applied sciences

MDPI

Review

Privacy and Security in Cognitive Cities: A Systematic Review

Juvenal Machin, Edgar Batista, Antoni Martínez-Ballesté and Agusti Solanas *

Department of Computer Engineering and Mathematics, School of Engineering Avinguda dels Paisos Catalans, Universitat Rovira i Virgili, 26, 43007 Tarragona, Spain; juvenal.machin@estudiants.urv.cat (J.M.); edgar.batista@urv.cat (E.B.); antoni.martinez@urv.cat (A.M.-B.)
* Correspondence: agusti.solanas@urv.cat; Tel.: +34-977-55-88-67

Featured Application: This article recalls the concept of cognitive city and provides a timely review of the state of the art in the field of information security and privacy for cognitive cities, understood as artificial-intelligence-augmented smart cities. Also, it suggests several research lines that are going to be relevant in the years ahead, thus, representing an up-to-date starting point for researchers interested in exploring the most relevant security and privacy aspects of cognitive cities.

Abstract: The emerging paradigm of the *cognitive city*, which augments smart cities with learning and behavioral change capabilities, is gaining increasing attention as a promising solution to the challenges of future mega-cities. Cognitive cities are built upon artificial learning and behavioral analysis techniques founded on the exploitation of human-machine collective intelligence. Hence, cognitive cities rely on the sharing of citizens' daily-life data, which might be considered sensitive personal data. In this context, privacy and security of the shared information become critical issues that have to be addressed to guarantee the proper deployment of cognitive cities and the fundamental rights of people. This article provides a thorough literature review using the recommendations for systematic reviews proposed by Vom Brocke et al. and the PRISMA statement. We analyze peer-reviewed publications indexed in ACM Digital Library, IEEE Xplore, Scopus, and Web of Science until July 2020. We identify the main challenges on privacy and information security within cognitive cities, and the proposals described in the literature to address them. We conclude that many challenges remain open and we suggest several research lines that will require further examination in the years to come.

Keywords: cognitive city; security; privacy; artificial intelligence; cybersecurity

Citation: Machin, J.; Batista, E.; Martinez-Balleste, A.; Solanas, A. Privacy and Security in Cognitive Cities: A Systematic Review. *Appl. Sci.* **2021**, *11*, 4471. https://doi.org/10.3390/app11104471

Academic Editor: Gianluca Lax

Received: 24 April 2021
Accepted: 11 May 2021
Published: 14 May 2021

1. Introduction

The world population is steadily growing and moving towards urban settlements. The United Nations prospects estimate that, by 2030, a third of the population will dwell cities inhabited by more than half a million citizens. This unrestrained urbanization process will create mega-cities that will need to provide citizens with suitable mobility and utilities, services, and jobs while addressing huge threats, such as scarcity of resources, pollution, and global warming, to name a few. All these issues will seriously challenge the efficiency, sustainability, and resiliency of our future overpopulated human societies.

With these challenges in mind, the *smart city* idea was first introduced to control cities' infrastructures with Information and Communication Technologies (ICT), the aim being to provide efficient and environmentally-friendly services to their citizens (e.g., smart energy, smart water, smart traffic management, smart healthcare [1], etc.). This is performed under the assumption that gathering lots of data would—hypothetically—lead to the making of better informed decisions [2]. However, efficiency often contradicts resiliency, and ICT alone will not be able to build livable cities. In recent years, technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and Ubiquitous Computing (UC), along with

connected learning theories (i.e., *Connectivism* [3]) have allowed the development of the new augmented urban paradigm of *cognitive cities*, which are drawing the attention of the research community.

Cognitive cities learn and adapt their behavior based on past experiences and are able to sense, understand, and respond to changes in their environment [4]. There is a variety of views on the concept in the literature [5,6] but, to sum up, a cognitive city exploits the collective intelligence of the city, that is, the pervasive bidirectional flows of information that circulate among humans and the city. These information flows create what is known as an *intelligence amplification loop* [7], which allows the city to *learn* from the constant interaction between agents (humans and machines) and *adapt* as the environment changes, achieving sustainability and resiliency. Unlike smart cities, cognitive cities use other sources of information, besides technological sources, to *sense* their conditions: thanks to the interactions among human and non-human agents, cognitive cities are able to use the cultural, behavioral, spatial, and political information that makes up the *personality* of a city.

Let us illustrate the concept of cognitive city with a very simple example that compares its behavior to that of a smart city and a regular city:

- In a *regular* city, traffic lights are hardwired, and their behavior is fixed: if a change is needed, controls have to be rewired.
- In a *smart* city, traffic lights react to the data coming from nearby sensors to regulate the flow of traffic, and to provide an efficient response when needed, such as in case of traffic incidents.
- In a *cognitive* city, traffic lights learn from humans and vehicles passing by, generate hypothesis about the future, and evaluate the possible consequences of their decisions. Hence, they are no longer reactive, but proactive.

Following this traffic lights example, let us enrich it so as to further highlight the features of cognitive cities. Figure 1 illustrates the scenario that is next explained:

An intelligent vehicle has a blowout, and remains stopped blocking a lane. Due to the incident, the communication capabilities of the intelligent car have become affected and it is not able to notify its state to nearby agents, thus remaining unresponsive and blocking the lane ①. A nearby citizen, who has witnessed the incident, reports it by sending an alert using his/her smartphone. This alert is, therefore, forwarded to other nearby agents such as other citizens, vehicles and smart things ②. Upon the reception of the alert, the closest traffic light (i.e., a nearby agent) adapts its behavior/role and coordinates with nearby traffic lights to rearrange their lights patterns, so that traffic continues to flow without major disturbances ③. Moreover, the built-in camera of the traffic light records details about the incident (e.g., location, pictures . . .) and sends an alert to emergency teams if needed ④. In such case, the traffic lights adapt their light patterns to prioritise the arrival of the emergency services to the incident. In the midterm, after several blowouts in the same location, agents send a collective report to the authorities so they could be aware of the numerous incidents in that area. With this process, the cognitive city learns that the area is prone to vehicles blowouts, and recommends to asphalt the pavement again so as to prevent further incidents in the future ⑤.

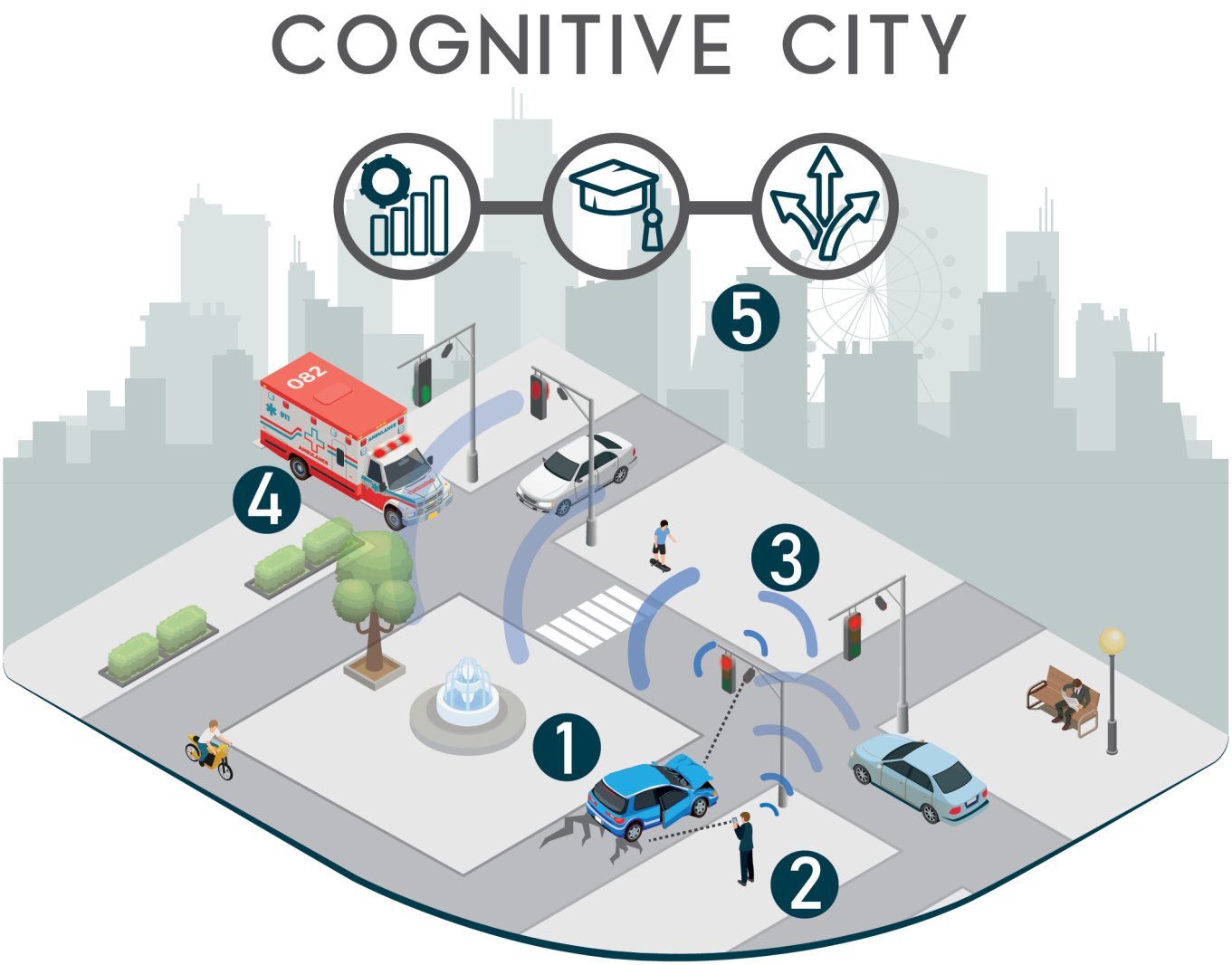

Figure 1. A cognitive city scenario.

1.1. Privacy and Security in the Cognitive City

Given that citizens' data are the primary material that allows the cognitive city decisions and that these decisions influence daily lives of citizens, protecting this information becomes crucial, not only at the individual level, but also at the societal level. First of all, the ubiquitous collection of citizen-related information at the city level introduces serious threats on individual privacy, such as: personal information disclosure, appropriation, or stigmatization. Thus, data will need to be anonymized. Even in aggregated data sets, there still exists a risk of re-identification of the individuals. As a consequence, statistical disclosure control methods should be applied prior to releasing any information [8,9]. Furthermore, the availability of diverse urban-wide data sources (e.g., transportation, healthcare, energy, surveillance cameras, etc.) plus the inferential capabilities of cognitive and AI systems, deepens the knowledge on citizens' daily activities. This allows for a richer and more detailed profiling and modeling on citizens' actions: not only we could answer questions such as: *'who is he with?'*, *'where is she?'*, *'where does he use to buy groceries?'*, etc., but also *'what will he likely want to do tomorrow at six?'*. Despite potential benefits, individuals could suffer an invasion of privacy, and a reduction of liberty. Also, from a social perspective, the consequences could be even more dramatic, opening the door to threats, such as over-surveillance, power imbalance, and manipulation in favour of governments, corporations, or whoever is in control of the city data.

Given that cognitive cities will become the natural environment for the interaction among humans and cognitive systems (e.g., autonomous cars), failures or malfunctions in this context can paralyze the city activities, causing a deep impact on citizens' lives. When these malfunctions occur on mission-critical infrastructures, such as healthcare, damages can be vast in terms of trust and economic loss and, even further, they can also cause harm to individuals and lost of human lives. Moreover, far from simply protecting the city from occasional breakdowns and malfunctions, cognitive city infrastructures will need to be prepared to face denial-of-service, ransomware, and other disruptive attacks, and implement proper security protection countermeasures.

Also, these autonomous decision-making processes rely on true, accurate, and complete data to make proper rational decisions, but important issues can arise if the data gathered are incomplete, inaccurate, or wrong. Furthermore, the impact of data quality and integrity-related issues can become paramount if data are maliciously injected, modified, or deleted by malicious agents. Particularly, machine learning (ML) models are prone to data poisoning attacks, where a group of data points are stealthily added to the training set so that the algorithm output (i.e., tag) satisfies the attacker intentions. These data-set-oriented attacks can be carried out through sophisticated high-end methods [10], or by simpler trivial ones, like the artist that recently tricked Google Maps injecting false traffic jam, by simply dragging a cart with ninety nine smartphones while connected to the *ask for directions* feature [11]. Recalling the aforementioned traffic lights example, the consequences of altering the information workflow amongst the involved agents can be fatal. With the aim to highlight the importance of security and privacy aspects in this context, next, we list some privacy and information security-related situations within cognitive cities, and their possible consequences.

Illustrative examples of privacy and information security-related situations in a cognitive city:

- Following the news of a cognitive city app being hacked, the citizens become reluctant to participate in the cognitive city project that the government is developing. Despite all the funds and high-end technology involved, the project fails.
- A cognitive transportation system provides unmanned vehicles with alternate routes, sensing the status of the transport network and vehicles in real time, by making a trade-off between the best routes and user preferences and learned routines. Unfortunately, due to a bug in the communications protocol, the gateway misses one in five sensors readings. As the system does not validate inputs, it keeps recommending the same routes, regardless of their actual status.
- A participatory government platform feeds a data model to make automatic decisions. A malicious chatbot is introduced to alter the algorithm input. Final decisions do not reflect the will of citizens.
- An error with a faulty sensor makes the water pump feedback mechanism to inject ten times more chlorine into the tap water system. Thousands of citizens get sick.
- Terrorists hack into a self-driving car, *weaponizing* it. The car runs into the crowd. Fifty people die.

