retrieving Data of China's Shanghai National Police Database. Available online: https://www.outlookindia.com/international/hackers-claim-retrieving-data-of-china-s-shanghai-national-police-database-news-206975 (accessed on 19 December 2022).
86. Tax Authority Data Mismanagement: Details of Thousands of Dutch Leaked. Available online: https://nltimes.nl/2017/10/19/tax-authority-data-mismanagement-details-thousands-dutch-leaked (accessed on 19 December 2022).
87. Gürses, S.; Troncoso, C.; Diaz, C. Engineering Privacy by Design Reloaded. *Comput. Priv. Data Prot.* **2011**, *14*, 25.
88. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [CrossRef]
89. Uluagac, A.S.; Subramanian, V.; Beyah, R. Sensory Channel Threats to Cyber Physical Systems: A Wake-up Call. In Proceedings of the 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 301–309.
90. McDaniel, P.; McLaughlin, S. Security and Privacy Challenges in the Smart Grid. *IEEE Secur. Priv.* **2009**, *7*, 75–77. [CrossRef]
91. Zhao, K.; Ge, L. A Survey on the Internet of Things Security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Washington, DC, USA, 14–15 December 2013; pp. 663–667.
92. Bloessl, B.; Sommer, C.; Dressler, F.; Eckhoff, D. The Scrambler Attack: A Robust Physical Layer Attack on Location Privacy in Vehicular Networks. In Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 16–19 February 2015; pp. 395–400.
93. Han, J.; Owusu, E.; Nguyen, L.T.; Perrig, A.; Zhang, J. ACComplice: Location Inference Using Accelerometers on Smartphones. In Proceedings of the 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012), Bangalore, India, 3–7 January 2012; pp. 1–9.
94. Barnes, J.D.; Distler, P.H.; McMullen, M.P. Location Inference Using Radio Frequency Fingerprinting. U.S. Patent 7,945,271, 17 May 2011.
95. Martinez-Balleste, A.; Perez-martinez, P.A.; Solanas, A. The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. *IEEE Commun. Mag.* **2013**, *51*, 136–141. [CrossRef]
96. European Union Agency for Cibersecurity. Privacy and Data Protection by Design 2015. Available online: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (accessed on 9 February 2023).
97. Cavoukian, A. *Privacy by Design: The 7 Foundational Principles*; Information and Privacy Commission of Ontario, Canada: Toronto, ON, Canada, 2009.
98. Spiekermann, S. The Challenges of Privacy by Design. *Commun. ACM* **2012**, *55*, 38–40. [CrossRef]
99. Preuveneers, D.; Joosen, W. Privacy-Enabled Remote Health Monitoring Applications for Resource Constrained Wearable Devices. In Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, 4 April 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 119–124.
100. Kung, A.; Freytag, J.-C.; Kargl, F. Privacy-by-Design in ITS Applications. In Proceedings of the 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Lucca, Italy, 20–24 June 2011; pp. 1–6.
101. Hoepman, J.-H. *Privacy Design Strategies*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 446–459.
102. Choi, H.; Chakraborty, S.; Charbiwala, Z.M.; Srivastava, M.B. SensorSafe: A Framework for Privacy-Preserving Management of Personal Sensory Information. In Proceedings of the Secure Data Management; Springer: Berlin/Heidelberg, Germany, 2011; pp. 85–100.
103. Dhungana, D.; Engelbrecht, G.; Parreira, J.X.; Schuster, A.; Valerio, D. Aspern Smart ICT: Data Analytics and Privacy Challenges in a Smart City. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 447–452.
104. Layouni, M.; Verslype, K.; Sandıkkaya, M.T.; De Decker, B.; Vangheluwe, H. Privacy-Preserving Telemonitoring for EHealth. In Proceedings of the Data and Applications Security XXIII; Springer: Berlin/Heidelberg, Germany, 2009; pp. 95–110.
105. Le Métayer, D. Privacy by Design: A Formal Framework for the Analysis of Architectural Choices. In Proceedings of the Third ACM Conference on Data and Application Security and Privacy, Dallas, TX, USA, 18 February 2013; Association for Computing Machinery: New York, NY, USA, 2013; pp. 95–104.
106. Monreale, A.; Rinzivillo, S.; Pratesi, F.; Giannotti, F.; Pedreschi, D. Privacy-by-Design in Big Data Analytics and Social Mining. *EPJ Data Sci.* **2014**, *3*, 10. [CrossRef]
107. Samarati, P. Protecting Respondents Identities in Microdata Release. *IEEE Trans. Knowl. Data Eng.* **2001**, *13*, 1010–1027. [CrossRef]
108. Sweeney, L. K-Anonymity: A Model for Protecting Privacy. *Int. J. Unc. Fuzz. Knowl. Based Syst.* **2002**, *10*, 557–570. [CrossRef]
109. *HG150170-O*; 2017. Available online: https://www.gerichte-zh.ch/fileadmin/user_upload/entscheide/oeffentlich/HG150170-O11.pdf (accessed on 9 February 2023).
110. Dwork, C. Differential Privacy: A Survey of Results. In Proceedings of the Theory and Applications of Models of Computation, Xi'an, China, 25–29 April 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 1–19.
111. Boneh, D.; Boyen, X. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In Proceedings of the Advances in Cryptology—EUROCRYPT 2004, Interlaken, Switzerland, 2–6 May 2004; Cachin, C., Camenisch, J.L., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 223–238.

