

Review

Cybersecurity and Regulatory Compliance in Smart Cities: A Comprehensive Review

Maria Papaioannou ^{1,*}, Mila Georgieva Valcheva ¹, Metehan Gelgi ¹, Lejla Islami ¹ and Lars Sommer ²

¹ DTU Compute, Technical University of Denmark, 2800 Kongens Lyngby, Denmark; mival@dtu.dk (M.G.V.); metge@dtu.dk (M.G.); lejis@dtu.dk (L.I.)

² DTU Engineering Technology, Technical University of Denmark, 2750 Ballerup, Denmark; lasom@dtu.dk

* Correspondence: marpapa@dtu.dk

Highlights

What are the main findings?

- The review classifies smart city research across seven application domains, stakeholder groups, and regulatory-driven measures, showing how EU regulations are addressed in technical, organisational, and operational implementations.
- Regulatory requirements are unevenly reflected across domains and smart city solutions, with gaps in stakeholder roles, implementation maturity, and support for scalable and interoperable systems.

What are the implications of the main findings?

- Smart city development requires interdisciplinary approaches that integrate legal and technical perspectives, supported by clearer stakeholder roles, stronger governance, and active citizen involvement to ensure trust, accountability, and regulatory alignment.
- Further research should prioritise scalable and interoperable solutions and focus on translating regulatory requirements into concrete system design and implementation, moving beyond fragmented and localised approaches.

Abstract

Smart cities increasingly rely on urban digital systems deployed across domains such as mobility, public safety, surveillance, and governance, involving large-scale collection and processing of sensitive data. These systems raise significant cybersecurity and privacy challenges, shaped by European regulatory frameworks that influence how data are collected, secured, shared, and governed within urban environments. While existing research has examined legal and regulatory aspects alongside technical cybersecurity solutions, these areas are often addressed in isolation, limiting insight into how regulatory requirements translate into concrete implementations. This paper presents a comprehensive review of regulatory-driven cybersecurity approaches for smart cities. It maps the literature across major application domains and analyses how regulatory objectives are reflected in technical, organisational, and operational measures, as well as in implemented solutions. By jointly examining legal and technical perspectives, the review links regulatory compliance requirements with concrete security practices and system-level design choices. Based on this analysis, the paper proposes a structured classification of regulatory-driven smart city approaches and identifies key trends, gaps, and challenges in the literature. The findings provide a foundation for future research on regulatory-driven cybersecurity and privacy protection in smart systems.



Academic Editor: Pierluigi Siano

Received: 24 March 2026

Revised: 16 April 2026

Accepted: 22 April 2026

Published: 28 April 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

Keywords: smart cities; cybersecurity; privacy protection; urban digital systems; data governance; regulatory compliance

1. Introduction

In recent years, Europe has experienced an accelerated push toward digitalisation, driven by technological progress, as well as external pressures such as the COVID-19 pandemic and rising geopolitical tensions (<https://www.econstor.eu/bitstream/10419/331274/1/ITS-E-2025-29.pdf>, accessed on 15 December 2025). These developments have deepened the reliance of society on digital infrastructures and have exposed new vulnerabilities simultaneously. As cities expand their digital capabilities, the scale and complexity of cyber threats increase, making cybersecurity, resilience, and regulatory compliance essential components of sustainable digital development. This shift is also reflected in Europe's policy priorities, where digitalisation and cybersecurity now play a central role. Several European Union (EU) initiatives, including the Digital Europe Programme, which allocates €8.1 billion under the 2021–2027 framework (<https://digital-strategy.ec.europa.eu/en/activities/digital-programme>, accessed on 15 December 2025), emphasise that Europe's digital transformation must be supported by trustworthy, resilient, and secure infrastructures.

At the national level, Denmark illustrates this challenge clearly: although the country ranks among the most digitised countries in Europe, it places only 17th on the National Cybersecurity Index (<https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1>, accessed on 15 December 2025). This gap between high digitalisation and comparatively low cybersecurity readiness leaves organisations vulnerable to an increasing number of cyber threats and highlights the need to strengthen digital security capabilities. In parallel to this, the growing volume of data processed within smart city environments, including mobility patterns, biometric data, and behavioural data, raises significant privacy concerns. Large-scale digital traces can reveal sensitive insights about individuals, creating risks of profiling, misuse, or unauthorised surveillance [1]. Ensuring trust, transparency, and legal protection is therefore fundamental for the long-term viability and public acceptance of smart cities.

In response to the evolving threat landscape, the EU has introduced several new regulatory frameworks, including Network and Information Security Directive 2 (NIS 2) [2], the Cyber Resilience Act (CRA) [3], the Digital Operational Resilience Act (DORA) [4], and the Artificial Intelligence Act (AIA) [5]. These regulations impose extensive obligations on organisations to conduct risk assessments, implement appropriate security measures, and ensure lawful processing of personal data. However, the growing number and complexity of these legal instruments present challenges for both public authorities and private entities, who must navigate overlapping requirements and evolving compliance expectations.

Despite the central role of regulation in shaping secure and trustworthy smart cities, previous research has largely focused on technical security and privacy challenges, often without examining how proposed solutions align with EU regulatory obligations [6]. There is a limited understanding of how the scientific literature addresses regulatory-driven security and privacy technical measures, or how these requirements are operationalised in concrete technical implementations. This gap motivates the present work.

This research is conducted in the context of the Interreg Denmark–Sweden project [Interreg ØKS: InnoTech 20358659], which aims to strengthen cybersecurity competence, competitiveness, and readiness in the Øresund region through cross-border collaboration. Within this broader initiative, the objective of our work is to assess the current state of the scientific literature on regulatory-driven cybersecurity approaches for smart cities, with

particular attention to the measures, requirements, and needs emerging at the intersection of technology and EU regulation in regard to cybersecurity and smart city service development. To address this objective, this work investigates the following research question:

What is the current state of the art of cybersecurity solutions for smart cities that address EU regulatory requirements?

To answer this question, we conduct a comprehensive review to examine how privacy, security, and legal compliance are addressed in implemented smart city solutions as well as in conceptual analyses of relevant EU regulatory frameworks. By analysing the interplay between technological approaches and regulatory requirements, this paper aims to provide insights that can support decision-makers, city planners, and technology developers in designing trustworthy and resilient smart city ecosystems. We postulate that the results can benefit the local decision-makers and city planners (e.g., the city of Copenhagen) in developing smart societies that prioritise citizens' trust, safety, and well-being. Guided by this research question and established review guidelines, this work makes five main contributions, which are complemented by constructive reflections and a broader discussion. In particular, the contributions are the following:

- First, it classifies the reviewed works across seven application domains, revealing clear differences in how EU regulations are addressed.
- Second, it identifies the main stakeholder groups appearing across the literature and shows that their roles are often shaped by the regulatory frameworks discussed in each paper, with citizens largely treated as passive data subjects.
- Third, it synthesises the cybersecurity and data protection measures proposed in the reviewed studies into three main categories: technical, organisational, and operational, and it analyses how these measures support regulatory compliance.
- Fourth, it identifies all implemented and validated smart city solutions and evaluates them in terms of scalability, interoperability, usability, and regulatory compliance, highlighting common patterns and existing gaps.
- Fifth, this review provides an overview of how cybersecurity solutions for smart cities address key EU cybersecurity and data protection regulations. This analysis highlights which regulatory aspects are most commonly reflected in existing solutions and where gaps remain.

Finally, based on the synthesis of all reviewed works, this review discusses relevant trends and gaps, challenges and risks, recommendations and good practices, as well as legal perspectives concerning regulatory ambiguity and gaps in the current EU regulatory landscape.

The remainder of this paper is structured as follows. Section 2 presents the background information about the smart city paradigm, EU regulations on smart cities, and local implications of regulations in Denmark. Section 3 describes the methodology used for our review. Section 4 presents the main results in terms of application domains, stakeholders, measures, smart city solutions, and key EU regulations covered in this paper. Section 5 discusses and assesses results in terms of trends and gaps, challenges and risks, recommendations, and legal perspectives. Section 6 gives an overview of the related work. Section 7 finally provides the main conclusions of our work.

2. Background

This section introduces the core concepts underlying this work, including the definition of smart cities, associated privacy and security goals, and the role of EU cybersecurity and data protection regulations in the context of smart city systems.

2.1. Smart City

Smart cities have emerged as a new paradigm that uses digital and networked technologies to enhance service delivery, resource efficiency, and overall quality of life. While there is no common definition for smart cities that is accepted by related work on the topic, NIST Technical Publication 1900-206 [7] defined smart cities as the efficient and effective use of digital technologies to provide prioritised, high-quality infrastructure services and community benefits. These benefits include improvements in transportation systems, smarter energy grids, more responsive public services, enhanced healthcare, and other areas of city life. A smart city integrates Internet of Things (IoT) devices, sensors, network infrastructure, software systems, client devices, big-data analytics, and Artificial Intelligence (AI) to interconnect and coordinate critical urban components and services [8]. Together, these technologies collect data from different sources (e.g., traffic sensors, Closed-Circuit Television (CCTV), mobile devices), process, and act on large volumes of real-time data.

These data-intensive infrastructures raise important privacy and security considerations, as they often process sensitive personal and behavioural information across interconnected systems. Unauthorised access or misuse of such data can result in privacy violations, data linkage attacks, and data manipulation. Hence, robust protection measures are an indispensable requirement for the reliable operation of smart city solutions. Furthermore, the same technologies allow for identification, profiling, and surveillance of individuals and pose privacy and security threats as well as undermining other fundamental human rights [9]. Hence, the core idea of the democratic developments is put in question. Smart city data collected in public environments is further vulnerable to function creep, where information gathered for legitimate purposes is gradually repurposed for broader or more intrusive uses. For instance, data originally collected to optimise traffic flow, when combined with facial recognition systems, could be redirected to track individuals or monitor protest activities, creating the risk of intrusive monitoring and overreach by law enforcement authorities [10].

2.2. Regulations on Smart City

This section provides a brief overview of key EU cybersecurity and data protection regulations relevant to smart city implementations. Rather than offering an exhaustive legal analysis, the aim is to contextualise these instruments in relation to the classification presented in Section 4. This limitation is motivated by our research focus: reviewing the cybersecurity regulatory-driven solutions for smart cities. Because the use of such technologies has the potential to endanger the privacy and other fundamental rights of individuals, the EU is well-positioned to take a fundamental-rights and risk-based approach to technology regulation [11], as reflected in emerging regulations. Hence, the regulations are seen in the EU as a proxy for the protection of individual fundamental rights related to smart city data-driven technologies. These legal instruments govern the legal, ethical, behavioural, and standardisation aspects of privacy, data protection, and security. There are fundamental divergences, but also similarities and overlaps between the cybersecurity laws.

The General Data Protection Regulation [12], applied since 2018, establishes a harmonised framework for personal data protection, including principles such as lawfulness, purpose limitation, data minimisation, and accountability. In the context of smart cities, of particular importance is the obligation to the data controllers to comply with the Data Protection by Design (DPbD) enshrined in Art 25 GDPR. This principle demands the adoption of technical and organisational measures to be in place to implement the data protection principles effectively and enforce these requirements throughout the lifecycle of system development. It also imposes the implementation of the necessary safeguards in the processing of personal data. Similarly, the risk-based approach under GDPR is represented

by the obligations to carry out Data Protection Impact Assessment (DPIA) to address the risks to data protection and, in general, fundamental rights of data subjects.

With the recent introduction of AI systems in different application areas, the EU introduced the AI Act (AIA) [5], which is the first attempt globally at horizontal regulation of trustworthy AI systems [13]. It focuses on mitigating the risks AI poses to human rights; hence, Europe aims to move from a data-protection approach to a human-rights-based approach with the development and design of AI systems. Fundamentally, the AIA seeks to adopt a human-centred, ethical, and value-based approach, even though it is less flexible and less focused on protecting citizens' rights than the GDPR. Similar to the GDPR, though, the AIA follows a risk-based approach for technology regulation. Aiming to prohibit AI applications that have a negative impact on human rights, the regulation mandates risk management, conformity assessments, and continuous evaluation of system performance and biases.

A very important aspect of the proposed regulations is the fact that they are part of a tranche of regulations and directives and need to be analysed and considered jointly due to overlaps and interactions. One of these examples is the case of the AIA and other related regulations, such as the Digital Services Act (DSA) [14], the Digital Markets Act (DMA) [15], and the Data Governance Act (DGA) [16], and their considerations of AI systems, hardware, or services. For example, regarding the high-risk AI recommender systems, DSA has explicit rules for transparency—explaining how recommender systems work or the DMA rules for gatekeepers in order to prevent unfair access to data. Likewise, even though the act bans some uses of real-time biometric systems by law enforcement, the Law Enforcement Directive (LED) [17] from 2016 takes precedence and would make the AI Act *lex specialis* regulation in this case. DMA complements existing laws in the EU, and its goal is to make the digital markets fairer by establishing explicit rules for gatekeepers (large technological companies such as social media networks, online search engines, app stores). It particularly ensures data portability in the interest of users, who will have a say regarding allowing tracking and profiling for advertising purposes.

The NIS 2 Directive [2] from 2022 repeals the older NIS directive [18] from 2016 and strengthens cybersecurity requirements for critical sectors, including smart city services, by introducing incident management, incident reporting, and general cybersecurity measures with explicit mentions of important International Organisation for Standardisation (ISO) standards. NIS 2 also addresses the overlap with the Regulation on Digital Operational Resilience (DORA) [4] from 2022 for the financial sector by introducing a *lex specialis* rule. Even though the scope of NIS 2 as a horizontal regulation is broader, this rule means that in case of overlap between the two regulations, DORA takes precedence over NIS 2, and the requirements from the latter will not apply to financial entities. DORA focuses on the financial sector and introduces requirements such as threat-led penetration testing (TLPT).

The Cyber Resilience Act (CRA) [3] is a horizontal legal act that seeks to improve the cybersecurity of software and hardware products. Common traits between NIS 2 and CRA have been found in terms of risk analysis and risk management, definitions regarding criticality, incident handling, and market surveillance provisions. On the other hand, the Cybersecurity Act (CSA) [19], adopted in 2019, strengthens the EU Agency for Cybersecurity (ENISA) with a permanent mandate, and establishes the European Cybersecurity Certification Framework (ECCF) for certifying digital products and services.

The eIDAS (electronic IDentification, Authentication and Trust Services) regulation [20] from 2014 enables secure digital identity and trust services across the EU. This regulation is evolving for the purpose of increased security and efficiency, with new features like the European Union Digital Identity (EUDI) Wallet in an updated version of eIDAS 2.0 [21].

3. Methodology

The comprehensive review reported here was conducted in accordance with the guidelines proposed by Webster and Watson [22] and Kitchenham et al. [23], which provide guidelines to identify, evaluate, and synthesise relevant research. The objective was to collect, analyse, and categorise publications that address the intersection of smart cities, cybersecurity, and EU data protection regulations. Their approach is based on an initial database to perform the search using well-defined search terms instead of starting with a handful of pre-selected publications. The process begins with the definition of a structured search strategy to identify relevant studies, followed by a screening and selection phase guided by inclusion and exclusion criteria. As per the instructions of [22,23], we carefully documented all the phases of the publication retrieval and reviewing process. While the review follows a structured approach to ensure transparency, the emphasis is on providing a comprehensive synthesis and interpretation of the research landscape rather than adhering to a strictly protocol-driven systematic review.

3.1. Formalising the Research Question

The primary focus of this paper is to examine how European Union data-protection and cybersecurity regulations are addressed within smart city initiatives, what the properties of the proposed solutions in the literature are, and what technical and organisational measures are proposed that support and enable regulatory compliance. To guide this process, the following research question was formulated:

What is the current state of the art of cybersecurity solutions for smart cities that address EU regulatory requirements?

To answer the research question, we conducted a comprehensive review to identify high-quality peer-reviewed research articles published in well-reputed databases in the last seven-year period. The search involved a structured and targeted process, heavily directed to the research question and the intersection of three subtopics: cybersecurity, EU regulations, and smart city. Figure 1 illustrates the scope of this review, highlighting the intersection of the three focus areas that guided our screening and selection process.