These examples illustrate the need for an urgent study on privacy and security issues in the cognitive city context, and for the development of the appropriate safeguards that will be required (not only into the technologies used, but also into infrastructures, processes, laws, and people) to identify and manage the associated risks. The cognitive city concept is gaining momentum but, because it rests upon the active sharing of citizens' information, which is used to build models of the environment and to make decisions about the urban daily life, privacy and security of this sensitive information become an unavoidable need that entails important challenges. These challenges must be addressed as soon as possible to make the development of cognitive cities a reality.

Despite the relevance of the subject, to the best of our knowledge, this is the first article that analyzes the topic. This lack of research contrasts with the large number of security-

related [12–16] and privacy-related research [17–21] within smart cities, besides works on underlying technological paradigms, such as machine learning [22–24], big data [25–27], IoT [28–30], cloud and fog computing [31–33], or UC [34–36], to name a few. However, the number of security and privacy research articles on cognitive cities is expected to grow in the years to come, because of the natural evolution of smart cities towards cognitive cities.

1.2. Contribution and Plan of the Article

The first goal of this study is to review research done on privacy and information security in the cognitive city context, in terms of focus and challenges. The second goal is to identify further research lines in the field. In accordance with these goals, a set of research questions have been proposed to smoothly guide the review:

- RQ1: Which focus has been used in the scientific literature to address the information security and privacy aspects of cognitive cities (i.e., technical, social, regulatory)?
- RQ2: What are the challenges that have been identified in the field?
- RQ3: What do authors have proposed to address those challenges?
- RQ4: Which issues remain open?

Based on the research questions, PICO [37] was implemented as follows:

- Population: peer-reviewed published studies.
- Intervention: privacy and information security in cognitive cities.
- Compared: with works selected by issue type, issue category, proposals made, and focus.
- Outcome: privacy and information security in the context of cognitive cities research: focus, challenges, and proposals.

The remainder of the article is organized as follows: Section 2 presents the review methodology used, Section 3 summarizes the results of the review, Section 4 discusses the results, and Section 5 summarises our conclusions and points out to further research lines that are going to be relevant in the years ahead.

2. Methodology

We have adopted the methodology proposed by Vom Brocke et al. [38], which is based on the guidelines described in Webster and Watson [39], for conducting literature reviews. This well-known procedure consists of five phases: (i) definition of the review scope, (ii) conceptualization of the topic, (iii) literature search, (iv) literature analysis and synthesis, and (v) definition of a research agenda.

2.1. Definition of the Review Scope

First, the scope of the review must be clearly defined. To this end, the taxonomy of literature reviews presented by Cooper [40] is used. This taxonomy categorizes reviews according to focus, goal, organization, perspective, audience, and coverage. The details are provided below:

- Focus: It represents the pivotal area of interest, and it could include: research theories, outcomes, methods, and/or applications. Given the relevance of the topic, we are interested in getting a wide understanding of the field. Therefore, our literature review focuses on all types of academic articles, ranging from theoretical to practical ones.
- Goal: It represents the overall goals that authors aim to accomplish with the review. In particular, we aim to synthesize past literature and to investigate which approaches have been used by the scientific community to address the security and privacy aspects of cognitive cities, what are the challenges identified in the field, and what do authors have proposed to address those challenges.
- Organization: The review is organized using a conceptual structure, i.e., grouping the same ideas.
- Perspective: This category refers to the point of view used by the authors to discuss the literature. In this review, we adopt a neutral but critical position, that is: we have analyzed the articles and then studied them critically.

- Audience: This review is intended for researchers in the field of cognitive cities.
- Coverage: With the aim to include and analyze relevant contributions, an exhaustive coverage of the available scientific literature on the topic is considered.

2.2. Topic Conceptualization

Vom Brocke et al. advise that a review must begin *"with a broad conception of what is known about the topic and potential areas where knowledge may be needed"*. To this end, a working definition of the key terms should be provided [38] (p. 8). The two key topics addressed in this review are cognitive cities, on the one hand, and information security, on the other. Regarding the meaning of the concept *cognitive city*, we refer the readers to the introductory section of this study. Regarding the meaning of the concept *information security*, a concise introduction of the term is provided next.

Information security is frequently referred to as the preservation of confidentiality, integrity, and availability of information, which is known as the *CIA triad*. This is in agreement with the international standard ISO/IEC 27000:2018, which additionally states that *"other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved."* [41] (p. 4). Other definitions have been proposed and, despite the great interest of the topic, there is still no commonly agreed definition encompassing the broad scope of the subject, from a professional and academic perspective [42]. To address a broad approach to the topic and its involved features, we use the definition of information security proposed by Cherdantseva and Hilton, which states that:

> *"Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats. Threats to information and information systems may be categorised and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability."* [43] (p. 191).

Following this definition, we include as information security-related topics the following dimensions: confidentiality, integrity, availability, privacy, authenticity, trustworthiness, non-repudiation, accountability, and auditability. It is worth noting that, according to this definition, privacy is considered as a component of information security and, therefore, *embedded* in the information security concept. However, being privacy distinguished as a human right by the European Court of Human Rights [44], we consider privacy as a sufficiently important topic to justify a distinctive analysis throughout this research.

2.3. Literature Search

This phase involves: database selection, keyword search, backward and forward search, and an ongoing evaluation of the sources [38]. We have followed a strict review protocol, based on the Preferred Reporting Elements for Systematic Reviews (PRISMA) statement [45], that is summarized in Figure 2. For the sake of reproducibility, in this section we elaborate on the steps and decisions made to select and analyze the literature resulting from the application of this review protocol, namely the search strategy, and the data collection and analysis.

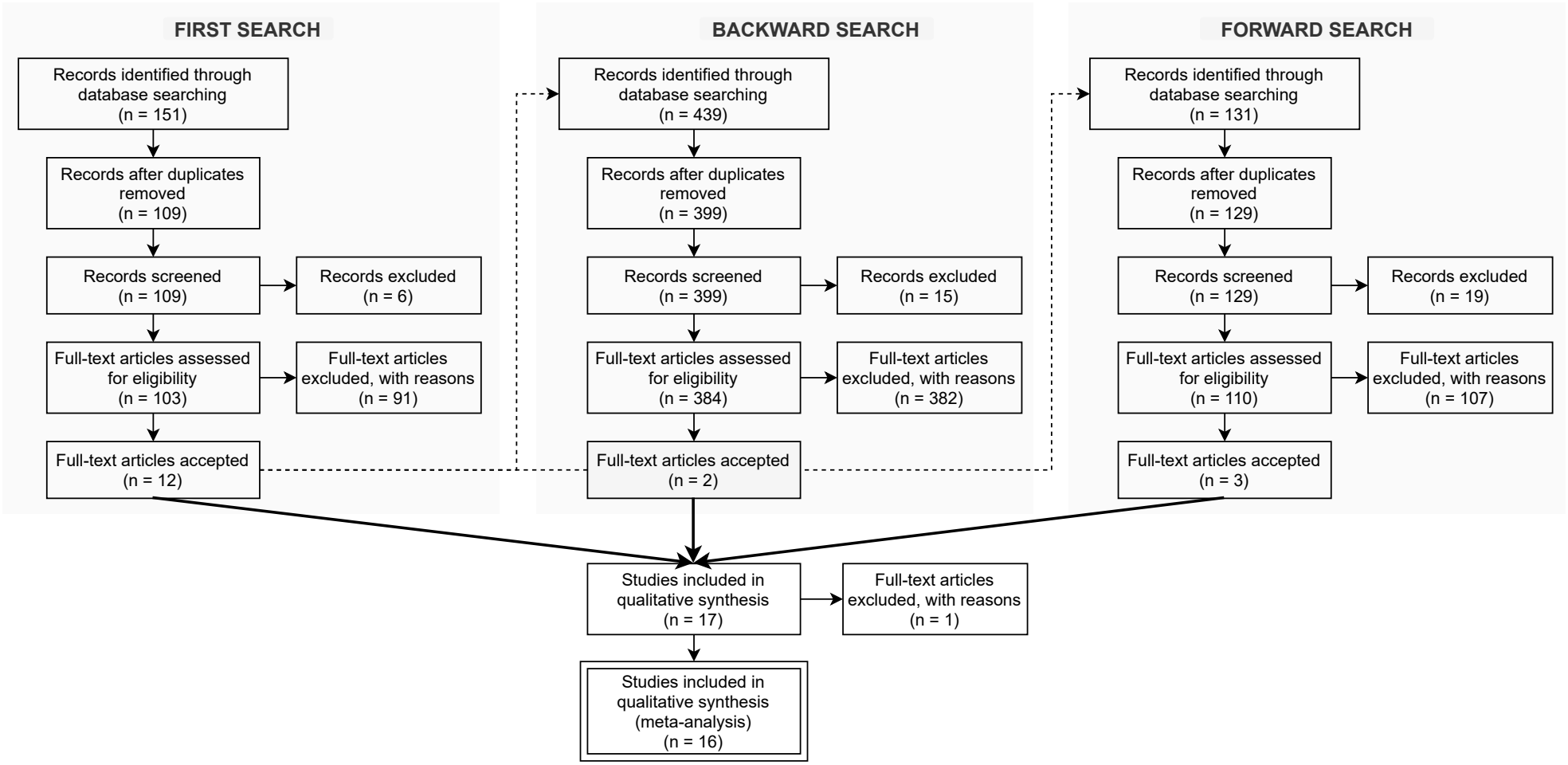

Figure 2. Literature search evaluation methodology.

2.3.1. Database Selection

To ensure the quality of the contributions, Vom Brocke et al. suggest to identify the leading journals in the field and then choose the databases providing access to those journals. However, to the best of our knowledge, there is no specific journal on cognitive cities. To find journals that have published articles on the cognitive city topic, on July 2020 we searched in the *Web of Science* database. We searched for articles having the topic (*"cognitive city" OR "cognitive cities"*) with an *all years* timespan (1900 to 2020), and refined the results by *article* document type. The query returned 16 references, 15 of which were book chapters and only one was a journal article published in the *Journal of Place Management and Development*. Given the reduced number of journals identified, this procedure is deemed unsuitable to determine the data sources of this study. Alternatively, we selected four well-known and widely recognized on-line databases as our publications sources: *ACM Digital Library*, *IEEEXplore*, *SCOPUS*, and *Web of Science*, to thus guaranteeing the coverage of our research and including high quality references.

2.3.2. Keyword Search

With the aim to avoid any misconception, the keywords on cognitive cities were limited to "cognitive city" or "cognitive cities". Moreover, given that information security is a multi-faceted concept which encompasses multiple goals, the search string was built using the key terms identified in the topic conceptualization stage. By doing so we avoid missing any article that focuses on a particular dimension of information security and, at the same time, we avoid limitations derived of not having specified other synonyms. The resulting search string was the following:

> *ALL (("cognitive city" OR "cognitive cities") AND ("security" OR "privacy" OR "confidentiality" OR "integrity" OR "availability" OR "authenticity" OR "trustworthiness" OR "non-repudiation" OR "accountability" OR "auditability"))*

Given the different features of the databases, we had to adapt the search string used to each database, named *S1*, *S2*, *S3*, and *S4*. Table 1 shows the strings used on each database and the number of obtained results.

- *S1* was used to query the *ACM Digital Library*, with the *advanced search* feature and selecting *Anywhere* on the *Search Within* combo.
- *S2* was used to query the *IEEEXplore*, with the *command search* feature.
- *S3* was used to query the *Scopus* database with the *advanced search* feature.
- *S4* was used to query the *Web of Science* database with the *advanced search* feature.

With the aim to obtain the widest possible coverage on the topic, we did not apply any timespan criteria to our search. Inasmuch as no lower bound was set, we fetched from the oldest eligible year on each database. Also, we did not set an upper bound on the publication date either. We searched the databases during July 2020. Further details and the specific search dates are given in Section 3.

Data extraction was performed in several stages. First, we exported to BibTeX format the resulting references from each query. Then, we imported the BibTeX files into a shared Mendeley database.

Table 1. Search strings used to query the databases and number of results (first search).