112. Wu, D.J.; Taly, A.; Shankar, A.; Boneh, D. Privacy, Discovery, and Authentication for the Internet of Things. In Proceedings of the Computer Security—ESORICS 2016, Heraklion, Greece, 26–30 September 2016; Springer International Publishing: Cham, Switzerland, 2016; pp. 301–319.
113. Raghunathan, B. *The Complete Book of Data Anonymization: From Planning to Implementation*; CRC Press: Boca Raton, FL, USA, 2013; ISBN 978-1-4398-7730-2.
114. Domingo-Ferrer, J.; Sánchez, D.; Soria-Comas, J. Database Anonymization: Privacy Models, Data Utility, and Microaggregation-Based Inter-Model Connections. *Synth. Lect. Inf. Secur. Priv. Trust* **2016**, *8*, 1–136. [CrossRef]
115. Solé, M.; Muntés-Mulero, V.; Nin, J. Efficient Microaggregation Techniques for Large Numerical Data Volumes. *Int. J. Inf. Secur.* **2012**, *11*, 253–267. [CrossRef]
116. Aggarwal, C.C.; Yu, P.S. Aggarwal, C.C.; Yu, P.S. A General Survey of Privacy-Preserving Data Mining Models and Algorithms. In *Privacy-Preserving Data Mining: Models and Algorithms*; Advances in Database Systems; Springer: Boston, MA, USA, 2008; pp. 11–52, ISBN 978-0-387-70992-5.
117. Li, H.; Muralidhar, K.; Sarathy, R. The Effectiveness of Data Shuffling for Privacy-Preserving Data Mining Applications. *J. Inf. Priv. Secur.* **2012**, *8*, 3–17. [CrossRef]
118. Abawajy, J.H.; Ninggal, M.I.H.; Herawan, T. Privacy Preserving Social Network Data Publication. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1974–1997. [CrossRef]
119. Ishwar, K. Sethi Biometrics Overview and Application. In *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*; Springer: Berlin/Heidelberg, Germany, 2006.
120. Mach, A.; Trampusch, C. The Swiss Political Economy in Comparative Perspective. In *Switzerland in Europe. Continuity and Change in the Swiss Political Economy*; Routledge: London, UK, 2011; pp. 9–26.
121. Pascal Sciarini Introduction. Political Decision-Making in Switzerland. In *The Consensus Model Under Pressure*; Palgrave Macmillan: London, UK, 2015; pp. 1–23.
122. Schenkel, W. Uwe Serdült Intergovernmental Relations. In *Handbook of Swiss Politics*; Neue Zuercher Zeitung: Zurich, Switzerland, 2004; pp. 393–427.
123. Kriesi, H.; Trechsel, A.H. *The Politics of Switzerland: Continuity and Change in a Consensus Democracy*; Cambridge University Press: Cambridge, UK, 2008; ISBN 978-0-521-60631-8.
124. Linder, W.; Mueller, S. *Swiss Democracy: Possible Solutions to Conflict in Multicultural Societies*, 4th ed.; Springer Nature: Berlin, Germany, 2021; ISBN 978-3-030-63266-3.
125. eGovernment Suisse EGovernment Strategy Switzerland. Available online: https://www.digital-public-services-switzerland.ch/en/media/landingpage-egovernment (accessed on 19 December 2022).
126. eGovernment Suisse. *Étude Nationale Sur La Cyberadministration 2019. La Cyberadministration En Suisse Selon Le Point de Vue de La Population, Des Entreprises et Des Administrations*. Available online: https://www.administration-numerique-suisse.ch/application/files/6416/3895/8851/Etude-nationale-sur-la-cyberadministration-2019-compte-rendu.pdf (accessed on 9 February 2023).
127. Boukamel, O. *Sept Leviers Pour l'Innovation Publique*; Éditions Seismo: Zurich, Switzerland; Geneva, Switzerland, 2020; ISBN 978-2-88351-093-7.
128. D'Acunto, A. La città del futuro è digitalizzata, sostenibile e inclusiva. *EY Italy*. 30 June 2022. Available online: https://www.ey.com/it_it/workforce/la-citta-del-futuro-e-digitalizzata-sostenibile-e-inclusiva (accessed on 9 February 2023).
129. Smart City Observatory Web Page. Available online: https://www.imd.org/smart-city-observatory/home/ (accessed on 19 December 2022).
130. Osservatori Digital Innovation del Politecnico di Milano. Available online: https://www.osservatori.net/it/home (accessed on 19 December 2022).
131. Dinev, T.; Bellotto, M.; Hart, P.; Russo, V.; Serra, I.; Colautti, C. Privacy Calculus Model in E-Commerce—A Study of Italy and the United States. *Eur. J. Inf. Syst.* **2006**, *15*, 389–402. [CrossRef]
132. Dinev, T.; Bellotto, M.; Hart, P.; Russo, V.; Serra, I. Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States. *JGIM* **2006**, *14*, 57–93. [CrossRef]
133. FRA. *Your Rights Matter: Data Protection and Privacy—Fundamental Rights Survey*; European Union Agency for Fundamental Rights: Vienna, Austria, 2020.
134. Kitchin, R. The Real-Time City? Big Data and Smart Urbanism. *GeoJournal* **2014**, *79*, 1–14. [CrossRef]