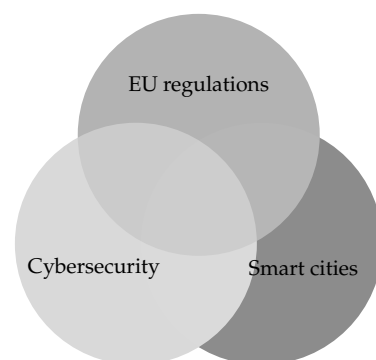


Figure 1. The scope of this comprehensive review is in the intersection of EU regulations, cybersecurity, and smart cities.

3.2. Initial Search and Search String

We undertook an initial informal search of articles from 2018 to 2025, which confirmed that there was a substantial number of publications on the topic and the relevance of our review. Since the topic of smart cities and IoT deployments emerged only in the last decade, and the most important data protection and cybersecurity regulations in the EU began with the enactment of the GDPR in 2018, we considered articles published between 2018 and 2025 to focus on the most recent developments and solutions. The initial search was carried out using DTU Findit (<https://findit.dtu.dk/>, accessed on 10 March 2025). This database was

chosen because it aggregates Open-Access and institution-licensed publications indexed from multiple reputable databases, including Scopus, Web of Science, IEEE Xplore, and the ACM Digital Library. The database query was limited only to the abstract of the papers. This was done on purpose to remove the irrelevant articles that mention the search terms only in body text or keywords (keywords set by authors, indexed keywords, etc.).

The search string can be seen in Table 1. Having set the core focus of the work on the review of cybersecurity regulatory-driven solutions for smart cities, a further degree of clarity is needed to focus the review only on general smart city solutions and not sector-specific ones. A review of the latter would not have been possible due to the extensive literature on the wide range of application domains covered by the smart city ecosystem. This resulted in limiting ourselves only to general smart city solutions, reflected in the search query. Hence, we exclude sector-specific keywords such as: transportation, healthcare, energy, smart grids, and more as part of the search query. Instead of restricting the research to a single smart city domain, we chose a more general approach to smart cities that addresses a wider range of solutions over a longer period of time. The search query consists of generic synonyms of well-defined search terms to cover as many usage contexts in the literature as possible. The semantic equivalent search terms were from the area of privacy, security, and legal instruments in the EU, in the intersection of which the retrieved articles should reside.

Table 1. Search string on DTU Findit.

Search string	abstract:("smart city" OR "smart cities") AND abstract:(security OR "cyber security" OR cybersecurity OR privacy OR "data protection") AND abstract:(regulation OR directive OR Act OR GDPR OR legislation OR compliance OR EU OR Europe)
---------------	---

3.3. Criteria

In this section, we specify the criteria that the papers were scrutinised against in the initial search. Publications were evaluated against the following inclusion criteria:

- The publication must have undergone a formal peer-review process.
- The paper must be published between 2018 and 2025.
- It must be written in English.
- The paper must be open-access/publicly available in full text.

Publications that did not meet the inclusion criteria or were outside the scope of our research question were generally excluded for the following reasons: (i) purely theoretical articles providing an overview of EU regulation(s) and smart cities that lacked a substantial contribution to the research question, (ii) studies did not focus on the European regulatory context (examining policies specific to regions such as China or the USA), (iii) articles lacking sufficient technical or analytical depth, including those without comprehensive or substantive contributions (e.g., short papers under four pages), (iv) papers presenting smart city solutions at a purely conceptual or proof-of-concept level, and thus lacking necessary empirical validation or implementation details. These criteria were applied to ensure that the review focuses on solutions with sufficient technical maturity and empirical grounding. For instance, proof-of-concept studies were excluded because they typically lack validation in realistic environments and do not provide sufficient evidence on how regulatory requirements are implemented and operationalised in practice, thus lacking comprehensive or substantive contributions to the research question.

Madjoubi et al. [24] is a good example of a relevant article not meeting our selection criteria. Despite providing a technical solution that preserves security and privacy in smart cities based on blockchain and smart contracts, their solution is a proof-of-concept and lacks sufficient performance evaluation or evidence that it is GDPR-compliant. Christofi et al. [25]

is an example of a relevant article giving an overview of data protection and cybersecurity European regulations in a smart city context, but it was excluded from the final pool of papers due to it being purely theoretical and not contributing to our research question.

The focus of this review lies on the intersection between cybersecurity solutions and EU regulatory requirements in smart cities. While AI is widely used in smart city applications, this review does not focus on AI techniques per se. AI-related studies were included only when they explicitly addressed cybersecurity, privacy, or regulatory compliance aspects, including the analysis of regulatory frameworks such as the AI Act in relevant domains. Consequently, studies focusing solely on algorithmic performance or data analytics without a clear link to security or regulatory requirements were excluded.

3.4. Screening

We ended the search on 31 March 2025, as no new relevant studies were identified in subsequent searches. Therefore, articles published after this date were not considered for this comprehensive review. Figure 2 gives an overview of the search and the multi-stage selection process, which is described in more detail below. In the primary querying of the database, 1300 articles were retrieved from the DTU Findit database. After removing duplicates and studies that are out of scope, the number of aggregated papers reached 1098. Three authors evaluated each article for inclusion, as well as performed the initial screening process through reading the title and abstract. Papers, which at least two authors agreed to exclude, were excluded mainly due to having little relevance to our research question or for other reasons (based on exclusion reasons 1 and 3). Publications without a unanimous inclusion/exclusion assessment between the authors were discussed until an agreement was reached. We then proceeded to the second stage of screening of publications based on defined criteria, which led to 129 candidate publications for full-text reading. At this stage, three authors discussed each of the papers, and any papers that did not fully fit the criteria involved the opinion of a fourth author.

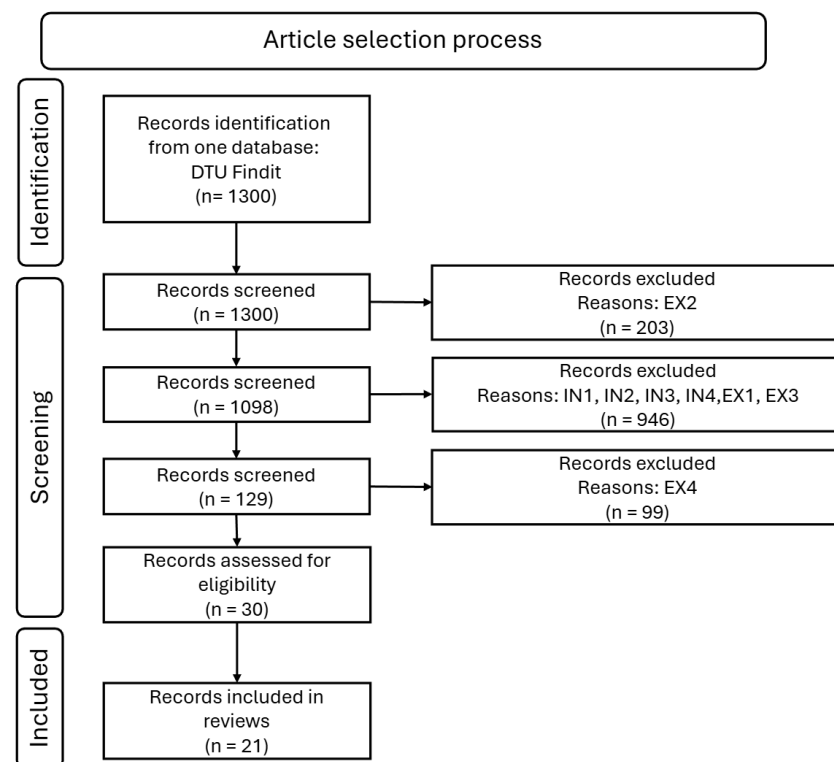


Figure 2. Article selection process.

3.5. Final Selection

In the final stage of the screening process, we performed a thorough analysis through full-text reading of the remaining papers (129) and identified 12 key publications for in-depth analysis. In addition, two authors checked the references of all selected papers (backward snowballing), after which another 56 papers were added for full-text reading by three authors. After a final discussion among four authors based on the exclusion criteria, we selected 9 more papers from the one-iteration of snowballing for a total of 21 publications for the final set of papers analysed in this review. These are listed in Table 2. Figure 3 presents the distribution of the selected articles over the years, as per the publication date. Among the 21 selected publications published between 2018 and 2025, the majority are in the period 2019 to 2022, with 5 publications in the year 2022. This could be due to many of the cybersecurity EU regulations that have entered into force in the past three years, while GDPR is a more mature regulation from May 2018 that provides more legal clarity. By 2022, GDPR was no longer ‘new’ to researchers, allowing more empirical studies and real-world implementations to be documented.

Table 2. Overview of papers analysed in this review.

Year	Authors	Title (Abbreviated)
2018	E.J. Kindt [26]	Having yes, using no? About the new legal regime for biometric data.
2019	Alonso et al. [27]	An Identity Framework for Providing Access to FIWARE OAuth 2.0-Based Services According to the eIDAS European Regulation.
2019	George et al. [28]	GDPR bypass by design? Transient processing of data under the GDPR.
2019	Buccafurri et al. [29]	An Attribute-Based Privacy-Preserving Ethereum Solution for Service Delivery with Accountability Requirements.
2019	Buccafurri et al. [30]	Ethereum Transactions and Smart Contracts among Secure Identities.
2020	Badii et al. [31]	Smart City IoT Platform Respecting GDPR Privacy and Security Aspects.
2020	Buccafurri et al. [8]	Smart-contract based Access Control on Distributed Information in a Smart-City scenario.
2020	I. N. Rezende [32]	Facial recognition in police hands: Assessing the ‘Clearview case’ from a European perspective.
2021	Asghar et al. [33]	Deep Learning based Effective Identification of EU-GDPR Compliant Privacy Safeguards in Surveillance Videos.
2021	Schwemer et al. [34]	Legal AI systems in the EU’s proposed Artificial Intelligence Act.
2021	Veale and Borgesius [35]	Demystifying the Draft EU Artificial Intelligence Act.
2022	Benyahya et al. [36]	The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis.
2022	Chhetri et al. [37]	Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent.
2022	I. N. Rezende [38]	Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces.
2022	Stach et al. [39]	Can Blockchains and Data Privacy Laws be Reconciled?
2022	Tauqeer et al. [40]	Automated GDPR Contract Compliance Verification Using Knowledge Graphs.
2023	Anedda et al. [41]	A social smart city for public and private mobility: A real case study.
2023	Eckhardt and Kotovskaia [42]	The EU’s cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive.
2024	B. Fabregue [43]	Artificial intelligence governance in smart cities: A European regulatory perspective.
2024	E. Kun [44]	Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act.
2025	Seid et al. [45]	Cyber Resilience Using ASFA: DORA-Compliant Threat-Led Penetration Testing.

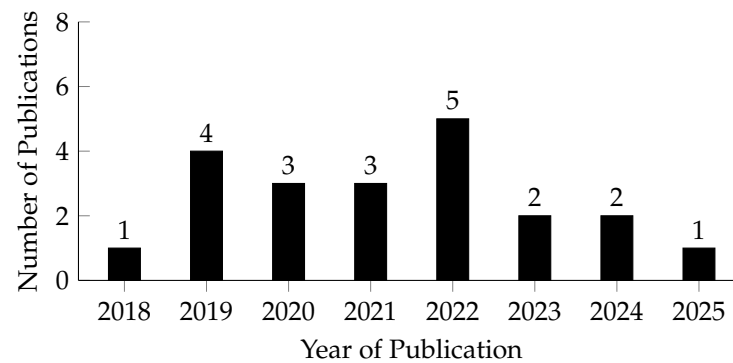


Figure 3. Number of selected publications according to the year of their publication.

3.6. Classification Scheme

The classification scheme used in this review is understood as a formal system for organizing complex, multifaceted phenomena into a set of shared dimensions [46]. Following the guidelines proposed by Petersen et al. [47], the classification scheme developed in this work is topic-specific, with its categories derived from a detailed analysis of the reviewed literature. Each category therefore reflects a distinct property against which the articles were evaluated, enabling a comprehensive understanding of the studied artifacts, such as smart city application domains, involved stakeholders, etc.

3.7. Limitations

This review follows a structured and systematic approach in accordance with the guidelines proposed by Webster and Watson [22] and Kitchenham et al. [23]. However, it is not intended to be exhaustive.

The literature search was conducted using a single aggregated database (DTU Findit), which integrates open-access and institution-licensed publications from multiple reputable sources, including Scopus, Web of Science, IEEE Xplore, and the ACM Digital Library. While this ensures broad coverage of high-quality and relevant studies, it may exclude works indexed exclusively in other databases.

In addition, the search strategy relied on title and abstract screening using a focused search string aligned with the research question. Although this approach improves the precision and relevance of the selected studies, it may omit papers where regulatory or cybersecurity aspects are discussed only in the full text. To reduce the probability of missing relevant studies, we included commonly used synonyms and related generic terms in the search query. Furthermore, the use of predefined keywords and the exclusion of sector-specific terms were intended to maintain a general smart city perspective, but may have led to the omission of studies that address regulatory-driven cybersecurity within specific application domains without explicitly using the selected terms.

The review is also limited to publications within the time period 2018–March 2025, reflecting the date of the final literature search. This seven-year window may exclude relevant studies published outside this period; however, it was selected to capture the most recent developments in smart cities and related EU regulatory frameworks. Nevertheless, studies published after this cut-off are not included, which may affect the coverage of the latest advancements in the field.

Therefore, the final corpus of 21 papers should be interpreted as a representative and focused sample of the literature addressing regulatory-driven cybersecurity solutions for smart cities, rather than a complete inventory of all related work. This relatively small corpus is also a result of the strict inclusion criteria applied, particularly the requirement for implemented or validated solutions, which excluded early-stage or proof-of-concept studies.

4. Results

After a brief overview of the cybersecurity and regulatory aspects addressed by the selected articles, this section provides an analysis and classification of the papers in terms of the application domains in which cybersecurity measures are implemented (Section 4.1), the stakeholders involved (Section 4.2), the cybersecurity and data protection measures deployed in smart cities (Section 4.3), the smart city solutions (Section 4.4), and the EU regulations and directives covered by the reviewed literature (Section 4.5).

4.1. Application Domains

With the integration of the most advanced and emerging technologies, such as IoT, cloud computing, data mining, blockchain, and more, smart city deployments have seen success across different sectors, such as smart grids, smart transportation, and smart healthcare, to name just a few. Hence, the combination of the underlying technologies and the rules set out by different regulatory instruments has an impact on the properties of the technologies used and the potential to transform our cities into smart(er) ones. Most EU digital regulations adopt a risk-based approach, meaning that privacy, security, and compliance obligations scale with the level of risk associated with the specific system, product, or processing activity. Therefore, in this work, we assume a mutual influence between the application domain and the security and privacy requirements, as well as the solutions provided.

Hence, this section presents the main application domains identified in this review, illustrating how Cybersecurity and EU Regulations are addressed across different Smart City environments. The reviewed articles were classified into seven domains based on their primary focus (see Figure 4): Public Safety and Surveillance [26,28,32–35,38], Digital Identity Management [8,27,29,30], Data Management [31,37,39,40], Finance [44,45], Smart Mobility [28,36,41], Smart Governance [34,43], and Critical Infrastructure [42]. In total, 21 papers were analysed (please note that this overview provides an indication of the smart city application domains in which regulatory-driven cybersecurity approaches have been addressed in the scientific literature over the last seven years). Sector-specific terms (e.g., smart healthcare, smart transportation, smart grid) were not included in the search query, as the focus of this review is on general smart city solutions aligned with the research question. As a result, the identified application domains emerged inductively from the analysed literature rather than being predefined. Consequently, the classification may not capture all domain-specific research conducted in individual smart city sectors.