Database	Search Feature	Query	Results
ACM DL	Advanced search (*Anywhere* on the *Search Within* combo)	[[All: "cognitive city"] OR [All: "cognitive cities"]] AND [[All: "security"] OR [All: "privacy"] OR [All: "confidentiality"] OR [All: "integrity"] OR [All: "availability"] OR [All: "authenticity"] OR [All: "trustworthiness"] OR [All: "non-repudiation"] OR [All: "accountability"] OR [All: "auditability"]]	6
IEEExplore	Command search	("Full Text .AND. Metadata":"cognitive city" OR "Full Text .AND. Metadata":"cognitive cities") AND ("Full Text .AND. Metadata":"security" OR "Full Text .AND. Metadata":"privacy" OR "Full Text .AND. Metadata":"confidentiality" OR "Full Text .AND. Metadata":"integrity" OR "Full Text .AND. Metadata":"availability" OR "Full Text .AND. Metadata":"authenticity" OR "Full Text .AND. Metadata":"trustworthiness" OR "Full Text .AND. Metadata":"non-repudiation" OR "Full Text .AND. Metadata":"accountability" OR "Full Text .AND. Metadata":"auditability")	42
Scopus	Advanced search	ALL (("cognitive city" OR "cognitive cities") AND ("security" OR "privacy" OR "confidentiality" OR "integrity" OR "availability" OR "authenticity" OR "trustworthiness" OR "non-repudiation" OR "accountability" OR "auditability"))	88
Web of Science	Advanced search	ALL = (("cognitive city" OR "cognitive cities") AND ("security" OR "privacy" OR "confidentiality" OR "integrity" OR "availability" OR "authenticity" OR "trustworthiness" OR "non-repudiation" OR "accountability" OR "auditability"))	15

2.3.3. Literature Evaluation

We analyzed whether the results fulfilled the following inclusion and exclusion criteria: publications were included if they contained any valid keyword combination AND were peer-reviewed research literature (to avoid grey literature) AND full-text was available AND were relevant to the subject. For our purposes, *relevant* means that the publication contextualizes information security and privacy issues of the cognitive city, and that the keyword terms are used within the intended lexical context. This excludes, e.g., those articles in which the terms only appear in the references section, and those resulting from typos. We excluded duplicated publications and those that did not meet the inclusion criteria. The selection process was performed in two stages:

- Step 1: We removed duplicate publications.
- Step 2: We performed an abstract and full-text screening to limit the literature review to only those articles that fulfilled the inclusion criteria. During the screening, we classified each article as: *1, accepted* (i.e., the article is relevant, according to the inclusion criteria) or *0, rejected* (i.e., the article is not relevant according to the inclusion criteria).

With the aim to lessen researcher bias, a cross-checked evaluation was conducted among several researchers, each of them independently classifying the articles according to the aforementioned criteria. To this end, we uploaded the references to a shared repository and sorted them alphabetically by title. Then, references were assigned to reviewers as follows: odd-numbered references were assigned to reviewer number one, even-numbered references were assigned to reviewer number two, lower-half references were assigned to reviewer number three, and higher-half references were assigned to reviewer number four.

For the sake of completeness, we followed a *conservative* approach for the screening. That is: a reference was considered *accepted* if it had at least one favorable assessment. Conversely, a reference was *rejected* if and only if it did not get any positive vote. We created a form to register and summarize the voting procedure, containing: reference number, title,

authors, year of publication, and reviewers assessments. Each assessment included vote and reason.

2.3.4. Backward and Forward Search

Vom Brocke et al. suggest to perform a *backward search*, i.e., reviewing older literature cited in the selected articles, and a *forward search*, i.e., reviewing additional sources that have cited the selected articles. Vom Brocke et al. suggests using the Web of Science database for the forward search. We selected Scopus, instead, because it had the highest number of results in first search (see Table 1). Following this approach, we conducted a backward search and, then, a forward search using *Scopus* for all the articles accepted in the first search, getting a new set of publications which we evaluated again following the procedure described in Section 2.3.3. This iterative approach enables a more in-depth literature search, thus making our review more robust.

2.4. Literature Analysis and Synthesis

We performed a quality assessment to address discrepancies between researchers in the previous steps. Articles with dissenting votes were discussed among the four reviewers over several meetings, to find out to which extent the accepted articles fulfilled the inclusion criteria. A poll was then conducted and any article not achieving a majority of votes was filtered out.

The analysis of accepted references involved full-text readings and the extraction of all relevant information. With the aim to generate new knowledge grounded on the selected articles, we chose a conceptual synthesis approach to identify common themes across the articles and grouped the privacy or security issues into categories (e.g., willingness to share, data integrity and quality issues, IoT-related privacy problems, etc.), and we distinguished between three types of issue: technological, societal, or regulatory.

We created a form to collect the information required for our analysis and literature synthesis. For every publication, we registered: title, year of publication, bibliographic reference, text excerpts, whether it was privacy-related, or security-related, or both, issues identified, type of issue, issue category, main focus, and proposals made by authors. A summary of the form is shown in Table 2.

2.5. Research Agenda

The purpose of this literature review is not only to survey what has been studied in the field, but also to provide solid foundations for further research on the topic. Based on the results of our study, in Section 5 we suggest further research lines.

Table 2. Accepted articles analysis.

Ref.	Excerpts	Issues	P/S	Proposals
[46]	*"The main challenge for urban governance is achieving the conflicting goal of enhancing accessibility to resources, security, and empowerment of citizens at the same time."*	Balance and trade-off.	S	-
	"The significant point is to secure the shared data (particularly those who were shared with citizens) and to verify correct information is used in analytics and thus, making policies. The procedures for verification of authenticity, sanitation of data, and security of the anonymous information and ultimately knowledge bases, should also become a part of urban governance in cognitive cities. Only the secure data should be shared through city dashboards in public or through smart phone applications."	Authenticity and integrity of anonymous data used for analytics and policy making.	S	Integration of the procedures for verification of authenticity, sanitation of data, and security into urban governance in cognitive cities. Only secured (anoynmized and sanitized) data should be shared through city dashboards.
	"Privacy, security, and understanding of human behaviour are main challenges of network society and user experience design and social computing are the tools that can be considered to deal with these challenges."	Privacy and security as challenges of the network society (unspecified).	P/S	user experience design and social computing
[5]	*"Also, it is essential to consider the risks, which are not few, and might prevent the early adoption of the concept. In this sense, focusing on the healthcare domain, we have to learn from the errors of the past and avert the privacy and security problems of mobile health and smart healthcare. Important challenges in data security and privacy, accountability, transparency, and ethical issues must be addressed"*	Privacy and security challenges (unspecified) that might impede the development of the concept.	P/S	Briefly advises to learn from the errors of the past and avert the privacy and security problems of mobile health and smart healthcare, citing technical-related articles.
[47]	Privacy in IoT: *"Potential harm is amplified in the IoT by the scale and greater intimacy of personal data collection"*, *"Privacy breach (i.e., when a thing is put online, it remains online)"*, *"Privacy requirement in the IoT is currently only partially covered"* Vs privacy in WoT: *"Potential privacy violations (i.e., Web services having drawbacks)"*, *"Public sharing might result in serious privacy implications"*, *"Standard protocols for securely encrypting data between clients and servers on the Web"*	IoT-related and WoT-related privacy issues.	P	
	Security in IoT: *"Vulnerable to attack (e.g., unattended components, wireless, communications, low capabilities of energy and computing resources)"*, *"Possibility of personal data being stolen"*, *"Security problems"* Vs security in WoT: *"Secure interactions with HTTPS"*, *"Less risky (i.e., constantly tested, updated, and fixed systems)"*, *"Authenticated and secure communication between clients and gateways with HTTPS and OAuth"*	IoT-related and WoT-related security issues.	S	Use WoT (it is more secure than IoT.)

Table 2. *Cont.*

Ref.	Excerpts	Issues	P/S	Proposals
	"However, both approaches are confronted by issues of privacy and security. In the IoT, privacy requirements are generally only partially addressed, which makes the connected devices highly vulnerable to attack. In the worst case, personal data might be stolen. In the WoT, the Web continues to display several drawbacks that could have serious privacy implications. However, by applying the HTTP programming model, particularly HTTPS, it is possible to offer authenticated, secure communication between mobile clients and gateways. In addition, there is less risk of attack because Web services are constantly used, tested, updated, and fixed. Even if the issues of security and privacy are difficult, the Web is better able to counter these challenges than the Internet."	IoT privacy requirements are generally only partially addressed and in Wot, the Web continues to display several drawbacks that could have serious privacy implications.	P/S	HTTPS to secure and authenticate communication between mobile clients and gateways. In addition, "less risk of attack".
[48]	*"Data should be checked for completeness, conformity, consistency, accuracy, duplication, and integrity, and good practices around data quality do exist. Data issues can also emerge from the integration, federation or conglomeration of data, and given the variety and volume of big data, testing this data can be a big task".*	Volume and variety of data complicates data integrity and quality testing.	S	A new global regulatory framework is needed to address invalid conclusions that may arise from data analysis difficulties.
	On predictive capabilities: *"Preemptive action is based on prediction and prediction on predictive algorithm based on social information and this curtails civil liberties replacing proof with risk estimates."*	Threats to civil liberties (predictive capabilities).	P	
	"Profiling individuals on the basis of their health, location, electricity use, and online activity raise risks of discrimination, exclusion and loss of control."	Discrimination, exclusion, and loss of control (profiling individuals).	P	
[49]	*"Privacy protections will be critical to the adoption of Cognitive City sensor technologies—individuals must feel comfortable that their privacy will not be violated as they move about in public spaces"*	Willingness of sharing information.	P	Privacy-by-design for every technology, system, standard, protocol and process that touches the lives and identities of citizens in a Cognitive City.
	"More broadly, privacy underpins freedom. Privacy relates to freedom of choice and exercising control in the sphere of one's identity or self—making choices regarding what personal information one wishes to share and, perhaps more importantly, what information one does not wish to share with others."	Threats to civil liberties: freedom of choice (depends on privacy).	P	
	"[. . .] the digitization of data has caused the definition of personal information to expand. It now includes, for example, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational information. Grey areas are also arising from the collection of metadata. In the case of our internet communications, the detailed pattern of associations revealed through metadata can be far more revealing and invasive of privacy than merely accessing the content of one's communications"	Patterns inferred from big data and metadata aggregation threatens privacy.	P	
	"individuals, with the growth of networked infrastructures and ICTs, no longer have complete control over one's own personal information. The potential exists for technology to become a surveillance tool that will diminish individual privacy, dignity and freedom."	Threats to civil liberties: technology as a surveillance tool.	P	

Table 2. *Cont.*

Ref.	Excerpts	Issues	P/S	Proposals
[49]	*"Users are concerned about lack of control, lack of transparency and more importantly privacy [. . .] So despite the promise of these technologies, in the context of a Cognitive City, there could be a backlash by citizens if their privacy is increasingly invaded, thereby diminishing any positive gains or benefits to be achieved"*	Willingness of sharing information.	P	
	"As data mobility increases vertically and horizontally, there is also less transparency for the individual to make informed decisions about the uses of their data. By removing the individual to whom the data relates, the potential for questionable data quality increases, as do false positives, lack of causality, inference-dependency and greater bias in the results."	Removing context (e.g. data anonymization) can bring concerns on data quality and result biases.	S	
	"Asymmetries of knowledge tend to foster asymmetries of power manifested by questionable data quality, lack of causality, inference-dependency, bias and false positives. Armed with greater and more detailed knowledge about its citizens, government organizations can embark on social engineering and manipulation, at an unprecedented scale."	Governments engaging in social engineering and manipulation.	S	
	Regarding cognitive systems (which learn from experience, generate and/or evaluate conflicting hypotheses, reports on findings, discover patterns in data, . . .): *"It is easy to see the impact on privacy of such a context computing system not to mention the security challenge. The fear is that the insights arising from such systems will be open to misuse by unauthorized individuals and that the system itself may be misused to further erode one's freedoms and liberty".*	Threats to civil liberties: misuse or unauthorized use of cognitive systems and their insights can erod freedom and liberty.	P/S	
	"The privacy challenge for MLA and other sensor based applications, whether deployed in the retail, health or other private or public sectors, is, ironically, the very objective of ubiquitous computing. [. . .] This very premise is one that permits the potential misuse of the technologies because of the lack of transparency and in turn, accountability to the individuals from whom the data is collected."	Lack of transparency and accountability of ubiquitous computing.	P	
	"[. . .] SmartData (or personal avatars) that can think, understand, learn and remember the needs and privacy preferences of the individual to whom the data relates. The goal is to surpass current limited and brittle data protection methods by being able to respond to unforeseen situations, adapt to novel threats, and provide an accurate and nuanced representation of an individual's privacy and data security preferences. This concept of a smart agent was extended to an application in the realm of intelligence-led surveillance. Privacy-protective surveillance (PPS) uses modern cryptography, to ensure that (a) any personally identifying information (PII) on any unrelated individuals is not collected by the intelligence agency and (b) in transactions associated with targeted activity, PII and the metadata of additional "multi hop" connections will be encrypted upon collection, analyzed securely and effectively, and only divulged to the appropriate authorities with judicial authorization (a warrant)."	-	P/S	Recalls the concept of SmartData and apply it to a privacy-protective surveillance scenario. Authors consider that this cognitive smartdata agent could learn and respond to unforeseen security or privacy situations.

Table 2. *Cont.*

Ref.	Excerpts	Issues	P/S	Proposals
[6]	*"For instance, the injection of tampered data into a cognitive system could lead to serious unwanted consequences, which could put in danger the very system and people lives. Assuring the trustworthiness and accuracy of communications among agents becomes essential."*	Integrity: injection of false data.	S	Securing communication among agents, for trustworthiness and accuracy.
	"Moreover, the massive collection of citizen data raises serious privacy concerns. Every component of the cognitive systems should be implemented with a privacy-by-design approach in mind, and the appropriate safeguards for the existing risks should be implemented and managed. Open data policies, needed to achieve citizens' involvement, will have to be balanced with strong privacy-preserving mechanisms."	The massive collection of citizen data raises serious privacy concerns.	P	Components built with a privacy-by-design approach and risk management, balancing open data policies with strong privacy-preserving mechanisms, and security risks analysis and management.
[50]	Preserving Security and Privacy: *"Data-driven machine learning approaches (e.g., deep learning) can be attacked by false data injection (FDI), which compromises the validity and trustworthiness of the system. Resilience against such attacks is a must for ML algorithms. Privacy preservation is another important factor since a large part of smart city data comes from individuals who may not prefer their data to be publicly available."*	Integrity: injection of false data.	S	ML algorithms should address false data injection and privacy preservation.
		Privacy preservation for ML algorithms.	P	
	On-Device Intelligence: *"Smart city applications also call for lightweight machine learning algorithms deployable on resource-constrained devices for hard real-time intelligence. This is also in line with the security and privacy preservation requirement since data is not transferred to the fog or cloud."*	-	P/S	On-device intelligence supported by lightweight ML algorithms, so that data is not transferred to the fog or cloud.
[51]	*"A further challenge is the protection of citizen's privacy. It is necessary that users of the meta-app allow processing all available information connecting different heterogeneous networks and systems to receive the best possible alternative for a decision-making. As it is a perfect target for attacks willing to disclose sensitive information from citizens, it is crucial to ensure the achievement of privacy within the metaapp to guarantee the fundamental right of them at all times[. . .] There is still a lot to do for the privacy issue and thus, important to develop techniques to enhance citizen's privacy."*	Protecting privacy from attacks.	P	
	"A limitation would be that the city, the application providers and the users all must be convinced that data privacy requirements are adhered to, as the meta-app can only reach its full capabilities with access to (open) data and information."	Willingness to share.	P	

Table 2. *Cont.*

Ref.	Excerpts	Issues	P/S	Proposals
[52]	*"The use of technology will not only increase the volume of data collected, but also the complexity of how systems interoperate with each other"*[...]. *"This poses a range of regulatory challenges, predominantly in the domain of data privacy, data security, and commercial liability when things go wrong. Current regulatory frameworks and legal policies are often not sufficient enough to deal with ownership of data, privacy protection, and security breaches"*	Regulatory challenges: privacy, security and liability in case of security breaches.	P/S	
	"Sharing data, be it through one's personal or home devices or in a public space, is becoming ubiquitous." [...] *"It is however unclear how privacy is or should be protected when data is transferred across multiple systems and technology owners. This includes the protection of personal information (e.g., social identity, health information, etc.), personal communication (e.g., emails, text messages), and personal behavior (e.g., information on daily routines)"*	Regulatory challenge: Ubiquitous nature of data makes hard to know how privacy should be protected.	P	
	"Another area of regulation that is becoming more complex is the issue of security and liability. Questions around who is responsible for security breaches or other accidents when machine to machine communication fails need to be resolved."	Regulatory challenges: liability in case of security breaches.	S	
	"[...]there will be a need for clear and transparent regulations around (data) privacy and security. This is especially important as citizens often do not have the knowledge and understanding of how they are interacting with technology and what the benefits and drawbacks might be."	Social: citizens do not have the knowledge and understanding of how they are interacting with technology and of the benefits and drawbacks.	P/S	A clear and transparent regulation on data security and privacy.
[53]	*"Addressing privacy and security concerns in more detail, however, will be an important point for the adoption of this kind of application. Preservation of privacy is of central concern to protect the user from ill will attacks or the sense of the Big Brother effect. The integration of privacy and security needs to be explored further in context with the prototype"*	Privacy preservation from attacks. Willingness to share (preservation from the Big Brother effect).	P	
[54]	*"An important consideration in secure system design is the ability to verify and validate the security of alternative systems architectures. In the case of smart infrastructure, verification and validation processes require suitable metrics that both represent the security of the cyber network as well as the physical processes it supports."*	The need for verifying the security of alternative systems architectures.	S	A triple-category security metrics intended to measure and assess the security level of infrastructures.
	[...]*"it is important that cyber security is considered as an integral part of the architecture rather than being added on as an afterthought"*		S	Cyber security must be an integral part of the architecture, and considered at the design stage.

Table 2. *Cont.*

Ref.	Excerpts	Issues	P/S	Proposals
[54]	*"Assuming that security metrics may be established by following the above guidelines, these metrics could then be used to compare two systems of the same type. The target security metrics could be used to verify whether designs were properly implemented. The vulnerability security metrics could be used to determine whether design goals for security were met. The usability security metrics could be used to determine whether the services provided by the infrastructure are themselves secure."*		S	Metrics proposed could be used to compare two systems of the same type: whether designs were properly implemented, design goals for security were met, or the services provided by the infrastructure are themselves secure.
	"Although systems engineering texts typically present cyber security as a non-functional requirement, increasingly frequent cyber security breaches have fostered recognition that security features are essential to the attribution of integrity and availability of the system as whole. Hence, systems as cyberdependent as a smart infrastructure must consider cyber security as a functional rather than a non-functional requirement" Also, the article considers availability-related metrics like mean time to failure (MTTF), mean time between failure (MTBF), and mean time to repair (MTTR).	Infrastructure availability.	S	
[4]	*"An important consideration for leveraging citizens as information providers in the urban environment is the issue of data privacy and security. This is an important area of research and policy within the cognitive city context. However, if only 1–2% of the urban population is willing to play an active role in the cognitive grid in exchange for better information access on urban infrastructure services, the implications would be dramatic. The details of such information exchanges have to be worked out in detail in each case, but current research at our research group focuses on frameworks and tools that enable such discussions between city governments and their constituents."*	Willingness to share	P/S	
[55]	*"Building cognition should not spoil but needs to coexist with security and privacy features. In the proposed framework, security and privacy are mainly considered through authentication and access control. Authentication provides the means to validate the identity of the user before s/he interacts with the system. Access control is used to regulate access to data and services (through access to the corresponding VOs/CVOs). In this respect, VOs/CVOs are created and managed with their associated policies and access rights, which define when, how, and to what extent the enclosed data/function can be disclosed."*	Balance and tradeoff: coexistence of cognition with security and privacy.	P/S	A cognitive management framework for IoT that uses authentication of the user before interacting with the system, as well as access control to data and services.
[56]	[. . .]*" the privacy menu was introduced. This functionality allows the user to decide which data will be shared only with the system (i.e., the data must be shared with the system because otherwise the meta-app would not work) without allowing other users to access it and which data can be shared in an anonymized manner with other users (which would allow the meta-app to be enhanced)."*	willingness to share	P	A privacy menu to allow the user to be in control: decide which data can be shared with the system and which data can be shared (anonymized) with other users.

Table 2. *Cont.*

Ref.	Excerpts	Issues	P/S	Proposals
[56]	*"One of the major challenges of the application of such a meta-app is the privacy issue, [...] One expert stated the importance of storing user information on secure servers and of encrypting all information transmitted to the internet. Additionally, it must be ensured that communication with third-party providers is secure and trustworthy. An expert proposed to address the privacy issue as a possible unique selling point by clearly stating the purpose of the assembled (and shared) information."*	Privacy is a challege for the use of the meta-app	P	Storing user information on secure servers and encrypt all the information transferred to the Internet. Additionally, assuring that communication with third-party providers is secure and trustworthy. An expert proposed to address the privacy issue as a possible unique selling point by clearly stating the purpose of the information.
	"The complexity is mainly technical but also business related and must address the question of willingness to share and provide data and interfaces to the meta-app."	Privacy: willingness to share is seen as a technical and social challenge.	P	
[57]	*"Data-driven ML approaches (e.g., DL) can be attacked by false data injection (FDI), which compromises the validity and trustworthiness of the system. Resilience against such attacks is a must for ML algorithms."*	Integrity: Data-driven machine learning can be attacked with false data injection.	S	ML algorithms must be resilient against false data injection.
	"Privacy preservation is another important factor since a large part of SC data comes from individuals who may not prefer their data to be publicly available [58]. ML algorithms should address these concerns to enable the wide acceptance of SC systems by organizations and citizens."	Privacy preservation for ML algorithms.	P	
	On-Device Intelligence: *"SC applications also call for lightweight ML algorithms deployable on resource-constrained devices for hard real-time intelligence. As intelligence is moving towards edge devices, increased computing power and sensor data along with improved AI algorithms are driving the trend towards ML run on the end device, such as smartphones or automobiles, rather than in the Cloud. This is also in line with the security and privacy preservation requirement because data is not transferred to the edge or Cloud."*	Limited resources of IoT devices make them vulnerable to attacks.	P/S	On-device intelligence with lightweight ML algorithms, so that data is not transferred to the cloud.
[58]	*"It is likely that citizens will not participate in urban learning processes if they are unsure whether the data they provide will be stored safely and if it is not transparent who will have access to the data. Privacy and data security are thus important concepts that cannot be ignored in city development. In future research, there should be a stronger focus on this aspect."*	Privacy: willingness to share is seen as a technical and social challenge.	P/S	Transparency.

3. Results

We queried the selected sources on 17 July 2020 and retrieved all publications indexed to the date. We searched for the aforementioned keywords in all fields (e.g., title, abstract, keywords, full-text, metadata, etc.). As a result of this search, we obtained 151 references. From those, 109 distinct references remained after duplicates were removed. Afterwards, six references were excluded because they were not articles, but table of contents, etc., and 103 references were assessed for eligibility. After full-text screening, 91 references were rejected and 12 publications were accepted by, at least, one reviewer.

From those 12 accepted publications in the first stage, we performed a backward search on 17 August 2020. The search returned 439 references. We excluded 40 duplicated references, plus seven references that had already come out in the first stage, and eight wrongly formatted references. Next, 384 distinct references remained and were screened following the same procedure. As a result, two new references were accepted by at least one reviewer and the other 382 references were rejected.

Finally, a forward search was performed on 1 September 2020, resulting in 131 references. Then, we excluded two duplicated references, plus 19 references that had already come out in the first stage, remaining 110 distinct references to be screened. The screening resulted in three references accepted by at least one reviewer and 107 being rejected.

Table 3 lists the selected articles. With the aim to enhance transparency, we provide the scientific community with the individual assessments made for each article screened. Records are available for replication in the Mendeley repository [59] and from our research group website (http://smarttechresearch.com/opendata/applsci2020/Screening.ods, accessed on 12 May 2021 . SHA-256 hash: 51B09258DB5E9163C052942F477074843EC10F5A 1893B4DBE4EC 8531976FA960).

Table 3. Articles selected from screening.

Search Phase	Reference	Title
First	Mansouri and Khansari [46]	A conceptual model for intelligent urban governance: influencing energy behaviour in cognitive cities
First	Machin and Solanas [5]	A review on the meaning of cognitive cities
First	D'Onofrio et al. [47]	Advancing cognitive cities with the web of things
First	Morabito [48]	Big Data and Analytics for Government Innovation
First	Cavoukian and Chibba [49]	Cognitive cities, big data and citizen participation: The essentials of privacy and security
First	Machin and Solanas [6]	Conceptual Description of Nature-Inspired Cognitive Cities: Properties and Challenges
First	Mohammadi and Al-Fuqaha [50]	Enabling Cognitive Smart Cities Using Big Data and Machine Learning: Approaches and Challenges
First	Kaltenrieder et al. [51]	Enhancing multidirectional communication for cognitive cities
First	Moyser and Uffer [52]	From smart to cognitive: A roadmap for the adoption of technology in cities
First	Kaltenrieder et al. [53]	Fuzzy knowledge representation in cognitive cities
First	Bayuk and Mostashari [54]	Measuring cyber security in intelligent urban infrastructure systems
First	Liu et al. [60]	Research on software quality evaluation for application of smart city
Backward	Mostashari et al. [4]	Cognitive Cities and Intelligent Urban Governance
Backward	Vlacheas et al. [55]	Enabling smart cities through a cognitive management framework for the internet of things
Forward	Kaltenrieder et al. [56]	Digital personal assistant for cognitive cities: A paper prototype
Forward	Al-Turjman and Houdjedj [57]	Learning in cities' cloud-based iot
Forward	D'Onofrio et al. [58]	Using fuzzy cognitive maps to arouse learning processes in cities

Inter-rater reliability (IRR): The average percent agreement between reviewers was 97.0% for the references gathered from the first search, 99.7% for the second (backward) search, and 100% for the third (forward) search. We calculated Cohen's κ values [61] for each pair of reviewers sharing publications, showing an agreement level ranging from *moderate* to *almost perfect*. Table 4 shows κ for the 95% confidence interval.

Table 4. Inter-rater reliability: κ values in every stage for each pair of reviewers sharing publications (95% confidence interval).