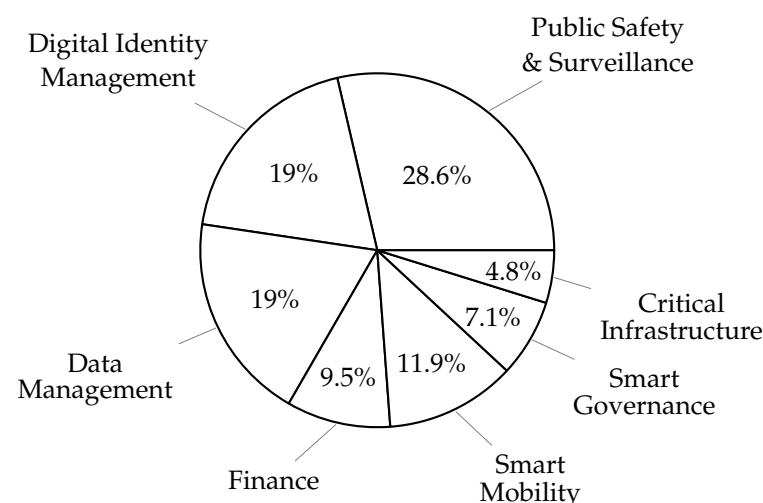


Figure 4. Distribution of reviewed papers across application domains.

Two papers [28,34] address aspects relevant to more than one domain and were therefore counted proportionally in the corresponding domains when calculating the distribution. Accordingly, the distribution of reviewed papers across application domains Figure 4 is as follows: Public Safety and Surveillance (7 papers; 28.6%), Digital Identity Management (4 papers; 19%), Data Management (4 papers; 19%), Finance (2 papers; 9.5%), Smart Mobility (3 papers; 11.9%), Smart Governance (2 papers; 7.1%), and Critical Infrastructure (1 paper; 4.8%).

A noteworthy observation from this analysis is that the identified application domains (seen in Figure 4) reflect both the EU regulatory landscape and the technological advancements of current research on regulatory-driven cybersecurity solutions for smart cities. Most studies concentrate on Public Safety and Surveillance, followed by Digital Identity Management and Data Management, likely due to the sensitive nature of personal data processed in these domains and the strict requirements imposed by the GDPR and related regulations. Digital Identity Management and Data Management also appear as the most mature domains, featuring several implemented and validated solutions. In contrast, domains such as Critical Infrastructure remain underrepresented despite their strategic importance, particularly given the potential impact of disruptions on essential services.

Table 3 maps each application domain to the relevant EU regulations, types of contributions, and implementation status, as well as the observed maturity of evidence. The latter reflects both the number of studies identified in each domain and the extent to which solutions are implemented and empirically validated in the reviewed studies. High maturity indicates domains with multiple studies and at least one validated implementation, medium maturity refers to domains with limited studies and/or at least one implemented solution alongside conceptual work, while low maturity indicates domains with sparse literature that is only conceptual or regulatory without any implementations. Regulatory trends vary across domains. While GDPR is the most widely addressed regulation, domain-specific instruments are reflected in particular areas, such as DORA in Finance, eIDAS in Digital Identity Management, NIS 2 and the CRA in Critical Infrastructure, and the AIA in Smart Governance. It should be noted that the regulations associated with each domain reflect only those addressed in the reviewed studies rather than the full spectrum of potentially applicable EU frameworks. Consequently, the absence of specific regulations within certain domains indicates a lack of corresponding studies in the literature, highlighting gaps in current research rather than suggesting limited regulatory relevance. The identified domains and selected use cases are further illustrated in Figure 5 and analysed in the following sections.

Table 3. Summary of application domains, pertinent EU regulations, types of contributions, and maturity of evidence identified in the reviewed literature.

Domain	Pertinent EU Regulations	Type of Contributions	Maturity of Evidence
Public Safety & Surveillance	GDPR [26,28,32,33,35], LED [26,32], AIA [35,38]	Mainly legal and ethical analyses; one implemented and validated GDPR-compliant solution [33]	High
Digital Identity Management	eIDAS [8,27,29,30]	Four implemented and validated eIDAS-compliant solutions [8,27,29,30]	High
Data Management	GDPR [31,37,39,40]	Three implemented and validated GDPR-compliant solutions [31,37,40]; one conceptual analysis	High

Table 3. Cont.

Domain	Pertinent EU Regulations	Type of Contributions	Maturity of Evidence
Finance	GDPR [44], NIS 2 [44], DORA [44,45]	One implemented DORA-compliant solution [45]; remaining contribution is regulatory analysis	Medium
Smart Mobility	GDPR [28,36,41]	One implemented and validated GDPR-compliant solution [41]; remaining studies provide regulatory/technical analysis	Medium
Smart Governance	GDPR [34,43], AIA [34,43]	Regulatory analysis; no implemented smart city solutions	Low
Critical Infrastructure	NIS 2 [42], CRA [42]	Regulatory analysis; no implemented smart city solutions	Low

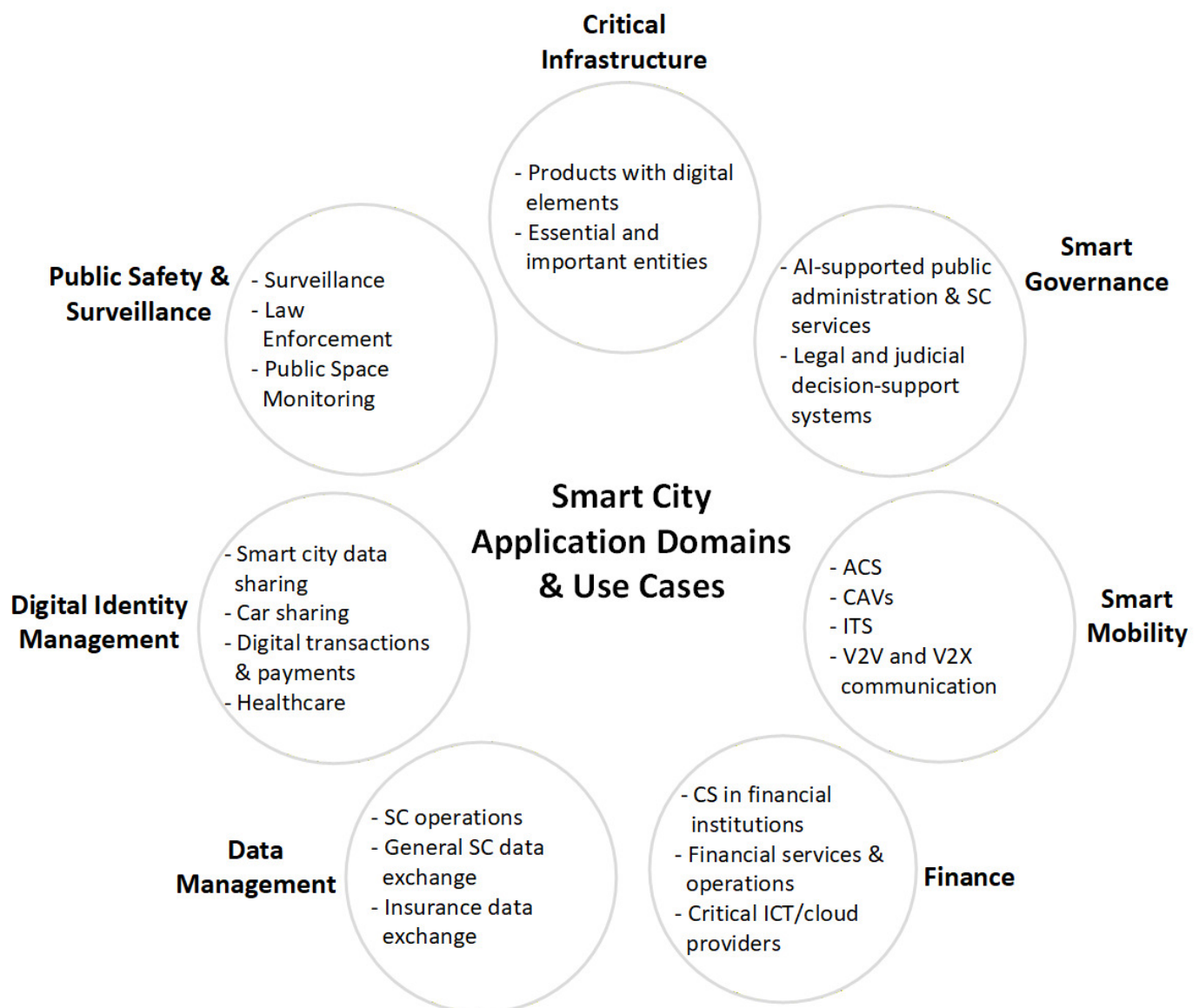


Figure 5. Smart city domain categories and use cases.

4.1.1. Public Safety and Surveillance

Public Safety and Surveillance emerges as a prominent application domain, with the reviewed studies primarily examining the deployment and regulatory implications of AI-based surveillance technologies, particularly facial recognition systems used by law enforcement in smart cities [26,28,32,33,38]. Across this domain, GDPR compliance is a

central concern [26,28,32–35], often complemented by discussions on the LED [26,32] and, more recently, the AIA [34,35,38]. Despite the strong regulatory focus, only one study presents an implemented and validated solution. Asghar et al. [33] propose a system developed within a Horizon2020 project that integrates IoT sensors, video streams, and crowd-sourced data to support real-time public safety monitoring, incorporating privacy-preserving measures to address GDPR requirements. In contrast, the remaining studies provide predominantly legal and ethical analyses of surveillance technologies. These works collectively highlight key regulatory challenges related to lawful bases for processing, proportionality, and data minimisation in the context of biometric and facial recognition systems [35,38]. Studies focusing on the LED further emphasise the strict conditions under which biometric data may be processed for law enforcement purposes [26,32]. In parallel, research addressing the AIA underlines the classification of such systems as high-risk, stressing requirements for risk management, data governance, and human oversight [34]. In addition, the authors state that the misuse of such a system could potentially significantly impact democracy in the EU. Overall, this domain is characterised by a strong emphasis on regulatory analysis and fundamental rights considerations, with limited translation into implemented technical solutions. Approaches such as transient data processing [28] illustrate attempts to reconcile real-time surveillance with data protection requirements, but remain largely conceptual.

4.1.2. Digital Identity Management

Another application domain category identified in this review is Digital Identity Management. All the papers reviewed in this domain [8,27,29,30] present implemented and validated solutions for secure electronic identification and access management, complying with the eIDAS regulation. The majority of them [8,29,30] utilise blockchain technology, specifically smart contracts, to manage digital identities in a decentralised way. In particular, in these works [8,29,30], identity information and access permissions are handled through blockchain-based mechanisms that remove the need for a central authority and allow transparent verification of user credentials and transactions. The implementations are typically built on Ethereum and have been tested in various use cases, including smart city data sharing and car sharing [29], healthcare [8], and digital transactions and secure payments [30]. Among these, Buccafurri et al. [30] integrate the Italian Public Digital Identity System (SPID), which is already compliant with eIDAS, with a blockchain-based framework to enable secure digital identity verification and authenticated transactions among users, even if they are not preregistered on the blockchain. However, Alonso et al. [27] differ from these works by proposing and implementing an identity management framework to enable cross-border authentication. Their solution extends the well-established Future Internet Ware (FIWARE) (<https://www.fiware.org/>, accessed on 10 April 2025) security framework, incorporating consent management and fine-grained access control.

4.1.3. Data Management

Another application domain identified in this paper is Data Management. The focus of the papers reviewed in this domain [31,37,39,40] is purely on the handling of data as a valuable/key resource; in other words, the management of smart city data from its collection to processing and storage, so that it can be analysed and support effective decision-making. In addition, all the reviewed works [31,37,39,40] address compliance with the GDPR. The majority of them [31,37,40] present implemented and validated solutions developed within European projects (Snap4City [31] and smashHit [37,40]), which enable interoperable and GDPR-compliant data sharing between different organisations and stakeholders in smart cities. These solutions have been tested in real or pilot environments,

including (i) smart city operations in mobility, environment, and utilities [31], (ii) general smart city data exchange [31,37,40], and (iii) insurance data exchange [37,40] use cases. Stach et al. [39] complement these works by examining the compliance of blockchain-based mechanisms with the GDPR, and by addressing how to achieve privacy-by-design blockchain-based mechanisms. In particular, the authors in [39] argue that blockchain, due to its immutable nature, is inherently difficult to reconcile with GDPR principles such as the right to erasure and data accountability. As a consequence, Stach et al. [39], after identifying key conflicts between GDPR requirements and blockchain properties, propose a set of technical privacy-preserving mechanisms together with an organisational governance model based on Data Protection Officer (DPO) oversight to support the development of privacy-aware blockchain-based solutions.

4.1.4. Finance

Within this work, the Finance domain emerged as a distinct area of focus. All the papers reviewed in this domain [44,45] address compliance with DORA and discuss its application within financial institutions in the EU. In addition, Kun [44] examines the relationship among DORA, NIS 2, and the GDPR in the context of critical cloud service providers (CSPs) in the EU. These overlaps are only briefly mentioned here, as they are discussed in detail in Section 4.5. Among these works, Seid et al. [45] is the only paper reviewed in this domain that presents an implemented and validated solution. The authors apply the Attack-Situation-Focused Analysis (ASFA) framework, developed previously by the same authors, for DORA-compliant Threat-Led Penetration Testing (TLPT) in a Swedish financial institution, using real incident data to evaluate operational resilience and compliance in practice. The framework requires manual intervention to identify relevant security incidents and can only be effectively used by individuals with adequate cybersecurity expertise. On the other hand, Kun [44] provides legal and regulatory analyses that clarify DORA's scope, oversight structure, and requirements, as well as its interaction with related EU stakeholders. In particular, Kun [44] analyses DORA's approach to Information and Communication Technology (ICT) third-party and cloud service supervision, highlighting the establishment of an EU-level oversight regime for critical ICT service providers and the coordination challenges it introduces among EU supervisory authorities.

4.1.5. Smart Mobility

Articles in this domain deal with Smart Mobility, which is an important application domain of smart cities, as it promises more efficient and safer transportation services for users. All the papers reviewed in this domain [28,36,41] address compliance with the GDPR and can be grouped into two main clusters: (i) an implemented mobility management system [41], and (ii) legal and technical analyses of data protection in automated and connected mobility systems, including transient data processing [28,36]. Anedda et al. [41] present and evaluate an implemented solution tested in a real scenario in Cagliari, Italy, an area with high traffic concentration. The proposed solution integrates real-time traffic monitoring, crowd monitoring in public transport, dynamic traffic light management, route optimisation, and a citizen mobility app, combining data from various city sensors through a Social IoT platform. To ensure GDPR compliance, the authors implement a combination of privacy-preserving techniques for data anonymisation, encryption, and secure transmission. The solution, validated within the Cagliari2020 project, demonstrated improved mobility management and reduced traffic congestion in the pilot area. On the other hand, Benyahya et al. [36] examine the application of GDPR principles in Automated City Shuttles (ACS), focusing on data flows generated through Vehicle-to-Everything communications and data collected from on-board sensors and mobility services. The authors further review the

responsibilities of data controllers and processors and identify when DPIAs are required. Furthermore, George et al. [28] focus on transient (ephemeral) data processing and its implications for GDPR compliance. Using case studies on facial detection in advertising and mapping for autonomous vehicles, they assess when transient data processing activities still fall within the GDPR and emphasise the need for organisational and technical safeguards to prevent misuse and unintended re-identification.

4.1.6. Smart Governance

Smart Governance deals with how public administrations use technologies, data, and citizen participation mechanisms to improve decision-making, public services, transparency, and citizen trust. The two papers reviewed in this domain [34,43] focus on the regulation and governance of AI systems in the context of smart cities and public administration. Additionally, the articles reviewed in this domain [34,43] examine compliance with the AIA and its relation to the GDPR. Fabregue [43] analyses AI governance in smart cities from a European regulatory perspective, highlighting how the AIA and GDPR intersect in ensuring fairness, privacy, and transparency. The paper focuses on high-risk AI applications such as behavioural manipulation, social scoring, and biometric identification, identifying governance gaps in data management and proportionality within smart city contexts. In addition, Schwemer et al. [34] complement this work by analysing the AIA in relation to legal AI systems used in the administration of justice and democratic processes. The authors note that the definition of AI under the Act is broad, but its scope for high-risk systems remains limited. They emphasise the need for risk management, data governance, and human oversight to ensure transparency and accountability in automated decision-making.