Stage	R1–R3	R1–R4	R2–R3	R2–R4
First search	0.65 ± 0.35	0.88 ± 0.12	1.00 ± 0	0.65 ± 0.35
Backward search	1.00 ± 0	1.00 ± 0	0.66 ± 0.34	1.00 ± 0
Forward search	1.00 ± 0	1.00 ± 0	1.00 ± 0	1.00 ± 0

Four of the 17 references accepted through the screening were accepted with discrepancies between reviewers (three from first search, and one from backward search). We conducted a final in-depth quality assessment to address discrepancies. Quality assessment involved an in-depth review of the full text of these articles and a meeting of the four reviewers to discuss the articles. A poll was then conducted and any article not achieving a majority of votes was filtered out. Table 5 shows a list of the articles accepted with discrepancies, together with the results of the quality control. Consensus among the four reviewers resulted in one article being filtered out and three references being accepted. Therefore, 16 references were finally accepted for literature analysis.

Table 5. Selected articles and quality assessment result.

Reference	QA1	QA2	QA3	QA4	Result
Machin and Solanas [5] (2018)	1	1	1	1	1
Morabito [48] (2015)	1	1	1	1	1
Liu et al. [60] (2015)	0	0	0	0	0
Vlacheas et al. [55] (2013)	1	1	1	1	1

The literature analysis involved extracting text excerpts related to the topic and classifying each issue found in the excerpts into: privacy or security-related, issue category, issue type (technical, societal, or regulatory). We also registered the main focus of each article (technical, societal, or regulatory), and proposals that authors made to address the identified issues. A condensed version of the data gathered during the analysis is shown in Table 2. Next, we summarize the findings.

3.1. Security and Privacy Challenges

In the literature about cognitive cities, privacy and information security are mainly regarded as important challenges that need to be addressed. For organizational purposes, we classified the challenges discussed in each article into technical, societal, or regulatory. Table 6 summarizes the main focus over privacy and security on each article.

Technical challenges mainly refer to:

Table 6. Articles and their main focus.

Article	Main Focus		
	Technical	Social	Regulatory
Al-Turjman and Houdjedj [57] (2019)	✓		
Bayuk and Mostashari [54] (2011)	✓		
Cavoukian and Chibba [49] (2016)	✓	✓	
D'Onofrio et al. [47] (2018)	✓		
D'Onofrio et al. [58] (2019)	✓	✓	
Kaltenrieder et al. [51] (2015)	✓	✓	
Kaltenrieder et al. [53] (2015)	✓		
Kaltenrieder et al. [56] (2016)	✓	✓	
Machin and Solanas [5] (2018)	✓		
Machin and Solanas [6] (2019)	✓		
Mansouri and Khansari [46] (2019)	✓		
Mohammadi and Al-Fuqaha [50] (2018)	✓		
Morabito [48] (2015)		✓	✓
Mostashari et al. [4] (2011)		✓	
Moyser and Uffer [52] (2016)			✓
Vlacheas et al. [55] (2013)	✓		

- Preserving citizen's privacy from disclosure attacks [6,47,50,51,53,56], and privacy preservation for ML algorithms [57].
- IoT-related privacy issues: privacy requirements partially covered [47], and that deleted online information can be recovered by experts [47].
- Data integrity and quality issues: the use of truthful information for analytics and governing policies [46,48,49], protections from false data injection for ML algorithms [6,50,57], the difficulties of data quality testing caused by the variety and volume of data and data sources [48], and data quality and bias concerns resulting from removing context from data [49].
- IoT-related security issues: unattended components, low computing and energy resources make IoT devices vulnerable to attacks [47,57], and security problems of IoT-supporting technologies [47].
- The need for measuring and verifying the security of alternative systems architectures [54].
- Data misuse caused by the lack of transparency and accountability of UC [49].
- Balance issues: coexistence of cognition with security and privacy [55], and the conflicting goal of enhancing accessibility to resources, security, and empowerment of citizens at the same time [46].
- And willingness to share also seen as a technical challenge [56,58].

Societal challenges are mainly oriented to:

- The willingness of citizens to actively share their information [4,49,51,56–58].
- Privacy and threats to civil liberties: predictive capabilities as a threat to privacy and civil liberties [48], the dangers of profiling individuals [48], privacy problems can erode freedom of choice [49], the effects on freedom and liberty of the misuse or unauthorized use of cognitive systems and their insights [49], and the risk that these technologies become a surveillance and manipulation tool against the society [49].
- The lack of knowledge and understanding of these technologies [52].

Regulatory challenges include (i) the need for transparent regulations on data privacy [48,52], (ii) liability in case of security breaches [52], and (iii) the difficulties of regulating data privacy, due to the ubiquitous nature of data [52].

3.2. Actionable Security and Privacy Proposals

Most of the analyzed articles discuss the need for privacy and security solutions and point out some of the main challenges that cognitive cities will face. However, only six articles present actual actionable proposals to face some of these issues [47,49,50,54–56]. We summarize them next:

In the context of a cognitive city mobile application, Kaltenrieder et al. [56] proposed a privacy menu that allows users to decide which data would be shared only with the system and which data would be shared in an anonymized manner with other users. Other aspects mentioned are: storing user information only in secure servers, using encryption, and clearly stating the purpose of the assembled (and shared) information.

Bayuk and Mostashari [54] discussed the need for taking into account cybersecurity aspects during the design process of the infrastructures that support smart and cognitive cities, and proposed to use a triple-category security metrics intended to measure and assess the security level of infrastructures. These metrics are (i) *target metrics*: a binary measure used to represent whether the system complies with a given standard configuration. Components would be weighted by component criticality and the compliance of each type of component would be measured separately. Finally, measures for each component type are aggregated, (ii) *vulnerability metrics*: consist of a vulnerability assessment combined with basic threat design, which describes how the system is likely to be attacked, and (iii) *usability metrics*, which test the ability of the system to provide the functionalities required by stakeholders.

Also in the design stage, Cavoukian and Chibba [49] proposed a privacy-by-design (PbD) approach that should be embedded into *"every technology, system, standard, protocol and process that touches the lives and identities of citizens in a Cognitive City"* [49] (p. 62).

This is an integrative approach to privacy and data protection measures, which includes technology, networked infrastructures, and physical design (besides policies, procedures, and operational processes). The proposed framework comprises seven principles that the aforementioned elements should fulfill: (i) proactive privacy, including managerial actions to demonstrate the value of privacy, a culture of continuous improvement, and advancing controls to detect and prevent privacy breaches, (ii) privacy as the default setting, with no action required to protect data, (iii) embedded into the design of technologies, operations and information architectures, (iv) avoiding the trade of privacy with other interests (e.g., performance), (v) end-to-end security–full life-cycle protection of confidentiality, integrity and availability, (vi) visibility and transparency of the policies and practices, and (vii) keeping interfaces *user-centric*, so that citizens are able to make informed privacy decisions in a reliable way. The authors also recall the concept of *SmartData* [62], as a cognitive web-based intelligent agent that holds an individual's personal information and the rules to protect security and privacy, so that the agent would be transmitted or stored as a proxy for data, not the personal information itself. The article considers that this cognitive SmartData agent could learn and respond to unforeseen security or privacy situations, and applies it for building a privacy-protective surveillance architecture. The architecture balances the collection of just the right significant data associated with terrorist-related activities by intelligence agencies and preserves privacy of other personally identified data, so that it would only be disclosed to the appropriate authorities for law enforcement.

Following a different approach, D'Onofrio et al. [47] suggested the adoption of the Web of Things (WoT) [63] as a more secure paradigm for building cognitive cities, instead of IoT, which is the most accepted approach for smart and connected cities. The authors stated that, despite the privacy problems of the Web, it is possible to offer authenticated and secure communications through the HTTPS protocol and, hence, lessen the risk of attacks *"since Web services are constantly used, tested, updated, and fixed"* [47] (p. 87). A new approach based on on-device *intelligence* with lightweight ML algorithms was proposed in Mohammadi and Al-Fuqaha [50], with the aim to avoid data transfers to other devices in the fog or cloud and, thus, strengthening privacy protection.

Following a different approach, to address the problem of balancing privacy and security with cognition, Vlacheas et al. [55] proposed a cognitive management framework for IoT that uses user authentication before interacting with the system and access control to regulate access to data and services.

Machin and Solanas [6] suggested that every component of the cognitive systems be implemented with a PbD approach in mind. Additionally, they suggested risk management and balancing the open data policies with strong privacy-preserving mechanisms. Regarding security, authors proposed to ensure data integrity, trustworthiness and accuracy of communications among the agents in the cognitive city. Mansouri and Khansari [46] proposed securing the channels of data collection through crowd sourcing and that only secured data is shared through city dashboards or through smart phone applications. They also pointed out to verifying that the *correct* information (authenticated and sanitized) is used in analytics, and that the verification procedures should become a part of urban governance in cognitive cities. They suggested using social computing and user experience design and to address privacy and security, as challenges of the network society (According to sociologist Manuel Castells, a network society is *"a society where the key social structures and activities are organized around electronically processed information networks"* . See http://globetrotter.berkeley.edu/people/Castells/castells-con4.html, accessed on 12 May 2021). Additionally, ref. [5] suggested to avoid the security and privacy problems of mobile health and smart healthcare paradigms.

There is a general lack of specific proposals regarding the social and regulatory issues. The need for a new legal framework to regulate life in the big data era, with special attention to data validation to make the right decisions was pointed out by Morabito [48]. Finally, Moyser and Uffer [52] mentioned the need for developing a city-wide regulatory framework around data privacy, data security, and liability.

4. Discussion

Cognitive cities have the sharing of citizen's information at their very core. Hence, privacy has been naturally identified as a general concern in most of the reviewed articles. Although privacy and security are widely identified as important challenges for the development of cognitive cities, few articles provide specific proposals to solve those problems. Furthermore, through our literature analysis we could identify only one article specifically focused on the topic (cf., [49]) and another one on measuring security for intelligent urban systems of smart and cognitive cities (cf., [54]). The rest of the articles merely refer to privacy or security issues of cognitive cities without deep discussion.

Moreover, although agreement among reviewers were generally high, some values of κ (the coefficient measuring inter-rater reliability) were not very high (i.e., $\kappa = 0.65$), showing only a *moderate* agreement. This can be explained by the low ratio of accepted references, 2.67%, which makes the smallest disagreement count. The scarcity of articles addressing the topic, together with the low number of articles with actionable proposals found in the review—only six—, are indeed indicators of the lack of development in the field. Moreover, we could not find any literature survey on the topic, which suggests that this may be the first.

Given that cognitive cities will be fed by a constant flow of information from cognitive agents—humans and machines—solving these issues becomes fundamental before the adoption and deployment of the cognitive city paradigm in real-life urban scenarios. Moreover, security (which is multifaceted by nature) is usually reduced to its confidentiality dimension and, so far, only a small number of integrity-related issues have received some attention. Despite this lack of attention to security, in an urban environment cognitive and smart systems would become critical because they will make decisions on *highly valuable* assets.

Although we have followed a strict review methodology, the cognitive city field is still in its infancy and other related terms have been used in the literature to describe similar urban constructs. Therefore, although performing a strict search by the term *cognitive city* contributes to rigor, it may also bring some degree of incompleteness to the study. The same applies to only having used English terms as keywords. However, we have made every effort to adequately represent the concepts in the search.

Next, we elaborate on the challenges and opportunities we have identified from the literature analysis, grouped by themes.

4.1. Privacy and Security Are Entangled

Several privacy enhancing technologies can be applied in the sensing layer of the city hardware infrastructure. In fact, a framework for a comprehensive view of privacy could be envisaged, inspired by a 5-dimensional model for privacy in smart cities [17], namely: identity privacy (using pseudonyms to prevent the disclosure of citizens' identity), query privacy (preserving the privacy of the queries made by citizens to services), location privacy (guaranteeing the exact physical location of citizens is preserved), footprint privacy (related to the information that can be inferred from microdata sets), and owner privacy (focused on privacy-aware computation of queries across databases from different entities). PbD principles must be applied in this privacy framework globally. For instance, regarding visibility and transparency, all stakeholders (from local governments and information system managers to cognitive city technology developers) must be subject to independent verification; moreover, respect for user privacy is essential: information about good practices, down-to-earth notices, and user-friendly interfacing with the technology must be developed.

In this line, end-to-end security is regarded as a linchpin in PbD. This is a serious issue, because privacy and security are completely entangled: if technology fails, then privacy cannot be guaranteed. Therefore, strong built-in security measures are essential. As an example, proposals for trustworthy privacy-aware video surveillance rely on good privacy practices, but also on strong security properties of hardware and software

infrastructures [64], and they are the current subject of study of European projects such as Goodbrother (European Cooperation in Science and Technology—COST Action 19121 http://goodbrother.eu, accessed on 12 May 2021).

Furthermore, given that a cognitive city can be seen as a set of cognitive agents and the *connections* that the agents make among them, any privacy analysis of the cognitive city must consider the authentication and communication processes among those agents (e.g., requiring mutual authentication). However, the humongous quantity and variety of devices that take part in the cognitive city, makes the authentication and checking of data integrity challenging. Identity and Access Management (IAM) systems must cope with authentication mechanisms providing information security for citizens, information systems, websites, and things. Moreover, queries, use of web services, and any interaction between parties must consider access control. Current public-key authentication mechanisms, based on certificate chains, revocation lists, and multiple-sourced trust, are hard to fit into cognitive cities infrastructures. On the contrary, the single-sourced nature of blockchain makes easier to manage credentials verification and legitimacy.