4.1.7. Critical Infrastructure

Critical Infrastructure consists of the essential physical and digital systems and services that drive city operations, whose disruption would significantly impact public safety, health, or security, among other goals. The single paper reviewed in this domain [42] analyses the EU's cybersecurity framework by examining how the CRA fits within the broader landscape of European cybersecurity legislation and interacts with existing instruments, in particular the NIS 2 Directive. The paper highlights the interaction between the CRA and the NIS 2 in areas such as risk management measures and market surveillance provisions. The authors observe that EU cybersecurity legislation remains fragmented in the context of product security and critical infrastructure, as different instruments address overlapping but not identical aspects of cybersecurity. In particular, they point to inconsistencies between the CRA and the NIS 2 Directive regarding the scope of risk management obligations, security requirements, and incident notification duties. These differences, combined with partially misaligned terminology and reporting thresholds, can create uncertainty for manufacturers and operators of critical infrastructure components and complicate compliance across Member States.

4.2. Stakeholders

In addition to the application domains, this work identifies a set of stakeholder groups that recur across the reviewed publications. These groups represent the actors involved in the design, deployment, regulation, and use of regulatory-driven cybersecurity solutions within smart cities. Based on the analysis of the selected papers, seven stakeholder categories were derived: service providers, technology providers, regulatory authorities, governments and municipalities, citizens/users, identity and attribute providers, and judicial authorities and professionals.

A notable observation is that the stakeholders discussed in the reviewed papers are often framed directly through the lens of the regulatory instruments addressed in each

work. For instance, papers focusing on the GDPR commonly distinguish between data subjects, data controllers, and data processors, while DORA-oriented papers refer to financial entities, critical ICT third-party service providers, or operators of essential financial services. This regulation-driven framing is also evident in domain-specific analyses. For example, Benyahya et al. [36] propose a stakeholder classification for automated city shuttles that explicitly follows GDPR terminology, identifying data controllers, data processors, and data subjects within the ACS ecosystem, rather than adopting a more generic stakeholder taxonomy. However, these regulation-specific classifications do not always map cleanly onto real-world roles: the same organisation may act as a data controller in one context and as a data processor in another, or simultaneously fulfil multiple functions depending on the service and data flow involved. Therefore, rather than adopting regulation-specific labels, this section takes a step back and aims to identify the broader stakeholder groups that actually appear across the reviewed papers, providing a more stable, cross-regulatory perspective on the actors involved in regulatory-driven cybersecurity solutions for smart cities.

A consistent trend across the reviewed publications is that the distribution of stakeholders differs across domains and follows the regulatory focus of the reviewed works. Service providers and technology providers appear most frequently, reflecting that many papers concentrate on system design, development, and implementation. Citizens and data subjects are widely mentioned, but mainly as individuals whose data must be protected, rather than as active participants in system design or governance. Regulatory and supervisory authorities feature mainly in papers addressing DORA, NIS 2, the CRA, or the AIA, where oversight and compliance are central topics. Identity and attribute providers appear only in the Digital Identity Management domain, which is consistent with the eIDAS orientation of those works. Judicial authorities are referenced in only a small number of papers, primarily in the context of AI systems used in justice and law enforcement. Finally, stakeholder diversity varies across domains: technically oriented domains are dominated by service and technology providers, whereas governance and regulation-focused domains involve regulators and judicial actors.

4.2.1. Service Providers

This group appears most frequently across the reviewed papers [8,27–30,33,36,37,39–45]. Service providers, whether public or private, are described as the entities delivering services to citizens within smart cities. Examples of public service providers mentioned in the reviewed papers include municipal utility companies, public transit agencies, public health systems, or waste-management services, while private service providers may include social-media platforms, ride-sharing and delivery companies, or banks. Across the reviewed works, service providers typically operate and manage the platforms and services supplied or developed by technology providers. Because they determine how these systems are used in practice, service providers are generally responsible for ensuring that the activities carried out through these systems comply with the applicable legal requirements. Their role therefore involves ensuring that the technical and organisational measures provided by other stakeholders are adequately applied for secure and lawful data processing, and coordinating data handling with other stakeholders involved.

4.2.2. Technology Providers (Developers, Integrators, Manufacturers)

Technology providers appear across most technical papers as the actors responsible for developing, supplying, or integrating the technological components used in smart city solutions [26–28,31–38,41–43,45]. They design or implement the underlying technologies (e.g., IoT platforms, AI tools, blockchain infrastructures) that enable service providers to successfully operate and deliver digital services within smart cities. While technology

providers ensure that the systems they supply support secure operation and include the mechanisms needed to facilitate compliance, they are not typically responsible for fulfilling the regulatory obligations themselves. Instead, their role is to provide the technological means that allow service providers to meet their legal responsibilities, with the actual compliance oversight resting on the service providers who operate these systems.

4.2.3. Regulatory Authorities and Supervisory Bodies

Regulatory authorities and supervisory bodies appear mainly in papers that focus on the legal and regulatory perspective of regulatory-driven cybersecurity solutions for smart cities [8,26,28,31,34,36,37,39,40,43–45]. These works refer to national and EU-level bodies responsible for overseeing and enforcing compliance with relevant EU regulations such as the GDPR, eIDAS, DORA, NIS 2, the CRA, and the AIA. Examples mentioned in the reviewed papers include EU agencies and data protection authorities, financial supervisory authorities, and EU-level bodies involved in oversight (e.g., the Lead Overseer under DORA). Their role is generally described as monitoring compliance, issuing guidance, conducting audits or inspections where required, and coordinating supervision across different actors, especially in cross-border or multi-stakeholder settings.

4.2.4. Governments and Municipalities

Governments and municipalities appear in several papers as the public authorities responsible for planning, organising, regulating, or supervising the digital services used in smart cities [26,27,31–33,36–38,41,43,45]. Unlike public service providers, which deliver operational public services, governments and municipalities carry out administrative and decision-making functions. Their responsibilities typically include planning or approving the deployment of digital infrastructures, defining public-sector data-processing practices, and ensuring that these activities align with the applicable legal frameworks. Local administrations often act as data controllers when offering public digital services, while national governments are referenced in papers that discuss the development of legal frameworks or the wider policy responsibilities of public authorities.

4.2.5. Citizens/Users

Data subjects appear in all papers that involve the processing of personal data [8,26–41,43]. They are described as the individuals whose information is collected or used across various smart city contexts, such as mobility services, surveillance systems, digital identity frameworks, and data-sharing platforms. In the reviewed works, data subjects are primarily presented as the stakeholders whose rights must be protected under the relevant regulations, with emphasis on transparency, consent, data minimisation, and safeguards against profiling or intrusive surveillance. Their role is generally passive, as they are the recipients of protections rather than active participants in system design or governance.

4.2.6. Identity and Attribute Providers

This stakeholder group appears only in the Digital Identity Management domain [8,27,29,30]. The papers addressing eIDAS-compliant identity solutions refer to identity providers, attribute providers, and trusted service providers responsible for issuing, validating, or managing verified digital identities [8,27,29,30]. Their role is central in the authentication processes described in these works, including cross-border identification and the use of national identity systems such as SPID. While these providers supply the verified identity information relied upon by other stakeholders, they do not operate the services that use this information.

4.2.7. Judicial Authorities and Legal Professionals

Judicial authorities and legal professionals appear in a limited number of papers [26,31,32,34,36,38], mainly those examining the implications of the AIA for legal AI systems [34,38] or discussing the Police Directive in connection with biometric surveillance [26,32]. These stakeholders are described as potential users or overseers of high-risk AI tools, such as decision-support systems used in judicial or law-enforcement settings. The papers emphasise that their activities must remain transparent and accountable, and highlight risks associated with biased or opaque algorithmic systems that could affect legal decision-making or individuals' rights.

4.3. Measures

This section presents the cybersecurity and data protection measures identified in the reviewed literature. The reported measures are grouped into three categories: technical, organisational, and operational measures (illustrated in Figure 6). In all reviewed studies, technical measures are reported more frequently than organisational and operational measures, which are often discussed more conceptually. The following subcategories present the measures identified in each category, and their contribution to fulfilling key security requirements and regulatory goals of smart city solutions.

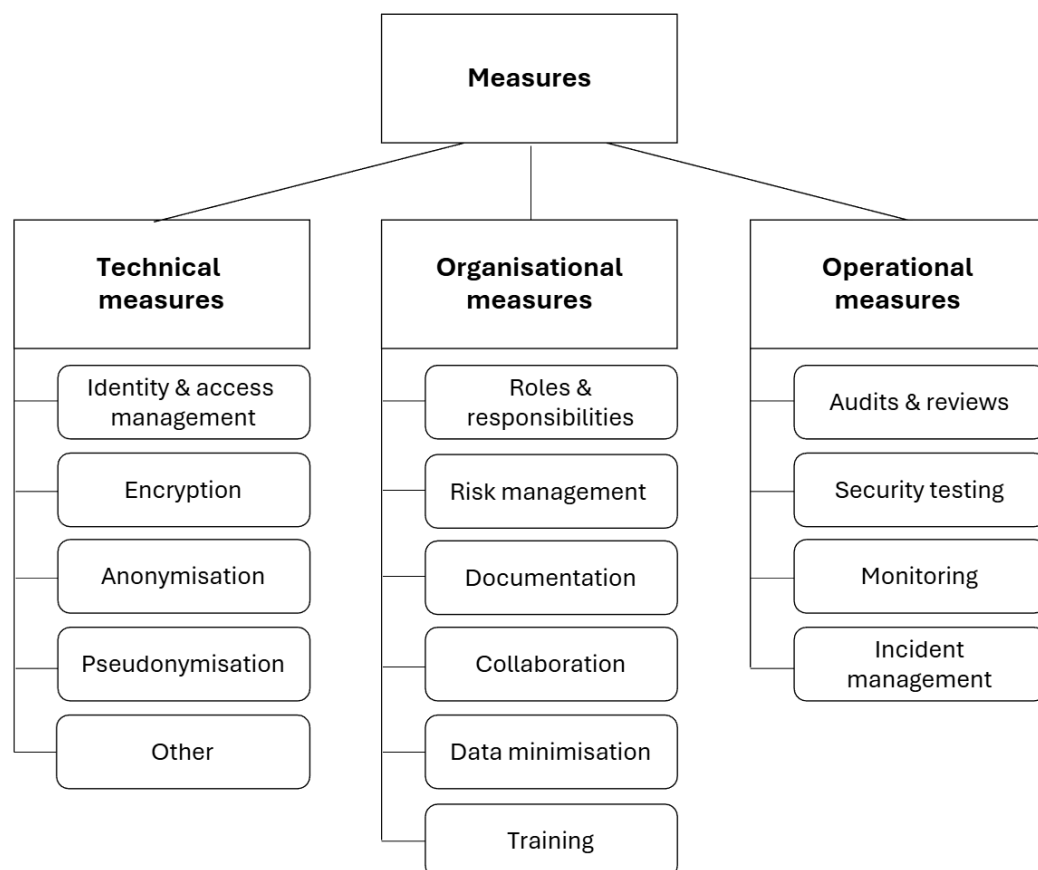


Figure 6. Classification of technical, organisational, and operational measures.

4.3.1. Technical Measures

Twelve papers [8,27–31,33,36,37,39–41] report measures classified in this review as technical. These measures are discussed or implemented in relation to data protection and security requirements in smart cities and are frequently referenced along with regulatory obligations, particularly under the GDPR. The reported technical measures are grouped into the subcategories of: (i) identity & access management; (ii) encryption; (iii) anonymisation;

(iv) pseudonymisation; and (v) other (as illustrated in Table 4). The measures presented below reflect those discussed in the reviewed studies and do not constitute an exhaustive set of technical measures for smart cities.

Table 4. Overview of technical measures.

Subcategory	Key Measures	References
Identity & access management	Standard protocols (OAuth 2.0, OpenID Connect)	[27,31]
	Role-based access control	[37,40]
	Attribute-based access control	[8,29,30,39]
Encryption	Hybrid encryption (AES & RSA)	[37,40]
	SSL/TLS	[31]
	Database/tablespace encryption	[31]
	Selective encryption	[33]
	Blockchain-based symmetric encryption	[8]
Anonymisation	Hashing	[41]
	Data generalisation (k-anonymity, l-diversity, t-closeness, differential privacy)	[36,41]
	Data masking	[36]
	Data removal	[33]
Pseudonymisation	Encryption-based pseudonymisation	[36]
	Zero-knowledge proofs	[36]
	Tokenisation	[36]
	Blockchain pseudonymity	[29]
Other	Transient processing	[28,41]
	Distributed storage	[8,37]
	Data purging	[39]
	Privacy filters	[39]

Identity & Access Management

Eight papers [8,27,29–31,37,39,40] address Identity and Access Management (IAM) measures. Authentication and access control are grouped under this category, as they are typically implemented together to enforce confidentiality, integrity, and accountability. Three main IAM approaches are identified: (i) standard authentication and authorisation protocols (Open Authorization (OAuth) 2.0 and OpenID Connect), (ii) Role-Based Access Control (RBAC), and (iii) blockchain-based Attribute-Based Access Control (ABAC) using Ethereum smart contracts.

Standard protocols are employed in smart city platforms to support interoperable identity management. Alonso et al. [27] integrate OAuth 2.0 with the eIDAS Security Assertion Markup Language (SAML) 2.0 infrastructure to enable authentication via national electronic identities, while Badii et al. [31] implement an OAuth-based solution in Snap4City combining OpenID Connect, JSON Web Tokens (JWTs)—based on session management, and a central Lightweight Directory Access Protocol (LDAP) registry. Compared with [27], which focuses on user authentication, ref. [31] extends access control to IoT devices and machine-to-machine communication.

Furthermore, RBAC-based approaches are adopted in [37,40], where JWTs are used to authenticate users and enforce role-based permissions in RESTful Application Programming Interfaces (APIs). Chhetri et al. [37] integrate JWTs within a next-generation access control architecture, while Tauqeer et al. [40] use RBAC to enforce access rights aligned with GDPR principles such as purpose limitation and data minimisation.

In addition, blockchain-based ABAC models are proposed by Buccafurri et al. [8,29,30], combining eIDAS-based identity verification with Ethereum smart contracts. Their work evolves from linking eIDAS identities to blockchain addresses using identity-based encryption [30], to attribute-based access control using Ciphertext-policy Attribute-Based Encryption scheme [29], and finally to a full ABAC workflow for secure data sharing, where

encrypted data are stored off-chain (Interplanetary File System) and access is enforced via smart contracts [8].

Finally, Stach et al. [39] extend ABAC to data-source authentication, requiring IoT devices to present certified attributes before submitting data to a blockchain, thereby enhancing data integrity and preventing untrusted inputs. Overall, IAM measures in the reviewed studies reflect a combination of standardised identity protocols and emerging decentralised access control models, with increasing attention to integrating regulatory requirements such as eIDAS and GDPR into access-control design.

Encryption

Five studies [8,31,33,37,40] employ encryption as a core technical measure to ensure the confidentiality and integrity of personal and sensitive data. In most cases, encryption is framed as a data-protection-by-design mechanism supporting GDPR requirements [33,37,40]. The reviewed approaches include: (i) hybrid AES–RSA schemes, (ii) SSL/TLS for secure communication, (iii) database encryption for data at rest, (iv) selective encryption of sensitive regions in CCTV data, and (v) encryption mechanisms integrated with blockchain-based systems. These measures are most frequently applied in the Data Management domain [31,37,40].

Hybrid encryption schemes are proposed in [37,40], combining Advanced Encryption Standard (AES) for bulk data encryption with Rivest-Shamir-Adleman (RSA) for key protection. Both approaches enable secure storage while maintaining limited data usability, as deterministic encryption allows encrypted data to remain searchable for automated compliance checks.

In addition, platform-level encryption is addressed by Badii et al. [31], who implement Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for secure data transmission and database-level encryption for data at rest, with keys protected by an external master key. This design reduces the risk of data exposure in case of system compromise.