To summarize, although PbD is a necessary starting point, it is not enough because serious problems in the cognitive city may arise from the security side.

4.2. Dealing with Legacy Software and Hardware Updates

While the cognitive city paradigm develops and gradually pervades our cities, different technologies are expected to converge and interact with each other within the urban arena. From *the old good* IoT devices to state-of-the-art ML systems, every single piece of hardware and software that comprises cognitive systems will play its part in the daily routines of citizens. Therefore, security vulnerability management processes must be planned thoroughly before deploying any technology, and periodically executed through all its life-cycle to detect security or privacy risks. Moreover, special care should be taken in managing obsolescence, so that discontinued or simply obsolete ICT components be identified beforehand and replaced by newer and patched equivalent products.

From a pure technological perspective, some new developments may help lessen the risks of using older technologies, by adding an extra layer of security on top of the latter. For example, with respect to the security problems of IoT, Ali et al. have suggested to take advantage of blockchain features [65], such as distributed consensus and pseudonymity, to address confidentiality and integrity issues. They have also argued that data modification attacks are useless in public blockchains, because there is no single point of attack, and that the cost added to making new transactions protects the network against flooding and DDoS attacks [66]. However, while in some of these examples the addition of an extra technological layer may help deter vulnerabilities exploitation, attackers will always try to find *the weakest link*, as long as the outcome worths the cost. For this reason, although WoT could be an improvement with regard to IoT, it is not the ultimate solution because there are still many privacy and security issues within the Web itself, which is built upon underlying protocols that have not been widely updated since they were created back in the past decades. As an example, the Domain Name Service (DNS) protocol, upon which the web relies, is still vulnerable to attacks such as cache poisoning, which can redirect data from a WoT device to some attacker-controlled infrastructure, thus affecting privacy and security of the information transmitted by the device. Fortunately, DNS security extensions, which provide DNS resolvers with cryptographic authentication of the retrieved data, and malware-aware public DNS resolvers, such as *Quad9* [67], pave the way for more secure name resolution services. Similar approaches could be adopted for name resolving tools in top-level domains used within the devices and information systems of the cognitive city ecosystem. Nevertheless, the interactions between coupling technologies must be analyzed to uncover new hidden security risks and attack vectors. For example, a study on the security issues of machine and deep learning algorithms coupled with IoT is provided in [68]. Moreover, new technologies can also introduce new unexpected risks, even when trying to protect from others. As Song et al. have shown in [69], adversarial defense

methods for ML models can increase vulnerability levels to privacy attacks. Also, Kwon et al. have highlighted in [70,71] the threats of adversarial examples in speech recognition systems, which may play a key role in the cognitive cities of tomorrow. Therefore, the integration of any new technology in the cognitive city environment must be studied thoroughly, for each layer of the architecture, to guarantee end-to-end privacy and security of citizens' data.

In summary, we sustain that ICT components will need to be managed over their entire life-cycles, from planning and integration to substitution and disposal stages, and the use of distinct technologies will require an in-depth study of its implications, particularly when mixing older with newer components.

4.3. The Balance between Computational Power and Intelligence

Regarding the discussion on the *location* of device intelligence (whether it resides within the device or in more complex distributed algorithms based on fog and cloud computing), we consider that on-device intelligence, or at least a certain degree of this ability, will be required to develop the full potential of cognitive cities. In particular, to be resilient, cognitive systems will need to operate autonomously, ideally with no central control, as cognitive agents. Thus, no single point of failure exists that could compromise the availability of the infrastructures and services enabling the cognitive city. At the same time, autonomy is an enabler for the type of flexible adaptive responses that are needed to address the ever-changing conditions of the real world [6]. To develop these autonomous agents, we suggest to adopt the *MAPE-K* reference model (monitor-analyze-plan-execute with knowledge), which is used in the fields of autonomic and self-adaptive computing [72,73].

Furthermore, infrastructures supporting cognitive city services will need a certain degree of self-awareness—i.e., the ability to sense their own state—to achieve real resiliency. Self-awareness would allow them to prevent, detect, and react autonomously to any event or failure that may affect their operation or mission or, alternatively, to alert an external *meta-cognitive* level which would manage disturbances accordingly. In addition, other desirable properties include self-reconfiguration and self-healing to recover from destructive events. Nevertheless, computational power of IoT devices will have to be improved to run the lightweight ML algorithms and blockchain-like features, needed to build secure cognitive city infrastructures.

In a nutshell, a trade-off between device intelligence and computational power is needed in order to meet availability and resiliency requirements.

4.4. The Role of the Physical Layer

Being cognitive cities cyber-physical systems [74], which integrate computational and physical processes to interact with humans, physical security must be also evaluated and managed because it has a direct impact on information security and privacy. Special attention should be put to the physical layer interface of the cognitive city. First and foremost, embodiements will need to be adapted to the environmental conditions of the city space in which they are located, such as weather conditions (e.g., average temperature and humidity), geographical conditions (e.g., altitude above sea-level), or pollution levels, so that they can operate reliably. Furthermore, societal features should be assessed too (e.g., criminality rate, percentage of elderly population), in order to adapt physical components and their interactive capabilities to specific sociological environments. In this line, physical protection mechanisms should be deployed for protecting physical assets against human threats, such as vandalism, robbery, or sabotage, whereas signaling and interfaces should be adapted for the elderly or impaired to avoid input errors and improve data quality. In addition, privacy-preservation methods, like differential privacy [75], must be studied from a cyber-physical perspective, and adapted to each *domain* of the cognitive city (i.e., water supply, energy, traffic and transportation, healthcare, home and living, government, etc.), as the survey on differential privacy methods in cyber-physical systems in [74] suggests. Last

but not least, given that information security issues can also have physical consequences, cognitive systems must be equipped with protected remote deactivation capabilities (i.e., secure *kill-switches* devices) to avoid dangerous situations for citizens.

In short, privacy and security threats derived from the physical world must be considered, and protection mechanisms adapted to the specific city space to detect, prevent, resist, or react to a wide range of physical threats. Besides deploying initial countermeasures at the design stage, these protective mechanisms should be built-in and managed over a continuous risk analysis process.

4.5. Data Integrity Is Fundamental

Data integrity becomes a crucial dimension in the cognitive city environment, because citizens and cognitive systems in the city are expected to learn from aggregated streams of information. Therefore, assuring that information is not tampered with and that it is generated by or sent to legitimate devices is fundamental. Additionally, regarding data quality for data mining and collective intelligence purposes, we need to pay attention to contents that might be automatically generated by AI conversational agents, especially when retrieving information gathered from online forums, websites, and social media, since it might not be easily distinguished from human-generated contents [76]. This issue is critical for developing reliable data-driven policies for government innovation and, therefore, it should be studied thoroughly. In addition, cognitive systems must be able to detect and resist Adversarial Machine Learning attacks, in which attackers use ML techniques, for example by supplying deceptive inputs to a ML algorithm [77]. Tangentially related to security, ML algorithms should be also carefully tested to avoid the *illusion inertial thinking* problem [78], i.e., poor generalizations as a result of applying concepts learned from one problem (that is, testing samples) to other significantly different problem, which can lead to wrong conclusions. This issue is particularly important given that the accuracy of ML methods depends on large number of training samples that may not always be available. Moreover, if these wrong conclusions are passed onto another system as inputs for a new cascading learning process, the deviation from the desired behavior can be considerable. Therefore, keeping data trustworthy and reliable is fundamental for a safe learning process.

4.6. A Unified View

The results of the backward search have revealed that the cognitive city paradigm emerges from the combination of a variety of fields and its development involves multiple technologies and paradigms, namely: cognitive computing, IoT, big data, cloud and fog computing, ML, natural language processing, multi-agent systems, etc. Although addressing the security and privacy issues of the underlying technologies is a starting point to understand their implications in the cognitive city arena, approaching these challenges from a technology basis only could be a mistake, because of the unexpected risks that arise as different technologies interact in different scenarios. Instead, we sustain that a holistic approach that takes into account the unique characteristics of cognitive cities is preferable. We advocate for a global Security by Default framework, especially designed for the cognitive city,

(i) that is built upon a formal description of the entities that constitute a cognitive city and their relations. This would require the creation of a cognitive city ontology.
(ii) that is based on a multi-layered model of the cognitive city, from the technological and agent layers, to the social interaction and city-level layers.
(iii) that encompasses all the stages in the life-cycle of cognitive products, processes, and services for the cognitive city, from the design and build phases, to the operation, monitoring, repairing, and disposal stages.
(iv) that takes into account the potential privacy and security risks that can arise in every phase and architecture layer.

(v) that includes a new specific threat model for cognitive cities, which should include goals, threat actors, attack vectors, and fault trees.
(vi) that includes metrics and risk assessment models to evaluate privacy and security at several levels (per individual, per building, per system, per district, etc.). These metrics should take into account the perspectives of several stakeholders, such as cognitive systems' manufacturers, infrastructures' providers, cities' councils, and citizens' fellowships, and balance their needs and requirements by using multi-criteria decision-making methods [79].

Moreover, in a globalized world, an internationally-accepted certification framework (led by certification bodies) on the basis of real-life urban scenarios could be created, and standards might be developed. This certification process would be required along the life-cycle of any cognitive system, and would complement law enforcement by transnational regulations.

4.7. User Awareness and Willingness to Share

Internet Users' Information Privacy Concerns (IUIPC) theory [80] can provide support for the willingness to share problem, which becomes a crucial issue for cognitive cities. According to IUIPC, the collection of personal data is perceived to be *fair* based on three factors: the perceived fairness of the outcome that the user receives (collection), the freedom to express an opinion or opt-out (control), and the degree of understanding of privacy practices (awareness), including transparency and ownership of information. Being willingness to share a fundamental requirement to make cognitive cities real, we suggest to address this challenge under the assumptions of IUIPC, namely providing the maximum degree of collection, control, and awareness to citizens. Perceived fairness will not only depend on the perceived benefits that technology can provide to citizens, but also on its drawbacks. First, privacy does not have to be at odds with user experience and, given the growing interest of citizens in preserving their privacy, vendors and service providers may incorporate privacy as an added valuable feature and a competitive business advantage [81]. Second, automatic data processing must strictly adhere to clear transparent practices so as to foster trust. In this line, a new *language* is needed to properly communicate the benefits and drawbacks of personal data gathering in a clear, concise, and understandable manner, especially taking into consideration the needs of elderly, handicapped, or unskilled people. Empowering users with the ability to make real-time interactive decisions about their data, such as the app menu proposed in [56], represents a starting point to achieve control over personal data, although it is hard for users to be aware of when they are sharing data, due to the ubiquitous nature of data acquisition in cognitive cities. Regarding opt-out mechanisms, they should take into account not only the data directly supplied by users, but also further processing of derivative information. In this sense, we sustain that a new enhanced blockchain-based smartdata concept is needed, to act like a locking mechanism in the cognitive city, regardless of whether data are original or derived. Finally, efforts should be made to narrow the digital divide, so citizens understand how they are interacting with the always-on ubiquitous technologies of cognitive cities.

4.8. Monitoring and the Human Factor

Given the possibly serious consequences of information security incidents in cognitive cities, they should be equipped with monitoring capabilities to detect and respond to security threats and anomalies. Security operational procedures should be developed and tested, and necessary data flows should be put in place and integrated into Security Operations Centers (SOC) to adequately detect and respond to events impacting the cognitive city infrastructures, services, or data. Besides the technological and procedural aspects involved, attention should be paid to the—often undervalued—human factor [82], because talent shortage, human errors, or coping behavior [83,84] can affect the mission of any organization. Particularly, and given the enormous amount of data expected, ML-based analytical and summarizing techniques should be developed to avoid *alert fatigue* of over-

whelmed SOC analysts. New promising security concepts, such as *cognitive security* [85] that takes advantage of the human-in-the-loop feature of cognitive cities, can help in the enormous task of monitoring and responding to security threats by integrating machine learning and decision support systems with the cognitive capabilities of security analysts. Last, human behavior-based risks must be also assessed and included in continuous risk management processes.

4.9. The Insider Threat

According to the *2020 Cost of Insider Threat Global Report*, both the number and cost of incidents caused by insiders have increased, reaching $11.45 million in the year 2020 [86]. Hence, besides external attacks, cognitive cities' designers should consider the chance of infractions committed by employees and contractual personnel responsible for the design, management, maintenance, or operation of cognitive cities' infrastructures and services, and include built-in risk analysis processes. In fact, addressing personal and social factors leading to attacks (e.g., detachment, social frustration, ethical flexibility, etc.) becomes paramount for the detection of shifts towards malicious actions before they happen [87]. An in-depth study should be conducted on this particular issue. We propose that it should be developed under the theoretical framework of *Rational Choice theory* [88–90], which suggests that infractors act in their own interest, based on a rational cost-benefit analysis process, when making a decision to commit a security policy violation. By lowering the perceived benefit or increasing the perceived cost of violation, some components of the potential risk can be adjusted, according to the asset value. For instance, a distributed database containing only portions of incomplete data that needs to be merged with others to be useful will be perceived as less valuable by offenders than a monolithic database. Rational choice theory has been used in [91] to support a risk analysis method against *rational* attacks. It is based on threat trees and comprises two stages: identifying the primary threats (ultimate goals for attackers) and breaking complex attacks into simpler ones and computing the threat tree to determine the most profitable attack. In addition, the pressure of being accountable—that is, the requirement of justifying one's actions to others—increases the likelihood of thinking deeply and systematically about one's behavior. Research has shown that Information Technology design artifacts can manipulate the core components of accountability and, thus, reduce intentions to commit access policy violation, without the need for disruptive interventions or training [92,93].