In surveillance contexts, Asghar et al. [33] propose selective encryption at the Feature-of-Interest level, where only sensitive regions of CCTV frames are encrypted using Output Feedback mode (AES-OFB). This approach preserves system usability while supporting GDPR-compliant protection of personal data.

Finally, Buccafurri et al. [8] integrate encryption within a blockchain-based architecture, where data are stored off-chain in encrypted form, and access is granted through smart contracts. Decryption keys are distributed securely to authorised users via public-key mechanisms, ensuring controlled access in a distributed environment. Overall, encryption is consistently employed as a foundational technical safeguard across domains, although its implementation is often limited to specific system components rather than integrated into end-to-end security architectures.

Anonymisation

In this work, three papers [33,36,41] employ anonymisation mechanisms as a privacy-preserving measure that supports confidentiality, unlinkability, and data-minimisation in the Smart Mobility domain [36,41], and Public Safety and Surveillance [33] domains. Anonymisation is used as the irreversible transformation or removal of identifiers to prevent re-identification, using different approaches, including (i) hashing, (ii) data generalisation, (iii) data masking, and (iv) data removal. Employing these methods, the authors aim to enable the processing of big data for mobility and surveillance without compromising individual identities.

Anedda et al. [41] implement a real-time anonymisation mechanism based on irreversible hashing, where vehicle licence plates are hashed with double SHA-256 at the

edge and the original strings are deleted immediately after processing. This ensures that only non-reversible hash values are sent to the cloud for further mobility analysis. Beyond this implemented safeguard, the authors conceptually discuss generalisation-based anonymisation methods, including k-anonymity and differential privacy, to address privacy risks in large-scale mobility datasets. Benyahya et al. [36] provide an analytical taxonomy of privacy-preserving techniques and explicitly group anonymisation methods such as data generalisation and data randomisation techniques (noise addition, differential privacy, permutation) for mobility datasets. Benyahya et al. [36] also note that data masking is used inconsistently in the literature and can refer to anonymisation or pseudonymisation, depending on whether masked values can be reversed. Data masking constitutes anonymisation only when it is irreversible. They emphasise that, in the context of data processing for Automated City Shuttles (ACS), incorrect classification can lead to unintentional noncompliance.

As discussed above, Asghar et al. [33] analyse two Features-of-Interest (FOI) video obfuscation techniques applied to CCTV video frames: selective encryption and data removal. In contrast to the reversible AES-OFB encryption scheme, the authors describe data removal as an anonymisation approach in which FOI pixel information is permanently eliminated from video frames. This method irreversibly breaks the link between the data and identifiable individuals, thereby constituting an anonymisation technique rather than a reversible safeguard.

Pseudonymisation

Two papers [29,36] discuss pseudonymisation measures, including (i) encryption-based pseudonymisation, (ii) tokenisation schemes, (iii) zero-knowledge proofs, and (iv) blockchain-based pseudonymous identifiers. Pseudonymisation replaces or transforms personal identifiers into pseudonyms (identifiers other than the user's real identity) so that data can no longer be attributed to specific individuals. However, it is reversible under controlled conditions [29], and re-identification remains possible when combined with additional information held separately. Therefore, pseudonymised data remain subject to the GDPR, as defined in Article 4(5).

Benyahya et al. [36] conceptually discuss pseudonymisation as a GDPR-aligned privacy-preserving measure in ACS environments, outlining approaches such as encryption, tokenisation, and zero-knowledge proofs. The authors highlight that these mechanisms reduce identifiability rather than eliminate it and discuss their applicability in mobility and Vehicle-to-Everything contexts. In blockchain-based service-delivery architecture, Buccafurri et al. [29] employ Ethereum addresses as the pseudonymisation mechanism, so that service suppliers interact only with the user's blockchain address rather than their civil identity. Using Ethereum's native pseudonymity, the authors note that privacy could be improved by using one-shot Ethereum addresses, which allow users to generate a fresh transaction pseudonym for every service request.

Other

This review also identifies a set of additional technical measures that appear only in one or two studies. Although less frequently discussed, these measures broaden the range of technical approaches observed in the literature. They include: (i) transient processing [28,41]; (ii) distributed storage [8,37]; (iii) data purging [39]; and (iv) privacy filters [39].

Transient processing is used to minimise data retention by processing personal data ephemerally and deleting it immediately after extracting the required attributes. George et al. [28] restrict the retention of camera and Light Detection and Ranging inputs to less than one second, ensuring that no raw data are stored. Similarly, Anedda et al. [41] apply

real-time transformations to licence plate data and delete raw inputs instantly, retaining only processed spatial objects in JSON format for traffic analysis.

In addition, distributed storage addresses privacy and scalability challenges, particularly in blockchain-based systems. Buccafurri et al. [8] store encrypted documents off-chain in Interplanetary File System, while maintaining only cryptographic hashes and access-control rules on-chain. Chhetri et al. [37] adopt a similar approach by placing consent records and compliance-verification outputs in external storage components, supporting auditability without overloading core services.

Finally, Stach et al. [39] address GDPR erasure requirements in immutable blockchain systems through data purging and privacy filters. Personal data are stored in encrypted form, with decryption keys held externally; erasure is achieved by deleting the keys, rendering the data permanently unreadable. Privacy filters further obfuscate sensitive information before on-chain storage, supporting data minimisation while preserving functionality. Overall, the limited occurrence and evaluation of these measures further reflect the shallowness identified across the reviewed literature, where regulatory alignment is often addressed through isolated technical design choices rather than systematically implemented and empirically validated approaches.

4.3.2. Organisational Measures

Seventeen papers [26–29,31,32,34–40,42–45] discuss organisational measures in the context of smart city cybersecurity and data protection. These measures concern policies, processes, role definitions, and procedural safeguards, and are commonly referenced in relation to regulatory obligations under the GDPR, AIA, CRA, and DORA. An overview of the identified organisational measures is provided in Table 5. Across the reviewed literature, organisational measures are predominantly addressed at a conceptual level and framed as regulatory compliance requirements, while their concrete implementation within system architectures is rarely demonstrated. This indicates a persistent gap between regulatory expectations and realised organisational practices in smart city solutions.

Table 5. Overview of organisational measures.

Subcategory	Key Measures	References
Roles & responsibilities	Trusted roles definition Role and responsibility allocation Ownership assignment	[29] [34–36,39] [31]
Risk management	Supply chain risk management ICT risk management DPIA	[42] [44,45] [26,36,43]
Documentation	Data syntax documentation Technical documentation based on regulatory requirements	[37,40] [34,35,42]
Collaboration	Collaboration with legal experts Collaboration between regulatory authorities	[37,40] [44]
Data minimisation	Consent management Reduction in non-required attributes Purpose limitation	[26–28,31,34,36,37,40] [32,37,40] [32,38,43]
Training	Employee training	[32,34,38]

Roles & Responsibilities

A clear definition of roles and responsibilities emerges as a frequently discussed organisational measure, addressed in five papers [29,31,34,36,39] across multiple domains, including Data Management [31,39], Smart Mobility [36], Digital Identity Management [29], and Smart Governance [34]. Across the reviewed studies, this measure is discussed along

three main dimensions: (i) the definition of trusted roles, which establishes which actors are formally recognised as trusted parties [29]; (ii) the allocation of roles and responsibilities, which assigns legal and operational duties to relevant stakeholders [29,34,39]; (iii) ownership assignment, which ensures that data and system components have clearly identified owners responsible for governance and compliance [31].

Buccafurri et al. [29] is an example of a work that explicitly limits which actors are considered trustworthy within a system. In particular, the authors propose a privacy-preserving Ethereum-based identity architecture in which trust is restricted to two independent third parties: the attribute provider and the private key generator (PKG). Service providers and users are treated as untrusted, while the link between a real identity and a pseudonymous blockchain address is known only to the certifying attribute provider. This explicit restriction of trust relationships is used to strengthen accountability and traceability in digital identity management.

Other works focus on role and responsibility allocation from a regulatory perspective [34,36]. Benyahya et al. [36] analyse how GDPR roles such as data controllers, processors, and joint controllership apply in the ACS ecosystem, highlighting that these roles may shift over time and that joint responsibility does not imply equal liability. Similarly, Schwemer et al. [34] examine responsibility allocation under the AI Act, emphasising that high-risk AI systems require shared responsibilities between providers and users. In this context, providers have to take extensive responsibilities, including risk-management processes, data governance, and documentation requirements, while users are expected to operate and monitor systems in line with the provided instructions. In contrast, although Stach et al. [39] do not propose a concrete role allocation, they highlight the difficulty of identifying a clear data controller in decentralised blockchain-based systems, framing controller responsibility as an unresolved organisational challenge under the GDPR. Finally, ownership assignment is discussed as a concrete organisational mechanism to support accountability.

Badii et al. [31] describe how the Snap4City platform assigns a clear owner to each IoT device, with owners responsible for access control, modification, and delegation. This approach ensures that data are private by default and supports GDPR-compliant governance through clear accountability structures.

Risk Management

Six papers [26,36,42–45] discuss risk management as an organisational measure. Across the reviewed literature, risk management is primarily framed as a regulatory obligation rather than as a fully implemented or operationalised practice. Three main forms of risk management emerge: (i) supply-chain risk management; (ii) ICT risk management; (iii) and Data Protection Impact Assessments (DPIAs).

Supply-chain risk management is addressed by Eckhardt and Kotovskaia [42] in the context of the NIS 2 Directive and CRA. The authors highlight that essential and important entities under NIS 2 are required to address risks arising from third-party products and services, given their potential impact on overall system security. This includes integrating explicit cybersecurity requirements into contracts and conducting audits of suppliers and service providers. Under the CRA, similar responsibilities are placed on manufacturers of products with digital elements, who must perform conformity assessments to guarantee that products are secure by design and free of known vulnerabilities.

ICT risk management under DORA is discussed in two studies [44,45]. Seid et al. [45] illustrate how an automated threat-led penetration testing approach can support DORA's ICT risk-management objectives by improving organisations' ability to identify, detect, and respond to ICT-related risks. Kun [44] focuses on ICT third-party risk management,

emphasising that financial institutions remain responsible for outsourced ICT services and must retain effective control through governance mechanisms and contractual safeguards. The study highlights proportionality and materiality as key principles, requiring stricter oversight for ICT services that support critical or important functions.

DPIAs represent a third form of risk management and are discussed in three papers [26,36,43]. Benyahya et al. [36] explain that ACSs must conduct DPIAs when engaging in high-risk processing, such as automated decision-making, large-scale monitoring, or processing of sensitive data. Kindt [26] frames the DPIA as an iterative and resource-intensive process that requires legal expertise and ongoing reassessment; if high risks cannot be mitigated, consultation with supervisory authorities is required before processing biometric data. Fabregue [43] further argues that traditional DPIAs are insufficient for AI-driven smart city systems and proposes enhanced DPIAs that explicitly address AI-specific risks, including bias, transparency, robustness, and liability.

Documentation

Across the reviewed papers, five papers [34,35,37,40,42] address documentation as an organisational measure supporting transparency, accountability, and regulatory compliance. Two complementary documentation practices emerge: (i) data syntax documentation used in GDPR-oriented technical tools, and (ii) regulatory-driven technical documentation mandated by EU legislation.

In the data management domain, Chhetri et al. [37] and Tauqeer et al. [40] implement data syntax documentation as part of their GDPR-compliant tools. Both studies adopt standard coding conventions (e.g., Python Enhancement Proposal 8—PEP 8) to improve code readability and maintainability and use Swagger to generate standardised documentation for RESTful APIs. This approach supports transparency and auditability of data processing structures in both consent verification and contract-compliance verification systems.

From a regulatory perspective, three legal-analytical papers [34,35,42] frame documentation as a mandatory compliance mechanism. Eckhardt and Kotovskaia [42] explain that the CRA requires manufacturers of products with digital elements to provide technical documentation describing how essential cybersecurity requirements are met, including information on cyber risks and update lifetimes, thereby supporting NIS 2 supply-chain due diligence. In the context of the AIA, Schwemer et al. [34] and Veale and Borgesius [35] highlight that high-risk AI providers must produce extensive technical documentation demonstrating compliance with data governance obligations. However, Veale and Borgesius [35] note that such documentation primarily serves regulators and conformity assessment bodies, rather than functioning as a user-facing transparency mechanism.

Collaboration

Three papers [37,40,44] address collaboration between stakeholders as an organisational measure supporting regulatory compliance. Two complementary forms of collaboration emerge: (i) interdisciplinary collaboration between legal experts, technical developers, and industry partners during system design and implementation; and (ii) institutional collaboration between regulatory authorities in oversight and enforcement. Together, these studies show that achieving GDPR and DORA compliance requires coordinated interaction beyond purely technical implementation.

Chhetri et al. [37] and Tauqeer et al. [40] demonstrate interdisciplinary collaboration in the development of GDPR-compliant tools. In both studies, legal experts contribute to translating legal requirements into Technical and Organisational Measures (TOMs) and supervise implementation to ensure alignment with GDPR, while industry partners provide real-world use cases and operational constraints. Across both works, collaboration is treated

as a structured organisational practice rather than as ad hoc legal consultation. From a regulatory perspective, Kun [44] highlights the need for cooperation and coordination between European and national supervisory authorities under DORA and NIS 2. Given that cloud service providers may fall under multiple overlapping regulatory regimes, the paper argues that enhanced information exchange and coordinated supervision are necessary to avoid duplicative enforcement and to respect the *ne bis in idem* principle.

Data Minimisation

Data minimisation is presented as a core GDPR protection goal and a technical–organisational measure requiring that only data strictly necessary for a given processing purpose are collected and used [37]. In this review, eleven papers [26–28,31,32,36–38,40,41,43] address data minimisation across multiple domains. The majority of these works appear in Public Safety and Surveillance [26,28,32,38] and Data Management [31,37,40] domains, reflecting the sensitivity and scale of the data processed in these contexts. Across the reviewed studies, data minimisation is implemented through three main mechanisms: (i) consent management, (ii) reduction in non-required attributes, and (iii) purpose limitation.

Consent management is the most frequently discussed measure and appears in eight studies [26–28,31,36,37,40,41]. Consent is framed as a prerequisite for lawful processing and as a practical tool to enforce data minimisation by restricting processing to explicitly authorised data and purposes. In the Smart Mobility domain, Benyahya et al. [36] stress that passengers of ACSs must be informed and able to exercise their data-subject rights prior to processing, while Anedda et al. [41] require specific consent for storing licence plate data. In contrast, studies in the Public Safety and Surveillance domain [26,28] highlight the limitations of consent in public space monitoring, arguing that it is often neither freely given nor practically obtainable. As an alternative, George et al. [28] propose transient processing to minimise data retention and avoid long-term storage of identifiable data. In addition, four papers [27,31,37,40] provide concrete implementations of consent management. In smart city IoT platforms, consent is operationalised as a granular authorisation mechanism for identity and data sharing [27,31]. In particular, Alonso et al. [27] integrate explicit user consent into an OAuth 2.0/eIDAS identity framework, requiring user confirmation before linking identity profiles. In the same direction, Badii et al. [31] implement signed consent within the Snap4City platform to control permissions for specific data types. Furthermore, in the data management domain, Chhetri et al. [37] and Tauqeer et al. [40] introduce consent-lifecycle management, where automated compliance checks ensure that processing stops immediately when consent expires or is withdrawn. In both tools, consent is defined using a minimal set of variables and is directly linked to automated verification mechanisms.

Reduction in non-required attributes is explicitly addressed in two studies [37,40]. Both limit consent records to essential attributes such as purpose, validity period, and required personal data, preventing the inclusion of unnecessary information and supporting data retention obligations through predefined expiry dates.

Purpose limitation is examined in three legal and governance-oriented studies [32,38,43]. Fabregue [43] frames purpose limitation as a privacy-by-design requirement for AI-based smart city systems, advocating for strict separation of data categories to prevent repurposing. Rezende [32,38] discusses purpose limitation in the context of biometric surveillance under the GDPR and LED, emphasising that biometric data processing must be strictly necessary, purpose-bound, and proportionate. Without such constraints, the studies warn of risks associated with excessive or blanket biometric surveillance in public spaces.

Training

Training emerges as an organisational measure supporting the lawful and responsible use of high-risk AI and biometric systems, and it is primarily discussed at a conceptual level in three studies [32,34,38]. Schwemer et al. [34] emphasise that individuals responsible for overseeing high-risk AI systems must possess sufficient technical competence to monitor system performance, detect errors, interpret outputs correctly, and recognise automation bias. The authors further note that the AIA explicitly requires human oversight roles to be performed by adequately trained and authorised personnel. Rezende [32,38] similarly stresses that biometric data processing tools should be operated exclusively by properly trained officers capable of handling sensitive biometric data and assessing the necessity and proportionality of their deployment. Although the reviewed studies identify training as a necessary organisational safeguard, they provide limited guidance on how such training should be structured or implemented in practice, highlighting a lack of operational depth for this measure within the reviewed literature.

4.3.3. Operational Measures

Eight papers [31,32,34,37,40,42,43,45] address activities related to the operation of systems, which are grouped under the category operational measures. Compared with technical and organisational measures, this category is less frequently represented in the reviewed literature. Across the reviewed studies, operational measures are predominantly discussed in relation to regulatory requirements rather than as implemented practices. Four subcategories of operational measures are identified: (i) audits and reviews, (ii) security testing, (iii) monitoring, and (iv) incident management. An overview of the operational measures identified in this review is provided in Table 6.

Table 6. Overview of operational measures.

Subcategory	Key Measures	References
Audits & reviews	Audit tool for reviewing logs	[31,37,40]
	Periodic review	[32]
	Human oversight	[34,43]
Security testing	Penetration testing	[31]
	TLPT	[45]
Monitoring	Continuous security monitoring	[31,45]
Incident management	Incident notification	[42,44]

Audits & Reviews

Six studies [31,32,34,37,40,43] address audits and reviews across the Data Management, Public Safety and Surveillance, Finance, and Smart Governance domains. Such measures are most frequently reported in the Data Management [31,37,40] and Smart Governance [34,43] domains. Across these studies, a common focus is on the need for a systematic review of system behaviour to support accountability, transparency, and regulatory compliance. Three key measures are identified in the literature: (i) audit tools for reviewing logs, (ii) periodic review, and (iii) human oversight.

In terms of audit tools for reviewing logs, three papers [31,37,40] integrate audit functionality into smart city data platforms and GDPR-compliance tools to support systematic review of logs and user activities. Badii et al. [31] integrate an auditing dashboard into the Snap4City IoT platform, enabling forensic analysis by controllers and transparency for end users through access-event monitoring. Chhetri et al. [37] and Tauqeer et al. [40] propose automated compliance verification tools that integrate auditability as a built-in feature of system design. While both rely on log-based auditing, they differ in scope: Chhetri

et al. [37] focus on the auditability of informed consent and revocation states, whereas Tauqeer et al. [40] frame auditing as part of a contract lifecycle used to assess contractual validity and compliance. Rezende [32] highlights periodic review as a procedural necessity to address data privacy risks. The study notes that, under the LED, agencies are required to conduct periodic reviews to assess the necessity of storing biometric data, positioning this measure as an ongoing operational activity rather than a one-time audit. Fabregue [43] and Schwemer et al. [34] discuss human oversight as a continuous review mechanism for high-risk AI systems. Both studies frame human involvement as part of transparency and accountability obligations, requiring providers to ensure that automated decision-making processes can be reviewed and addressed by natural persons. Fabregue [43] links this requirement to the GDPR's safeguard for meaningful human intervention, while Schwemer et al. [34] emphasise that high-risk AI systems must be designed to support effective oversight during operation.

Security Testing

Two papers address security testing through periodic penetration testing [31] and TLPT [45]. Although both papers frame testing as essential for maintaining an appropriate level of security, they are incorporated within different regulatory and operational contexts. Badii et al. [31] apply periodic penetration testing to the Snap4City IoT platform as part of GDPR-aligned security assurance. Testing is conducted by internal developers, external testers, and independent security companies to reduce bias and identify common vulnerabilities, such as those in the Open Worldwide Application Security Project Top 10. In contrast, Seid et al. [45] present TLPT as a requirement under DORA for financial institutions, distinguishing it from conventional testing through its threat intelligence-driven design and its focus on people, processes and technology. TLPT is operationalised using the ASFA framework to simulate realistic adversarial behaviour across cyber, physical, and social domains of cyber-physical systems.

Monitoring

Two papers [31,45] address security monitoring. Badii et al. [31] implement continuous monitoring across infrastructure and access layers in the Snap4City platform to detect unauthorised access and data breaches, while also supporting GDPR-compliant auditing through detailed access logs. In contrast, Seid et al. [45] conceptualise monitoring as part of the Event Model within the ASFA framework, where observable security events derived from behavioural attack models enable monitoring across cyber, physical, and social domains. This event-driven approach supports the detection and response to ICT-related incidents.

Incident Management

Two studies examine incident management primarily through regulatory incident-notification requirements under DORA, NIS 2, and CRA [42,44]. Both emphasise incident reporting as a central regulatory mechanism for timely escalation and coordinated response to threats affecting essential services. Eckhardt and Kotovskaia [42] compare notification obligations under NIS 2 and CRA. NIS 2 requires essential and important entities to follow a multi-stage process for significant incidents (early warning within 24 h, second notification within 72 h, and a final report within one month). CRA requires a single notification within 24 h to ENISA for actively exploited vulnerabilities or incidents. The authors highlight that organisations subject to both regulations must maintain parallel reporting workflows to accommodate different thresholds, timelines, and authorities. Kun [44] argues that DORA seeks to harmonise ICT-incident reporting between financial entities and competent authorities to strengthen coordination and mitigate systemic risk. The author cautions that

DORA's oversight framework for ICT service providers overlaps with supervisory regimes under the GDPR and NIS 2, creating the risk of redundant enforcement and potential duplicative penalties. While incident notification is discussed conceptually, the paper does not provide a detailed analysis of DORA's specific ICT-incident reporting requirements.

4.4. Smart City Solutions

This review identified ten papers that present implemented and validated smart city solutions designed to support compliance with EU regulations. All articles include implementation details and empirical validation, in line with the exclusion criteria of this review, which left out works that were purely conceptual, proof-of-concept only, or lacking implementation details (exclusion criteria #4). Although the reviewed solutions span different domains and rely on heterogeneous enabling technologies, they were examined through the prism of scalability, interoperability, usability, and regulatory compliance. This approach enables the identification of common patterns as well as differences in how regulatory requirements are translated into technical implementations in smart city environments. Based on their regulatory focus and functional characteristics, the identified solutions can be grouped into four main categories: (i) eIDAS-compliant identity and access management solutions, (ii) GDPR-compliant data management solutions, (iii) GDPR-compliant surveillance & public safety solutions, and (iv) a DORA-compliant cyber resilience solution.

One observation is that the reviewed solutions are unevenly distributed across EU regulations. Four papers provide eIDAS-compliant identity and access management mechanisms, four introduce GDPR-compliant data management or automated GDPR verification tools, one presents a GDPR-compliant surveillance solution, and one implements a DORA-compliant testing framework. This pattern mirrors the findings from the application domain analysis, where Digital Identity Management and Data Management emerged as the most technologically mature areas. The predominance of GDPR and eIDAS-related solutions is not unexpected, considering that these are the earliest and most operationalised EU regulations. By contrast, regulations such as the AIA, NIS 2, or the CRA are not represented through implemented solutions in the reviewed literature, suggesting that research in these areas is still primarily conceptual.

Regarding technical characteristics, several solutions demonstrate high scalability, particularly those deployed within large smart city infrastructures such as Snap4City [31] and SmartSantander [27]. Others explicitly acknowledge limitations in scalability or interoperability, as observed in the smashHit tools [40]. Interoperability is a recurring requirement across most of the reviewed solutions [31,37,40,41]. Usability varies depending on the intended users: solutions interacting directly with citizens (e.g., the mobility app in [41]) emphasise user-facing functionalities, whereas solutions targeted at operators (e.g., automated GDPR verification tools and blockchain-based identity and access management mechanisms) focus on configurability and support for compliance tasks. Across the set of GDPR-oriented solutions, the extent to which GDPR compliance is assessed also differs across papers. Some works [33,41] mention compliance only at a high level, while [31] provides a detailed module-level compliance analysis for Snap4City, and [37,40] introduce automated verification mechanisms, with implementations publicly available.

4.4.1. eIDAS-Compliant Solutions

Four papers [8,27,29,30] present implemented and validated identity & access management solutions that follow the requirements of the eIDAS regulation. The solutions include a FIWARE-based identity gateway [27], a smart-contract access control mechanism [8], an attribute-based service delivery approach [29], and an integration of the Italian SPID system with Ethereum to enable authenticated digital transactions [30]. Although the

implementations differ in purpose and technical approach, they share the common goal of enabling secure and verifiable identification in cross-service and cross-organisation settings.

FIWARE–eIDAS Gateway: The solution presented in [27] builds on FIWARE, an open-source smart city platform developed through several EU-funded initiatives, by extending the FIWARE Identity Manager to act as a gateway between OAuth 2.0 and the eIDAS SAML 2.0 protocol. This enables existing OAuth-based services to authenticate users through eIDAS-notified identities without changing their internal login mechanisms. The system was validated in the SmartSantander IoT infrastructure, where the authors demonstrate its applicability within a large-scale smart city deployment. Interoperability is enhanced by enabling two otherwise incompatible authentication protocols to function together. The authors further report that the solution helps address cross-border interoperability challenges identified in eIDAS deployments. From a user perspective, the authentication process remains familiar, as users authenticate through standard OAuth procedures and provide consent as usual. Compliance with eIDAS is supported through the use of SAML-based identity assertions. The main components of the solution include the FIWARE Identity Manager, policy enforcement and decision points, and the OAuth–SAML interface.

Smart-contract Based Access Control solution: The solution proposed in [8] implements access control logic through Ethereum smart contracts to manage distributed information in a healthcare scenario, and the authors suggest that it can be extended to broader smart city contexts. Its scalability is attributed to the decentralised nature of blockchain, which may support multiple organisations without a central authority. Interoperability is facilitated through eIDAS-compatible identity verification, allowing different entities to rely on shared access control rules. The system is primarily designed for operators managing permissions rather than end users. Compliance with eIDAS is supported by enforcing access rules based on verified identities. The implementation consists of Ethereum smart contracts and the supporting distributed data-sharing architecture.

Attribute-based Privacy-preserving Ethereum solution: This solution [29] uses Ethereum smart contracts to provide attribute-based access control and accountability for service delivery. The system is designed to scale across multiple service providers and has been tested in a car-sharing scenario (“Car4U” use case). Interoperability is supported by using shared attribute-verification logic on the blockchain. Usability is oriented toward minimising the information that users must disclose, as only the attributes required for authorisation are shared. Compliance with eIDAS is achieved by relying on verified attributes and by providing accountability through on-chain records. The main components of this solution include attribute-based access control contracts and supporting accountability mechanisms.

SPID–Ethereum Identity-binding Framework: The final solution in this category [30] integrates the Italian Public Digital Identity System (SPID), which is recognised under eIDAS, with Ethereum using Identity-Based Encryption. This approach links SPID-verified identities with blockchain addresses and enables authenticated transactions without requiring users to preregister on the blockchain, which may improve usability. Scalability is supported by the decentralised blockchain infrastructure, and interoperability is demonstrated through the connection between SPID and Ethereum. Because SPID is eIDAS-notified, transactions carried out through this system rely on verified identities that meet eIDAS requirements. The solution includes SPID identity validation, identity–address binding logic, and the supporting smart contracts.

4.4.2. GDPR-Compliant Solutions

Five papers [31,33,37,40,41] present implemented and validated solutions for managing and sharing data in smart city environments while meeting GDPR requirements.

Although the proposed solutions address different use cases, ranging from mobility management to multi-organisational data exchange, they all focus on ensuring lawful processing of personal data through technical and organisational safeguards. Nevertheless, the depth of compliance assessment varies substantially. For instance, Anedda et al. [41] state that the proposed solution is developed in accordance with GDPR, but GDPR is addressed only at a high level, with limited discussion of how specific requirements are met. In contrast, ref. [31] provides a detailed verification of GDPR compliance for each module of the Snap4City platform, based on the requirements of an ideal smart city IoT architecture (Table 3). Finally, Chhetri et al. [37] and Taukeer et al. [40] introduce automated GDPR compliance-verification tools, both developed within the smashHit project, with the implementation artefacts made openly available through public code repositories (i.e., GitHub).

Social Smart City for Public and Private Mobility solution: The solution in [41] is implemented and tested in the Cagliari2020 project and supports mobility management in an area with high traffic concentration. It integrates data from smart cameras, Wi-Fi access points, and crowding sensors through a Social IoT platform to enable real-time traffic monitoring, crowd estimation, dynamic traffic light management, and route optimisation. The proposed solution is reported by the authors to be designed to scale across multiple data sources and public transportation settings. Interoperability is supported through the integration of heterogeneous sensors and communication channels. Usability is addressed through a citizen mobile application that allows users to log in, store preferred destinations, and receive traffic and route information derived from the processed data. The authors claim that GDPR compliance is achieved through a combination of technical measures, but the regulatory focus is very limited. The main components include sensor devices, data-processing modules, anonymisation mechanisms, and the citizen-facing mobile interface.

Snap4City IoT data-management platform: The solution in [31] extends the Snap4City platform to support GDPR-compliant handling of large-scale IoT data in smart cities. Unlike the solution in [41], this work provides a detailed GDPR compliance assessment for each platform module, including nine GDPR-oriented requirements defined for an ideal smart city IoT platform. In addition, the solution was validated over an 18-month period and tested against 150 test cases covering: (i) secure IoT data exchange and analytics for smart city services; (ii) end-to-end encrypted communication between IoT devices, cloud, and dashboards; (iii) smart city operations in mobility, environment, and utilities using Snap4City. The solution is designed to support scalability and can manage data flows from various city infrastructures (i.e., mobility, environmental, and utility). Interoperability is facilitated through multiple IoT communication protocols and integration with external data sources. Usability is primarily aimed at operators through dashboards and analytics tools, while end users are able to review and update or remove their information as part of the system's GDPR-oriented design. GDPR compliance is addressed through technical safeguards embedded across the platform's components, including IoT ingestion services, data-processing workflows, dashboards, and security modules.

Data Protection by Design Tool for Automated GDPR Compliance Verification: The solution presented in [37] introduces a GDPR "data protection by design" tool developed in the smashHit project. The tool performs automated verification of GDPR-informed consent, and the implementation is publicly available on GitHub. In particular, it automatically verifies whether data processing is consistent with the consent provided by users, using a semantic model that represents consent terms, related obligations, and permitted data uses. The solution is intended by the authors to operate across different organisations, making scalability and interoperability central features. Usability is exclusively oriented towards service providers, who can use the tool to check consent validity before reusing or sharing data. GDPR compliance is addressed through explicit modelling of informed-consent

requirements and automated checking of compliance violations. The main components of this solution include the semantic consent model, the compliance-checking engine, and interfaces for retrieving consent and processing metadata.

Automated GDPR Contract Compliance Verification tool: The solution in [40] complements the work in [37] and is also part of the smashHit project. It implements an automated method for verifying GDPR compliance in data-sharing contracts using a knowledge graph that models contractual clauses, data-processing obligations, and relevant GDPR articles. The tool is also available on GitHub. Furthermore, it is designed to support scalability in multi-party environments in which organisations exchange data based on contractual agreements, enabling cross-organisational interoperability. Usability is primarily aimed at service providers, who can check whether their contractual terms allow the intended data operations. GDPR compliance is addressed by mapping contract terms to specific GDPR requirements and detecting inconsistencies or missing safeguards. The solution includes the knowledge-graph model, reasoning rules, and a verification module.