In summary, insider threats should be considered under the framework of behavioral theories, from the design to the operational stages of cognitive cities. Besides implementing technical security measures, a special focus should be placed on addressing the factors leading to attacks, and using education to foster engagement in and raise awareness about security and privacy practices.

4.10. Regulations and Digital Evidence

As we have discussed before, Ubiquitous Computing makes user awareness very complex. In addition, data protection regulations such as the European Union's General Data Protection Regulation (GDPR) make consent and awareness mandatory prior to data processing. This safeguard does not only apply to user-generated data, but also to derived secondary data, which is inferred from prior users' information, e.g., by ML algorithms. The fact that, in a cognitive city, data might be gathered opportunistically, and that GDPR requires a legal basis prior to data processing, makes it hard to balance the fulfillment of legal obligations with the development of innovative ubiquitous services. Technical and regulatory mechanisms should be developed to boost user awareness and guarantee consent across the ubiquitous landscape of cognitive environments. Furthermore, regulation complexity may grow as it is expected that cognitive city suppliers (e.g., cognitive system manufacturers, operators, and city services contractors) will be accountable under the laws of the *target* city territory or country, and that these laws may be in conflict with those of the supplier's country. Moreover, due to the diversity of technologies and scenarios that may

arise in the cognitive city environment, legal complexity can become intractable. In order to improve law enforcement across different jurisdictions and technologies, we suggest the development of an inter-operable markup policy language and protocol, so devices can automatically exchange data protection policies.

In the literature, liability has being identified as a concern. Hence it is expected that procedures for gathering evidence from massive amounts of data from cognitive systems will need international standardized procedures and techniques so as to capture, store, and process evidence data. This issue is particularly relevant because cognitive cities may become targets of cybercrime and terrorism. Blockchain is a promising technology to build a transnational trust system for digital evidence. In this sense, the European Union is currently developing several initiatives around technologies to enhance the fight against crime and terrorism, such as the *LOCARD* project, which aims to provide a platform for chain of custody assurance along the forensic workflow, through a blockchain-based trusted distributed platform allowing the storage of digital evidence metadata [94].

5. Conclusions and Further Work

In the field of cognitive cities, privacy protection and information security are mainly seen as open issues yet to be solved. By following a strict, reproducible and solid methodology, we have surveyed the literature, and have reported an analysis that reveals that the main focus of research attention has been set on privacy. However, little has been done to address the identified problems. The lack of actionable solutions is explained by the low number of relevant publications found, which reflects the youth of the field and the timeliness of this review. With this article, we have set solid ground for further studies in the emerging research field of Cognitive Cities, and we have discussed the most relevant topics that remain open. The following is a brief summary of the main takeaways:

- Privacy and security are interwoven and one can hardly achieve one without the other. In this sense, Privacy-By-Design approaches are a necessary first step, but security cannot be forgotten, for privacy cannot be guaranteed on an insecure basis.
- Legacy software and hardware might be a problem if they are not properly maintained: ICT components will need to be maintained over their entire life-cycles up to their very disposal, and the interaction between newer and older devices should be carefully monitored so as to guarantee proper interoperability and avoid leakages.
- Cognitive cities are complex cyber-physical systems and the physical layer has a decisive role in guaranteeing the security and privacy of citizens, which might be achieved through continuous monitoring processes. Moreover, the inherent distributed and heterogeneous nature of cognitive cities creates a huge attack surface that is hard to protect. Hence, efforts must be devoted to coordinate and efficiently harmonise the functioning of diverse technologies and devices, probably by fostering the creation of international standards and certifications.
- Cognitive cities are funded on learning processes, thus, it is paramount to guarantee the integrity of the data used in training and learning procedures. Also, the intelligence of the city agents will largely depend on their computational capabilities, and efficiently balancing the use of computational and communication resources among agents to maximise resiliency will be fundamental.
- Despite the importance of technology, the most significant aspect of Cognitive Cities is the Human Factor: It is essential to reduce the digital divide and to raise awareness on the security and privacy risks, hence providing citizens with the proper tools to share their data, collaborate and keep themselves safe. Also, it is essential to privately monitor the human interactions with the cognitive city so as to reduce or even avert errors, and lessen risks of insider attacks, which could be timely detected and the authors prosecuted by using strong evidence satisfying the highest international standards.

Promising research lines that deserve attention from the scientific community include: (i) balancing open and comprehensible data policies, that are needed for fostering citizen's participation, with strong privacy-preserving mechanisms, (ii) developing a new enhanced

smart data blockchain-based concept, to act like a locking mechanism in the cognitive city, regardless of whether data are original or derived, (iii) developing techniques to distinguish AI-generated contents, in order to build reliable data-driven policies for government innovation, (iv) introducing self-awareness capabilities into autonomous agents to make them able to detect and recover from outages, (v) balancing the fulfillment of user consent and the ubiquitous nature of cognitive environments in the city, (vi) developing information security standards on cognitive cities, (vii) developing ML-based analytical and summarizing techniques to avoid alert fatigue of SOC analysts, (viii) standardizing mechanisms and procedures to provide worldwide incontrovertible digital evidence, and (ix) enhancing existing models to achieve citizen's privacy in the cognitive city environment.

In conclusion, we have provided evidence that the field of cognitive cities is still in its infancy and many challenges and research lines related to security and privacy remain. We hope that this article helps to set the ground for further research and fosters the interest of the research community in this exciting field. Cognitive cities are still ahead in the future and, since information security and privacy are dynamic ever-changing issues, it is hard to imagine what new challenges future will bring to our cognitive cities. Chances are that, when cognitive systems begin to interact with citizens on a daily basis, new unforeseen privacy and security problems will arise. Only if we act in advance we will be able to avert these threats and guide the development of sustainable and resilient cities where technology is at the service of citizens.

Author Contributions: Conceptualization, J.M. and A.S.; methodology, J.M. and A.S.; validation, J.M., E.B., A.M.-B. and A.S.; formal analysis, J.M. and A.S.; investigation, J.M. and A.S.; resources, J.M.; data curation, J.M.; writing—original draft preparation, J.M. and A.S.; writing—review and editing, J.M., E.B., A.M.-B. and A.S.; visualization, J.M. and E.B.; supervision, A.S.; project administration, A.S.; funding acquisition, A.M.-B. and A.S. All authors have read and agreed to the published version of the manuscript.

Funding: The authors are supported by the Government of Catalonia (GC) with grant 2017-DI-002, by the GC with project 2017-SGR-896, and by Universitat Rovira i Virgili with project 2017PFR-URV-B2-41, and by the Spanish Ministry of Science & Technology with project IoTrain—RTI2018-095499-B-C32, and by the EU Commission with project LOCARD (Grant Agreement no. 832735) and COST Action 19121 Goodbrother. A.S. is partially supported by APWG.EU. Pictures designed by Freepik.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

AHP	Analytic Hierarchy Process
AI	Artificial Intelligence
DNS	Domain Name System
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IoT	Internet of Things
IRR	Inter-Rater Reliability
ISO	International Organization for Standardization
IUIPC	Intenet Users' Information Privacy Concerns
ML	Machine Learning
PbD	Privacy by Design
PRISMA	Preferred Reporting Elements for Systematic Reviews
WoT	Web of Things
SOC	Security Operations Center

References

1. Solanas, A.; Patsakis, C.; Conti, M.; Vlachos, I.S.; Ramos, V.; Falcone, F.; Postolache, O.; Perez-martinez, P.A.; Pietro, R.D.; Perrea, D.N.; et al. Smart health: A context-aware health paradigm within smart cities. *IEEE Commun. Mag.* **2014**, *52*, 74–81. [CrossRef]
2. Hall, R.E.; Bowerman, B.; Braverman, J.; Taylor, J.; Todosow, H.; Von Wimmersperg, U. *The Vision of a Smart City*; Technical report; Brookhaven National Lab.: Upton, NY, USA, 2000.
3. Siemens, G. Connectivism: A learning theory for the digital age. *Int. J. Instr. Technol. Distance Learn.* **2005**, *2*, 3–10.
4. Mostashari, A.; Arnold, F.; Mansouri, M.; Finger, M. Cognitive Cities and Intelligent Urban Governance. *Netw. Ind. Q.* **2011**, *13*, 4–7.
5. Machin, J.; Solanas, A. A Review on the Meaning of Cognitive Cities. In Proceedings of the 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), Zakynthos, Greece, 23–25 July 2018; pp. 1–5. [CrossRef]
6. Machin, J.; Solanas, A. Conceptual Description of Nature-Inspired Cognitive Cities: Properties and Challenges. In *Bioinspired Systems and Biomedical Applications to Machine Learning*; Ferrández Vicente, J.M., Álvarez-Sánchez, J.R., de la Paz López, F., Toledo Moreo, J., Adeli, H., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 212–222. [CrossRef]
7. Ashby, W.R. *An Introduction to Cybernetics*; Chapman & Hall Ltd.: London, UK, 1961.
8. Hundepool, A.; Domingo-Ferrer, J.; Franconi, L.; Giessing, S.; Nordholt, E.S.; Spicer, K.; de Wolf, P.P. *Statistical Disclosure Control*; John Wiley & Sons: Hoboken, NJ, USA, 2012; pp. 1–288. [CrossRef]
9. Machin, J. Triangulation-Based Multivariate Microaggregation. Master Thesis, Universitat Oberta de Catalunya: Barcelona, Spain, 2016.
10. Cheng, L.; Liljestrand, H.; Ahmed, M.S.; Nyman, T.; Jaeger, T.; Asokan, N.; Yao, D. Exploitation Techniques and Defenses for Data-Oriented Attacks. In Proceedings of the 2019 IEEE Cybersecurity Development (SecDev), Tysons Corner, VA, USA, 23–25 September 2019; pp. 114–128. [CrossRef]
11. Hern, A. Berlin artist uses 99 phones to trick Google into traffic jam alert. *The Guardian*. Available online: https://www.theguardian.com/technology/2020/feb/03/berlin-artist-uses-99-phones-trick-google-maps-traffic-jam-alert (accessed on 12 May 2021).
12. Ijaz, S.; Shah, M.A.; Khan, A.; Ahmed, M. Smart cities: A survey on security concerns. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 612–625. [CrossRef]
13. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*, 3–13. [CrossRef]
14. Hamid, B.; Jhanjhi, N.; Humayun, M.; Khan, A.; Alsayat, A. Cyber Security Issues and Challenges for Smart Cities: A survey. In Proceedings of the 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 14–15 December 2019; pp. 1–7. [CrossRef]
15. Ismagilova, E.; Hughes, L.; Rana, N.P.; Dwivedi, Y.K. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Inf. Syst. Front.* **2020**, 1–22. [CrossRef]
16. Dener, M. Cyber Security for Smart Cities. *Eurasia Proc. Sci. Technol. Eng. Math.* **2019**, *7*, 249–252.
17. 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]
18. van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [CrossRef]
19. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
20. Eckhoff, D.; Wagner, I. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 489–516. [CrossRef]
21. Curzon, J.; Almehmadi, A.; El-Khatib, K. A survey of privacy enhancing technologies for smart cities. *Pervasive Mob. Comput.* **2019**, *55*, 76–95. [CrossRef]
22. Barreno, M.; Nelson, B.; Joseph, A.D.; Tygar, J.D. The security of machine learning. *Mach. Learn.* **2010**, *81*, 121–148. [CrossRef]
23. Liu, Q.; Li, P.; Zhao, W.; Cai, W.; Yu, S.; Leung, V.C.M. A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View. *IEEE Access* **2018**, *6*, 12103–12117. [CrossRef]
24. Xue, M.; Yuan, C.; Wu, H.; Zhang, Y.; Liu, W. Machine Learning Security: Threats, Countermeasures, and Evaluations. *IEEE Access* **2020**, *8*, 74720–74742. [CrossRef]
25. Nelson, B.; Olovsson, T. Security and privacy for big data: A systematic literature review. In Proceedings of the 2016 IEEE International Conference on Big Data (Big Data), Washington, DC, USA, 5–8 December 2016; pp. 3693–3702. [CrossRef]
26. Binjubeir, M.; Ahmed, A.A.; Ismail, M.A.B.; Sadiq, A.S.; Khurram Khan, M. Comprehensive Survey on Big Data Privacy Protection. *IEEE Access* **2020**, *8*, 20067–20079. [CrossRef]
27. Salleh, K.A.; Janczewski, L. Technological, Organizational and Environmental Security and Privacy Issues of Big Data: A Literature Review. *Procedia Comput. Sci.* **2016**, *100*, 19–28. [CrossRef]
28. Aleisa, N.; Renaud, K. Privacy of the Internet of Things: A Systematic Literature Review. In Proceedings of the 50th Hawaii International Conference on System Sciences (2017), Hilton Waikoloa Village, HI, USA, 4–7 January 2017; pp. 5947–5956. [CrossRef]
29. Abi Sen, A.A.; Eassa, F.A.; Jambi, K.; Yamin, M. Preserving privacy in internet of things: A survey. *Int. J. Inf. Technol.* **2018**, *10*, 189–200. [CrossRef]

30. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
31. Grover, J.; Shikha; Sharma, M. Cloud computing and its security issues—A review. In Proceedings of the Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Hefei, China, 11–13 July 2014; pp. 1–5. [CrossRef]
32. Chiregi, M.; Jafari Navimipour, N. Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms. *J. Electr. Syst. Inf. Technol.* **2018**, *5*, 608–622. [CrossRef]
33. Kaur, J.; Agrawal, A.; Khan, R.A. Security Issues in Fog Environment: A Systematic Literature Review. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 467–483. [CrossRef]
34. O'Driscoll, C. Privacy in context: Privacy issues in Ubiquitous Computing applications. In Proceedings of the 2008 Third International Conference on Digital Information Management, London, UK, 13–16 November 2008; pp. 827–837. [CrossRef]
35. Ema, K.; Mark, S. A decade of security research in ubiquitous computing: Results of a systematic literature review. *Int. J. Pervasive Comput. Commun.* **2016**, *12*, 216–259. [CrossRef]
36. López, G.; Marín, G.; Calderón, M. Human aspects of ubiquitous computing: A study addressing willingness to use it and privacy issues. *J. Ambient. Intell. Humaniz. Comput.* **2017**, *8*, 497–511. [CrossRef]
37. Santos, C.M.d.C.; Pimenta, C.A.d.M.; Nobre, M.R.C. The PICO strategy for the research question construction and evidence search. *Rev. Lat. Am. Enferm.* **2007**, *15*, 508–511. [CrossRef]
38. Vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A. Reconstructing the giant: On the importance of rigour in documenting the literature search process. In Proceedings of the 17th European Conference on Information Systems, ECIS 2009. Association for Information Systems, Verona, Italy, 8–10 June 2009; Volume 9, pp. 2206–2217.
39. Webster, J.; Watson, R.T. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Q.* **2002**, *26*, xiii–xxiii. [CrossRef]
40. Cooper, H.M. Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowl. Technol. Policy* **1988**, *1*, 104–126. [CrossRef]
41. International Organization for Standardization. *ISO/IEC 27000:2018(E): Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary (2018) Standard*; International Organization for Standardization: Geneva, Switzerland, 2018; p. 27.
42. Cherdantseva, J.; Hilton, Y. Understanding information assurance and security. *J. Organ. End User Comput.* **2015**, *16*, 1.
43. Cherdantseva, Y.; Hilton, J. Information security and information assurance: Discussion about the meaning, scope, and goals. In *Organizational, Legal, and Technological Dimensions of Information System Administration*; IGI Global: Hershey, PA, USA, 2013; pp. 167–198. [CrossRef]
44. Council of Europe/European Court of Human Rights. *Guide on Article 8 of the European Convention on Human Rights*; European Court of Human Rights: Strasbourg, France, 2019.
45. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; Group, T.P. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Med.* **2009**, *6*, 1–6. [CrossRef]
46. Mansouri, M.; Khansari, N. A conceptual model for intelligent urban governance: Influencing energy behaviour in cognitive cities. *Stud. Syst. Decis. Control* **2019**, *176*, 185–202. [CrossRef]
47. D'Onofrio, S.; Franzelli, S.; Portmann, E. Advancing cognitive cities with the web of things. *Stud. Comput. Intell.* **2018**, *715*, 75–91. [CrossRef]
48. Morabito, V. Big Data and Analytics for Government Innovation. In *Big Data and Analytics: Strategic and Organizational Impacts*; Springer International Publishing: Cham, Switzerland, 2015; pp. 23–45. [CrossRef]
49. Cavoukian, A.; Chibba, M. Cognitive cities, big data and citizen participation: The essentials of privacy and security. In *Towards Cognitive Cities: Advances in Cognitive Computing and Its Application to the Governance of Large Urban Systems (Studies in Systems, Decision and Control (63))*; Portmann, E., Finger, M., Eds.; Springer International Publishing: Cham, Switzerland, 2016; Volume 63, pp. 61–82. [CrossRef]
50. Mohammadi, M.; Al-Fuqaha, A. Enabling Cognitive Smart Cities Using Big Data and Machine Learning: Approaches and Challenges. *IEEE Commun. Mag.* **2018**, *56*, 94–101. [CrossRef]
51. Kaltenrieder, P.; Portmann, E.; D'onofrio, S. Enhancing multidirectional communication for cognitive cities. In Proceedings of the 2015 Second International Conference on eDemocracy eGovernment (ICEDEG) , Quito, Ecuador, 8–10 April 2015; pp. 38–43. [CrossRef]
52. Moyser, R.; Uffer, S. From smart to cognitive: A roadmap for the adoption of technology in cities. *Stud. Syst. Decis. Control* **2016**, *63*, 13–35. [CrossRef]
53. Kaltenrieder, P.; Portmann, E.; Myrach, T. Fuzzy knowledge representation in cognitive cities. In Proceedings of the IEEE International Conference on Fuzzy Systems, Istanbul, Turkey, 2–5 August 2015. [CrossRef]
54. Bayuk, J.L.; Mostashari, A. Measuring cyber security in intelligent urban infrastructure systems. In Proceedings of the 2011 8th International Conference and Expo on Emerging Technologies for a Smarter World, Hauppauge, NY, USA, 2–3 November 2011; pp. 1–6. [CrossRef]

55. Vlacheas, P.; Giaffreda, R.; Stavroulaki, V.; Kelaidonis, D.; Foteinos, V.; Poulios, G.; Demestichas, P.; Somov, A.; Biswas, A.; Moessner, K. Enabling smart cities through a cognitive management framework for the internet of things. *IEEE Commun. Mag.* **2013**, *51*, 102–111. [CrossRef]
56. Kaltenrieder, P.; Papageorgiou, E.; Portmann, E. Digital personal assistant for cognitive cities: A paper prototype. *Stud. Syst. Decis. Control* **2016**, *63*, 101–121. [CrossRef]
57. Al-Turjman, F.; Houdjedj, A. *Learning in Cities' Cloud-Based IoT*; CRC Press: Boca Raton, FL, USA, 2019; pp. 209–234.
58. D'Onofrio, S.; Papageorgiou, E.; Portmann, E. Using fuzzy cognitive maps to arouse learning processes in cities. *Stud. Syst. Decis. Control* **2019**, *176*, 107–130. [CrossRef]
59. Machin, J.; Batista, E.; Martinez-Balleste, A.; Solanas, A. Dataset Privacy and Security in Cognitive Cities: A Systematic Review. *Mendeley Data* **2020**. [CrossRef]
60. Liu, Z.; Cai, L.; Hu, Y. Research on software quality evaluation for application of smart city. In Proceedings of the 2015 4th International Conference on Computer Science and Network Technology, Harbin, China, 19–20 December 2015; Volume 1, pp. 198–202. [CrossRef]
61. Cohen, J. A Coefficient of Agreement for Nominal Scales. *Educ. Psychol. Meas.* **1960**, *20*, 37–46. [CrossRef]
62. Tomko, G.J.; Borrett, D.S.; Kwan, H.C.; Steffan, G. SmartData: Make the data "think" for itself. *Identity Inf. Soc.* **2010**, *3*, 343–362. [CrossRef]
63. Duquennoy, S.; Grimaud, G.; Vandewalle, J.J. The web of things: Interconnecting devices with high usability and performance. In Proceedings of the 2009 International Conference on Embedded Software and Systems, Hangzhou, China, 25–27 May 2009; pp. 323–330. [CrossRef]
64. Rashwan, H.A.; Solanas, A.; Puig, D.; Martínez-Ballesté, A. Understanding trust in privacy-aware video surveillance systems. *Int. J. Inf. Secur.* **2016**, *15*, 225–234. [CrossRef]
65. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://nakamotoinstitute.org/bitcoin/ (accessed on 12 May 2021).
66. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717. [CrossRef]
67. Quad 9. Quad9 Frequently Asked Questions. Available online: https://www.quad9.net/faq/#How_does_Quad9_protect_me_from_malicious_domains (accessed on 12 May 2021).
68. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]
69. Song, L.; Shokri, R.; Mittal, P. Privacy Risks of Securing Machine Learning Models against Adversarial Examples. In *CCS '19, Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 241–257. [CrossRef]
70. Kwon, H.; Kim, Y.; Yoon, H.; Choi, D. Selective audio adversarial example in evasion attack on speech recognition system. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 526–538. [CrossRef]
71. Kwon, H.; Yoon, H.; Park, K.W. Acoustic-decoy: Detection of adversarial examples through audio modification on speech recognition system. *Neurocomputing* **2020**, *417*, 357–370. [CrossRef]
72. Kephart, J.O.; Chess, D.M. The vision of autonomic computing. *Computer* **2003**, *36*, 41–50. [CrossRef]
73. Kephart, J.; Chess, D.; Boutillier, C.; Das, R.; Walsh, W. An architectural blueprint for autonomic computing. *IBM White Pap.* **2006**, *31*, 1–6.
74. Hassan, M.U.; Rehmani, M.H.; Chen, J. Differential Privacy Techniques for Cyber Physical Systems: A Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 746–789. [CrossRef]
75. Dwork, C. Differential Privacy. In *ICALP'06, Proceedings of the 33rd International Conference on Automata, Languages and Programming, Venice, Italy, 10–14 July 2006*; Springer: Berlin/Heidelberg, Germany, 2006; Volume Part II, pp. 1–12. [CrossRef]
76. Macaulay, T. Someone Let a GPT-3 Bot Loose on Reddit—It Didn't End Well. Available online: https://thenextweb.com/neural/2020/10/07/someone-let-a-gpt-3-bot-loose-on-reddit-it-didnt-end-well/amp/ (accessed on 12 May 2021).
77. Huang, L.; Joseph, A.D.; Nelson, B.; Rubinstein, B.I.P.; Tygar, J.D. Adversarial Machine Learning. In *AISec '11, Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence, Chicago, IL, USA, 21 October 2011*; Association for Computing Machinery: New York, NY, USA, 2011; pp. 43–58. [CrossRef]
78. Li, H.; Wen, G. Modeling reverse thinking for machine learning. *Soft Comput.* **2020**, *24*, 1483–1496. [CrossRef]
79. Saaty, T.L. Decision making with the analytic hierarchy process. *Int. J. Serv. Sci.* **2008**, *1*, 83–98. [CrossRef]
80. Malhotra, N.K.; Kim, S.S.; Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Inf. Syst. Res.* **2004**, *15*, 336–355. [CrossRef]
81. Powers, B. Data Privacy as the New User Experience. Available online: https://martechseries.com/mts-insights/guest-authors/data-privacy-new-user-experience/ (accessed on 12 May 2021).
82. Nobles, C. Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA J. Bus. Public Adm.* **2018**, *9*, 71–88. [CrossRef]
83. Lazarus, R.S.; Folkman, S. Stress, appraisal and coping. *Assess. Coping Strateg.* **1984**, *56*, 267–283.
84. D'Arcy, J.; Herath, T.; Shoss, M.K. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *J. Manag. Inf. Syst. TA TT* **2014**, *31*, 285–318. [CrossRef]

85. Andrade, R.O.; Yoo, S.G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *J. Inf. Secur. Appl.* **2019**, *48*, 102352. [CrossRef]
86. Ponemon Institute LLC. *2020 Cost of Insider Threat Global Report*; Technical report; Ponemon Institute: Traverse City, MI, USA, 2020.
87. Colwill, C. Human factors in information security: The insider threat—Who can you trust these days? *Inf. Secur. Tech. Rep.* **2009**, *14*, 186–196. [CrossRef]
88. Paternoster, R.; Simpson, S. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law Soc. Rev.* **1996**, *30*, 549–583. [CrossRef]
89. Cornish, D.B.; Clarke, R.V. *The Reasoning Criminal: Rational Choice Perspectives on Offending*; Routledge: New York, NY, USA, 2017; pp. 1–246. [CrossRef]
90. Vance, A.; Siponen, M.T. IS security policy violations: A rational choice perspective. *J. Organ. End User Comput. (JOEUC)* **2012**, *24*, 21–41. [CrossRef]
91. Buldas, A.; Laud, P.; Priisalu, J.; Saarepera, M.; Willemson, J. Rational choice of security measures via multi-parameter attack trees. In *International Workshop on Critical Information Infrastructures Security*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 235–248.
92. Vance, A.; Lowry, P.; Eggett, D. Using accountability to reduce access policy violations in information systems. *J. Manag. Inf. Syst. TA TT* **2013**, *29*, 263–289. [CrossRef]
93. Vance, A.; Lowry, P.; Eggett, D. Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Q. Manag. Inf. Syst. TA TT* **2015**, *39*, 345–366. [CrossRef]
94. European Union. Lawful evidence collecting and continuity platform development. *Inf. Intell. Syst. Appl.* **2018**, *1*, 51–55.