Tool for Effective Identification of GDPR Compliance in Surveillance Videos: The solution presented in [33] focuses on analysing surveillance videos to identify whether GDPR-required privacy safeguards, such as blurring or masking of individuals, have been correctly applied. The proposed solution uses deep learning models to detect these safeguards directly in video frames and was validated as part of EU-funded projects involving real surveillance data. Scalability is supported by the ability of the model to process continuous video streams, making it suitable for environments with high volumes of footage. Interoperability is achieved through the use of standard video inputs without reliance on specific hardware. Usability is aimed at system operators who need automated assistance in checking whether video processing workflows comply with GDPR requirements. The paper states that the solution is designed to support GDPR compliance, but GDPR is discussed only briefly, with limited analysis of specific obligations. In practice, GDPR compliance is addressed solely through detecting whether required privacy safeguards are present or absent in the processed video output. The core components of the solution include trained deep-learning models for identifying privacy-preserving transformations and a module that flags non-compliant video segments.

4.4.3. DORA-Compliant Solution

ASFA DORA-Compliant Threat-Led Penetration Testing Tool: Seid et al. [45] propose a DORA-compliant cybersecurity solution based on the ASFA (Attack-Situation-Focused Analysis) framework. The solution applies ASFA to conduct TLPT in line with the requirements of DORA, which mandates advanced, intelligence-driven penetration testing for financial institutions. The ASFA framework consists of four core components—the Vulnerability Model, Attack-Mechanism Model, Behavioural Model, and Event Model—each capturing different phases of an attack and enabling structured modelling, analysis, and monitoring of adversarial behaviours. Scalability is supported through the framework's ability to model attacks across all three realms of cyber-physical systems (cyber, physical infrastructure, and social), enabling analysis of complex, multi-domain attack paths. Interoperability is facilitated through the integration of heterogeneous data sources, including IT incident reports and threat intelligence feeds, allowing the framework to operate across varied organisational environments. Usability is oriented toward cybersecurity professionals rather than end users: the authors emphasise that effective use requires expertise because manual intervention is still needed to identify critical incidents and interpret behavioural models. Regulatory compliance is presented by the authors as aligned with DORA. The solution operationalises DORA's requirements for threat-led penetration testing (Article 23), enabling financial entities to assess ICT vulnerabilities, evaluate detection and response

mechanisms, and document cross-realm attack progressions. The case study demonstrates the framework's application to real IT incident reports from a Swedish financial institution and to attack simulations (e.g., Cross-Site scripting exploitation through query strings). The main components of the solution are the ASFA modelling framework, the TLPT workflow, and the associated analysis pipeline for vulnerability detection, behavioural modelling, and event capture.

4.5. EU Regulations

The analysis of the selected papers reveals varying degrees of attention to key EU regulations in the context of smart cities, cybersecurity, and data protection. Figure 7 illustrates the representation of each regulation across the reviewed studies. GDPR is the most frequently addressed regulation (48.3% of the papers), appearing in 14 out of the 21 publications, followed by the AIA and eIDAS (13.8% each). NIS 2, DORA, and the LED are addressed uniformly (6.9% each), while only one paper discusses the CRA (3.4%).

In this section, we investigate how state-of-the-art literature addresses these EU regulations within a technical or legal context, to what extent the studies mention specific provisions, which regulatory aspects receive the most attention, and where legal uncertainties or gaps can be observed.

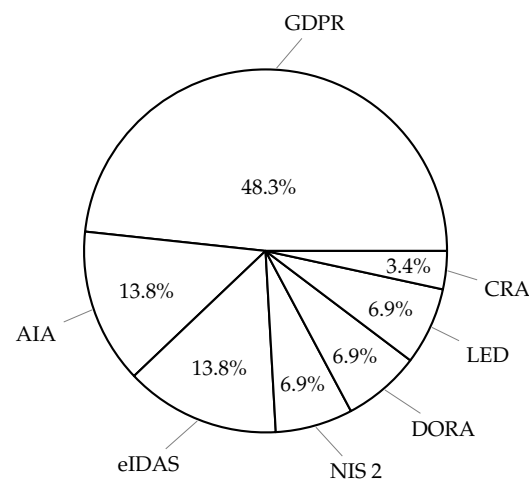


Figure 7. EU regulations representation in our research.

4.5.1. GDPR

Based on general patterns observed in the literature on GDPR, the following three key categories emerge: (i) technical papers on GDPR, (ii) legal papers on GDPR, and (iii) papers examining the interaction between GDPR and other EU regulations. The six technical papers on GDPR focus primarily on discussing GDPR in terms of smart city solutions or specific security countermeasures in compliance with the regulation. The legal papers instead analyse specific GDPR requirements, legal definitions, or legal uncertainty related to GDPR. The third category highlights the interaction between GDPR and other EU regulations, such as the AIA, the LED, and DORA, and discovers any similarities, differences, and potential gaps.

Technical Papers

Three studies [33,39,41] have a limited focus on GDPR related to GDPR safeguards, such as encryption and anonymisation. Anedda et al. [41] discuss GDPR in the context of protecting sensitive data like vehicle licence plates. Since GDPR prohibits the storage and transmission of such data without drivers' consent, the authors use anonymisation to assure users' privacy. Asghar et al. [33] mention GDPR in the context of data privacy and

obfuscation for large volumes of video surveillance data in smart cities. Data protection by design is achieved with the use of encryption as a reversible safeguard for data protection of CCTV frames in smart cities. Stach et al. [39] take a different approach to GDPR by assessing whether privacy-by-design blockchains are feasible. The authors highlight specific GDPR articles with which blockchains are in conflict when handling personal data. For example, immutability violates the right to be forgotten, while tamper-proofness makes anonymisation of data subjects impossible. The study presents technical solutions that can address these conflicts and how they can potentially be applied to blockchains.

The focus of papers [31,37,40] is GDPR-compliant smart city solutions based on high-profile funded projects, such as Snap4City and Horizon 2020 project smashHit. We expand more on these in Section 4.4. A common pattern about these three papers is that they all present the GDPR regulation and highlight various GDPR articles and requirements relevant to their corresponding solutions. Badii et al. [31] examine signed consent in the context of authorisation/delegation for managing personal data, the latter being treated as private for the user prior to any delegation. Encryption of personal data is another safeguard mentioned for preventing users' identification in case of compromise. The right to be forgotten in the context of data erasure, as well as auditing support for users so they can monitor access to their data, data breach detection, and data protection by design and by default, is all taken into account. Chhetri et al. [37] discuss challenges for companies when complying with GDPR and focus on consent, data subjects, fines for non-compliance, GDPR-required TOMs, and data protection by design when implementing their solution. What is unique about this paper is the authors' collaboration with legal experts to truly understand and fulfil GDPR's legal requirements in their solution, having the legal team supervise the implementation of TOMs into code. Tauqeer et al. [40] examine consent in relation to contracts and identify various scenarios where consent is not sufficient, such as online services that require a contract, or Business-to-Business and Business-to-Consumer data sharing with contracts. The authors explain that this is due to the need for complex terms and conditions between all contractual parties. The study highlights consent in the context of use cases in the insurance domain and the general smart city domain.

Legal Papers

Three articles [26,28,36] critically assess GDPR for legal gaps and uncertainties in different contexts. Benyahya et al. [36] analyse in depth the GDPR requirements for the collection and transmission of vehicle data that should be considered by stakeholders of automated city shuttles (ACS). Specifically, the authors examine data processing principles (purpose limitation, data minimisation, etc.), rights of data subjects (e.g., right to be informed, right to erasure, etc.), and obligations of ACS' stakeholders, such as data controllers, data processors, and joint controllers. The study states that the roles of these stakeholders are ambiguous in terms of compliance obligations due to GDPR not requiring a specific legal binding act, and the fact that the roles of data controller and data processor can overlap and change rapidly. In the context of DPIA (Art.35), the authors highlight that it is an accountability tool for controllers and part of their responsibilities, but also a challenge due to the rapidly evolving autonomous technologies and time constraints for performing and reassessing DPIA periodically. Their study also uncovers how legal requirements coexist with existing technological solutions for preserving data privacy within the ACS domain and identifies a gap between legal definitions and technological implementation of privacy-preserving techniques (mainly pseudonymisation and anonymisation). From a legal perspective, GDPR considers pseudonymisation as an appropriate measure by itself, but instead, the authors propose the use of a combination of pseudonymisation with further anonymisation for strengthening privacy. The regulation also considers pseudonymisa-

tion reversible and anonymisation as permanent, but forgets to highlight that the risk of de-anonymisation may lead to re-identification over time. Legal provisions are not precise about which anonymisation techniques should be applied to which context, despite the different likelihood of re-identification. From a technical perspective, the authors point out that the likelihood of re-identification is never zero. Therefore, anonymisation is not permanent and can be reverted in the future, and so it should be continuously assessed and selected on a case-by-case basis.

George et al. [28], on the other hand, examine whether transient processing of data by facial detection and mapping technologies falls under the GDPR and show through use cases how ephemeral processing may fall outside the scope of GDPR depending on interpretation. The argument is that transient data processing technologies minimise the retrieval of already processed data, and therefore data protection authorities deem such transient data as not legally ‘personal data’ because it does not allow for re-identification, but an effect-oriented interpretation of GDPR would allow transient technologies leading to discriminatory treatment of users to fall under the scope of the GDPR. Taking a risk-based approach to ‘personal data’ would make the regulation more relevant to technologies that try to bypass it.

In contrast, Kindt [26] addresses the use of biometric data for unique identification of a natural person, which is prohibited under the GDPR, and highlights ten exemptions to this prohibition in Article 9 of the regulation. The author argues that Article 9 does not consider all processing of biometric data as ‘sensitive data’ and points out a challenge with biometric data being collected and stored in a database under the guise of ‘processing’, which could permit future identification even though that is prohibited under GDPR. Kindt explains that identification is a one-to-many search and requires a database of listed individuals, while processing for the purpose of verification is a one-to-one biometric comparison, which is different from identification. The study highlights that verification does not fall under this GDPR prohibition, which is a problem when users and decision-makers do not understand the difference between the two functionalities and in which cases each is used. GDPR neither explicitly mentions nor reflects on this distinction, and the author argues that the prohibition in Article 9 leads to legal uncertainty. The article also criticises GDPR for the subjective and artificial distinction between categories of biometric data. Kindt identifies and explains the four different categories of personal data in GDPR, such as ordinary personal data, biometric data under Art.4, ‘sensitive’ biometric data under Art.9, and ‘sensitive’ biometric data that requires DPIA under Art.35, all of which allow identification or identity verification.

GDPR Interaction with Other EU Regulations

Six papers [26,32,34,35,43,44] examine GDPR in relation to other EU regulations, such as the AIA, the LED, and DORA. Three articles [34,35,43] focus on GDPR’s connection with the AIA in terms of the bias exceptions provided by Article 9 of GDPR on processing of special categories of personal data and highlight how Article 10 of the AIA introduces a legal basis for processing such sensitive data for debiasing purposes, especially in high-risk AI systems. Fabregue [43] takes a regulatory perspective on AI governance in smart cities and discusses touching points between GDPR and the AIA from an ethical perspective, as the fundamental approach of the GDPR (based on human rights) is carried over into the AIA. The author acknowledges that the AIA is, however, less focused on protecting citizens’ rights than the GDPR. Fabregue further highlights that GDPR is insufficient to address the AI reliance on personal data, but the AIA seeks to address this gap. The author questions whether GDPR and AIA work effectively together, since the AIA does not explicitly include

GDPR's guidelines on data collection and processing (such as Art. 5-14, 16-18, 21), and does not mention the GDPR in terms of data set characteristics.

Veale and Borgesius [35], on the other hand, draw a connection between the AIA and GDPR in the context of the AIA banning some uses of 'real-time' biometric systems. The authors point out that AIA does not ban the use of remote biometric identification for non-law enforcement purposes that typically fall under the GDPR. However, since the GDPR requires individual consent for each scanned person, that requirement is impossible to fulfil in practice, and is therefore a major shortcoming of the AIA.

The papers in [26,32] assess GDPR in relation to the LED. Kindt [26] discusses some similarities and differences between the two regulations. Both GDPR and LED agree on which data are considered biometric data for verification or identification of a natural person. The author explains that both regulations have a narrow and identical definition of biometric data. A database containing fingerprints or facial images without biometric processing may not be considered a biometric database according to the law, and Kindt argues that their existence is a risk for the fundamental rights of data subjects. As such, both regulations agree that facial images become biometric data only when used for biometric comparison, or 'specific technical processing'. The study highlights one interesting difference between the two regulations—the LED does not contain anything similar to Recital 51 of the GDPR, the latter clarifying that photographs can be defined as biometric data only if processed through biometric technical means that allow for the unique identification of a natural person. However, Kindt states that GDPR is unclear whether it applies to all 'photographs', which can also be termed 'images' of a fingerprint or an iris, among other examples. The retention of databases by law enforcement authorities is also concerning due to potential issues with fundamental rights.

Rezende [32] assesses GDPR and the LED in relation to data scraping activities of a facial recognition technology by Clearview AI, which plans to collaborate with EU law enforcement agencies. The author points to data scraping as an example of data processing operations that are not analysed sufficiently in the literature. In this case, it involves a private company collecting personal data with the intent to sell it to law enforcement agencies in Europe. Rezende provides a legal analysis of the impact of this facial recognition tool on human rights, and investigates whether these data scraping practices are compliant with the GDPR and the LED. The author concludes that any Clearview data scraping activities related to the monitoring of data subjects in the EU would fall within the scope of the GDPR (Art.3), and the LED is not applicable at this stage before law enforcement gets involved. Since a special category of personal data is being processed, the authors analyse whether the requirements of Article 9 GDPR apply. One identified problem with GDPR is that the regulation is not clear on what 'publicly available' data means, especially when it comes from social media websites.

In contrast, Kun [44] discusses the overlapping regulatory oversight for critical cloud service providers (CCSPs) in both DORA and GDPR. The author explains that this is due to the fact that CCSPs can play the role of a processor or controller depending on whether they process personal data for a financial institution or for their own purposes. When complying with GDPR, CCSPs are subject to oversight by supervisory authorities (Art.51, 55, 56 GDPR). The author gives a hypothetical example of a data breach, in which case GDPR and DORA will concurrently investigate the same incident with the supervisory authorities under GDPR and the Lead Overseer under DORA. This could potentially result in duplicative penalties that challenge the *ne bis in idem* principle. This duplicative oversight is, however, not addressed in either of the regulations, and the article recommends that the Lead Overseer and Supervisory Authorities coordinate in order to avoid any redundant enforcement measures resulting from the regulatory overlap.

4.5.2. LED

Two articles [26,32] analyse the LED in relation to biometric data for unique identification in the context of law enforcement and the legal uncertainties arising from processing such biometric data. Kindt [26] highlights that the LED, similarly to GDPR, has provisions related to biometric data for law enforcement authorities. The Directive adds a new category of special data to the list of sensitive data, namely biometric data that uniquely identifies a natural person. Such biometric data can be processed in the prevention of crime, execution of penalties, when preventing threats to public security, and when data are processed by ‘competent authorities’ under certain conditions. LED imposes obligations for controllers to make a DPIA, but it is based on a general provision similar to Art.35 GDPR. The LED also highlights that profiling by competent authorities is forbidden unless authorised by national law, which remains unclear on the subject of biometric data processing. The author expresses concern that national law on the storage of biometric data is lacking in the EU member states, and biometric databases are therefore allowed to continuously grow and be used without a clear legal basis in the EU.

Rezende [32] analyses whether the Clearview app complies with Article 10 of the LED, which sets criteria for lawful processing of biometric data. The author analyses the scope of the LED’s application in the context of a potential partnership between Clearview and EU law enforcement agencies. Rezende points to legal uncertainty when private parties and law enforcement authorities share data. First, when private entities are bound by a contract or a legal act to law enforcement agencies, this makes them ‘processors’ under the LED as they process data on behalf of competent authorities. As such, GDPR applies to the initial data processing, while the LED regulates data processing within the public-private partnership. Second, if the private and public parties in the partnership are equals, then this is a case of joint controllership, where the private party is also a ‘competent authority’ (Art.3 of LED). Since Clearview acts as a facial recognition provider to competent authorities in the US, joint controllership is unlikely in the EU, and Clearview would be a processor under the LED, which would partner with police departments and offer its processing services.

Furthermore, the author argues that since facial images that result from specific technical processing or allowing for unique identification of a natural person are considered biometric data under Art.3 LED, then biometric processing that allows identification of data subjects and also comparison using an AI system by Clearview will need to comply with Art.10 LED. As such, the author assesses the lawful processing requirement, the strict necessity test, and appropriate safeguards, and concludes that the Clearview system is deeply problematic in terms of compliance. One example is that it does not comply with Art.5 LED for appropriate time limits for data storage and erasure of personal data. The author points out that there is a need for stricter rules on staff access to the competent authority, as well as more focus on data security measures protecting Clearview’s databases, which have already been exposed to data breaches. Ultimately, providing such a powerful surveillance tool in the hands of law enforcement would make it challenging to prevent abuses and limit its use to strict necessity in the EU.

4.5.3. eIDAS

Four studies are based on the EU’s eIDAS regulation [8,27,29,30]. A notable observation is that all four articles are technical papers that propose eIDAS-compliant smart city solutions, and only two of the papers [27,30] provide a brief overview of the eIDAS regulation and its purpose. Alonso et al. [27] give an overview of eIDAS in the context of data protection, privacy, and the prevention of online fraud, highlighting its central role in enabling trust in smart cities. The implementation presented in this study addresses a key practical challenge for private and public service providers by significantly reducing

the complexity when integrating with the SAML-based eIDAS infrastructure. The papers in [8,29,30] present solutions that integrate Ethereum smart contracts and eIDAS-based attribute and identity management. Unlike legal papers that analyse regulations in terms of specific provisions, legal gaps, or shortcomings, the focus here is instead on real-world implementations that integrate with the eIDAS ecosystem. This trend could be attributed to the regulatory maturity of the eIDAS regulation and its wide deployment by industry. Specific details about the technical measures and implementations of these solutions can be found under the technical measure ‘Identity and Access Management’ in Section Identity & Access Management, as well as Section 4.4.1 under eIDAS-compliant identity and access management solutions.

4.5.4. AIA

Four studies [34,35,38,43] focus on the AIA and the risk of AI-based services on human and fundamental rights, but their approach towards this is different. A notable observation is that all four articles are legal papers on the AIA in a smart city context. The lack of technical papers on the subject could be attributed to the lag between the adoption of the AIA in 2024 and technical implementations focused on compliance.

The papers in [34,35,43] give an overview of the AIA, how AI systems are defined, and the four risk levels of AI practices—*unacceptable risk* (banned practices like manipulative systems, social scoring, and real-time and remote biometric identification systems), *high risk* (strict rules for biometric identification, critical infrastructure etc), *limited risk* (transparency for bots and deepfakes), and *minimal risk*, the latter not of focus in any of the papers. The paper by Veale and Borgesius [35] focuses also on *limited risks* regarding AI practices, and highlights the requirement of bot disclosure. However, this liability goes only to technology providers, and not to users of AI systems. Instead of the AIA making a distinction between a user and a provider, the paper in [35] urges a hybrid approach to interpretations of bots and chatbot vendors.

Schwemer et al. [34] see as noteworthy that the definition of an AI system is so broad that many existing legal AI use cases would fall under its scope, but at the same time, only very few legal AI systems would be considered in the high-risk category. As such, these non-high-risk AI systems are under self-regulation according to the AIA. Fabregue [43] highlights the lack of a generalisable legal definition of AI across smart city domains, and since the definitions of AI change significantly and often, the term is highly ambiguous, and the impact of AI technology in smart cities is likewise difficult to measure. Veale and Borgesius [35] also highlight grey areas in the AIA, such as the scope of the provisions being too limited and specific loopholes. For example, the regulation actually permits manipulative AI systems if they are unlikely to cause physical or psychological harm, instead of focusing on whether the manipulator’s goals are achieved. Moreover, harm can be cumulative and difficult to prove, and this is also valid for AI systems where distortion or harm arises from discriminatory ratings, recommendations, or classifications of people. Another limitation of the AIA observed in [35] is in terms of AI systems generating trustworthiness scores, where the AIA does not clearly define ‘trustworthiness’ and whether certain scoring practices are in-scope is open to interpretation.

The papers in [34,35,43] observe that the compliance framework for high-risk AI systems seems weak, as it relies primarily on AI provider-led self-conformity assessments conducted without external oversight. It leads to a lack of feedback and translation of rules for the industry, resulting in knowledge gaps in the practical implementation of the AIA in smart cities. Fabregue [43] assesses this regulatory gap as a fundamental weakness of the AIA, which gives AI providers a lot of freedom with decisions that can violate fundamental rights while failing to establish effective accountability mechanisms for violations.

In contrast, Rezende [38] examines the provisions of the AIA in relation to automated facial recognition (AFR) and emotion recognition technologies in the law enforcement context, particularly how the use of high-risk AI systems by law enforcement causes significant intrusion on fundamental rights (recital 38), such as privacy and data protection due to the power imbalance between the public authorities and individuals subjected to surveillance. This also increases the risk of profiling, discrimination, and misinterpretation of emotions leading to wrongful suspicion.

In terms of recommendations for improvement of the AIA, Fabregue [43] recommends three main principles the AIA could base itself upon—fairness, privacy, and transparency. The regulation proactively mandates fairness in high-risk AI systems but faces criticism for vague requirements and insufficient measures to prevent bias. Privacy is addressed by connecting to existing GDPR protections and technical cybersecurity for high-risk systems. However, the AIA treats privacy as an afterthought, failing to mandate robust privacy-by-design principles like data minimisation and purpose limitation in smart cities. While the goals of fairness and privacy are not met, Fabregue [43] affirms that the AIA provides decent protection of transparency in high-risk AI systems, by mandating its implementation by design, including proper template-based instructions, and proper human review for problematic cases (Art.12-14).

4.5.5. NIS 2

The papers in [42,44] examine points of interaction between the NIS 2 directive and EU regulations, such as CRA and DORA, and analyse regulatory overlaps and areas for improvement. Kun [44] investigates potential overlapping oversight between NIS 2 and DORA on critical cloud service providers (CCSPs) by conducting a legal analysis of both previous drafts and the final version of DORA. In NIS 2, CCSPs are considered digital infrastructure and are subject to full supervision by the competent authorities (e.g., on-site inspections, security audits, access to data, etc.). Such direct supervision is critical for the mitigation of systemic risk in the finance domain, but according to the article, the extent to which these regulatory frameworks can be implemented in a coordinated manner is unclear. The paper explores the argument that DORA could be considered *lex specialis* to NIS 2 Directive, such that DORA's more specific rules prevail over the general rules of NIS 2. This would imply no overlapping oversight between the two regulations, but Kun points to Recital 16 of DORA, which refers only to ICT-related incident reporting and risk management for financial entities. Therefore, Kun argues that CCSPs are not covered by DORA's *lex specialis* provisions, and concludes that there is overlapping oversight between NIS 2 and DORA on CCSPs. Kun highlights that the final version of DORA focuses on strengthening the oversight coordination between the two regulations to prevent disproportionate penalties, such as duplicative monetary fines, which contravene a key human right—the *ne bis in idem* principle of not punishing anyone more than once for the same offense. The article concludes that there is still room for improvement in the coordination between the competent authorities when it comes to excessive, duplicative monetary fines, as the Lead Overseer under DORA is not explicitly required to consider the penalties imposed by the national competent authorities under NIS 2.

Eckhardt and Kotovskaia [42] examine the regulatory interplay between NIS 2 and CRA on risk management measures, risk assessments, notification requirements, and market surveillance, as well as how the two regulations classify critical products with digital elements. The article points out obligations of operators of essential services and digital service providers in terms of risk management measures (such as supply chain security measures) under the NIS 2 directive, whose goal is to minimise the impact of cyber-related incidents. CRA's goal is to facilitate the compliance of digital infrastructure

providers with the supply chain requirements of NIS 2 through coordinated security risk assessments for critical ICT products and services. However, the authors highlight that CRA has different levels of criticality for products with digital elements, which are also regarded as critical ICT products by NIS 2, and so there may be overlaps between the two regulations in terms of identifying products critical for the supply chains. The authors point out one complication arising from the different notification requirements in NIS 2 and CRA, namely that essential and important entities as referred to in NIS 2 that are also manufacturers according to the CRA must use different procedures for incident reporting. The authors call for alignment between these provisions so that the burden on reporting actors and notified authorities is lowered.

4.5.6. DORA

The papers in [44,45] analyse different DORA requirements in the context of potential overlaps with NIS 2 and GDPR. Seid et al. [45] use their ASFA framework to conduct TLPT in accordance with DORA. The authors claim that their smart city solution is DORA-compliant, and this is discussed in more detail in Section 4.4. The authors refer to Article 23 DORA regarding the requirement for conducting TLPT once every three years, explaining that the frequency of penetration testing can be adjusted based on the risk profile and operating circumstances of the financial companies. Since this is a technical paper, it has a very limited regulatory perspective, which consists of an overview of DORA, its purpose, measures, and relevant stakeholders. Seid et al. highlight that for entities under NIS 2, there are no requirements for any TLPT, which means DORA does not overlap with other regulations regarding its testing requirements.

In contrast, Kun [44] provides an overall overview and legal analysis of DORA in the context of critical ICT third-party service providers, such as critical cloud service providers (CCSPs), where the overlapping oversight of CCSPs between DORA, NIS 2, and GDPR is of focus. Kun outlines the concurrent supervision of CCSPs under DORA and the NIS 2 directive, which can potentially result in duplicate legal proceedings and penalties. Therefore, DORA acknowledges the importance of a judicious coordination framework for the purpose of preventing disproportionate measures, such as duplicative administrative fines. To achieve this, the author mentions four aspects from Art.32, 42, 47 DORA, namely the addition of a representative competent authority under NIS 2 to the Oversight Forum, the Lead Overseer has to consult the competent authorities under NIS 2 to avoid imposing double technical and organisational measures, and the requirement for the competent authorities under DORA to voluntarily consult first with those under NIS 2 on oversight of CCSPs, including contract termination, technical assistance, advice, and on-site inspections. The author argues that this coordination can be improved further, especially in the context of monetary fines, as the Lead Overseer under DORA is not explicitly required to consider monetary fines imposed under NIS 2 upon the same CCSPs. Therefore, there is a risk of excessive burden on the CCSPs in terms of potential duplicative enforcement. Furthermore, the same risk applies if the Lead Overseer under DORA does not coordinate enforcement with the national supervisory authorities under GDPR (Art.55, 56 on CCSPs).

4.5.7. CRA

Eckhardt and Kotovskaia [42] examine the CRA and its relation to the smart city domain. The article focuses on the interaction between the CRA and the NIS 2 Directive in terms of risk management and the classification of critical products with digital elements. The authors argue that the CRA addresses a regulatory gap by introducing horizontal cybersecurity requirements aimed at improving the resilience of such products. It also provides legal certainty for economic operators, including manufacturers, importers, and distribu-

tors, by defining their obligations. These requirements apply across sectors, although the CRA excludes certain product categories (e.g., medical devices or motor vehicles) already covered by other EU regulations. The authors further highlight overlaps between the CRA and other regulatory frameworks for products such as radio equipment and AI systems. However, as this analysis is based on a single study, the insights related to the CRA should be interpreted as preliminary and reflective of the current state of the literature rather than the maturity or impact of the regulation itself.

4.6. Summary

Figure 8 illustrates the main findings of this comprehensive review. It synthesises the identified application domains and stakeholders, and relates them to regulatory-driven cybersecurity compliance solutions for smart cities, including the relevant measures and EU regulations addressed in the literature.

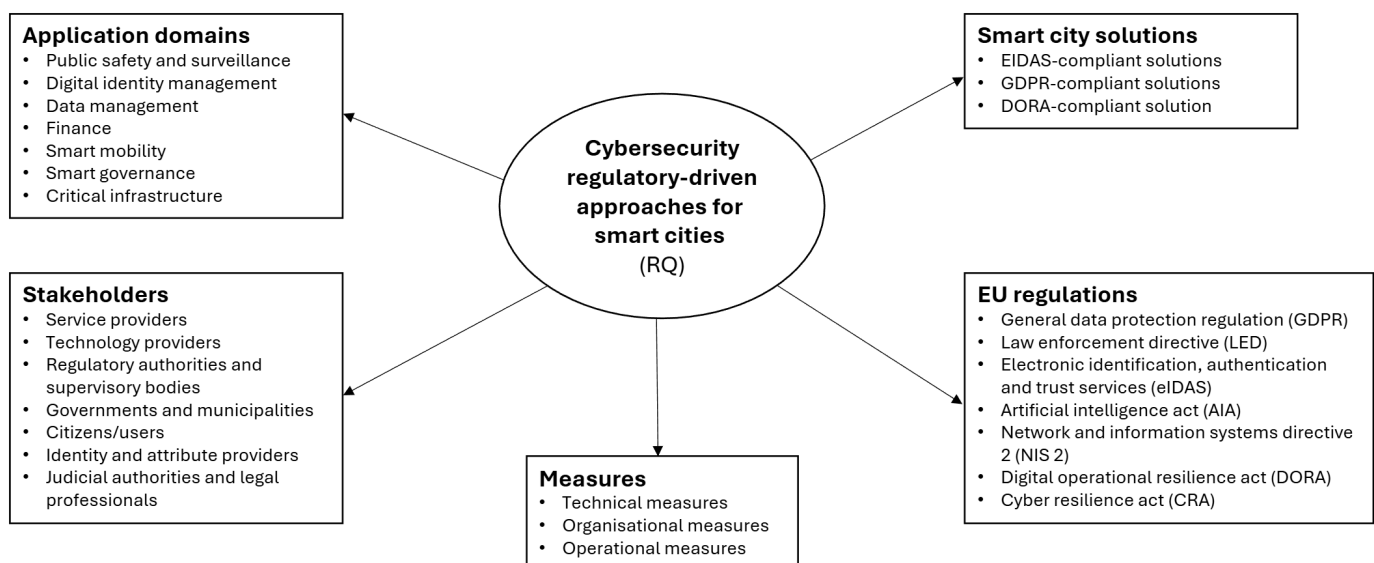


Figure 8. An overall summary of main findings.

5. Discussion

This review tackles the research question of how to map regulatory requirements and specifications to cybersecurity technical approaches for the smart city ecosystem. In addition to our primary results, the literature review allowed us to identify several emerging trends and research gaps (Section 5.1). This section also discusses our findings within the context of regulatory-driven cybersecurity solutions for smart cities that we observed while surveying the selected articles, and identifies challenges and risks (Section 5.2), legal perspectives (Section 5.3), and necessary directions for future research and strategic actions (Section 5.4). Overall, findings related to recently introduced regulations should be interpreted with caution, as they are based on a limited number of studies and reflect early-stage developments in the literature.

5.1. Trends & Gaps

Beyond the primary results, this review reveals several recurring trends and persistent gaps in the literature on regulatory-driven cybersecurity solutions for smart cities. Overall, the findings indicate that research in this area remains fragmented, both across disciplines and across regulatory and application contexts. A central gap concerns the limited interdisciplinary integration between legal and technical research. While the research question requires linking EU regulatory requirements to technical cybersecurity solutions,

most studies address only one side of this relationship. Legal works focus on interpreting obligations, overlaps, and risks, whereas technical studies prioritise system design with limited engagement with regulatory provisions. This divide is particularly evident for newer instruments such as the AIA, NIS 2, LED, and CRA, which appear mainly in legal analyses, while eIDAS is addressed primarily in technical implementations. GDPR and DORA are the only regulations consistently examined from both perspectives. As a result, regulatory insights are not easily translated into technical requirements, and technical solutions often lack depth in regulatory compliance, creating uncertainty for municipalities and solution providers.

A second gap relates to the uneven coverage of the EU regulatory landscape (see Section 4.5 regarding the distribution of the coverage of the regulations). Several relevant instruments, including the CER Directive, CSA, eIDAS 2.0, DGA, Data Act, DMA, DSA, Interoperable Europe Act, and the AI Liability Act, are largely absent from the reviewed literature. While this may partly reflect their recent introduction, it highlights the need for further research addressing emerging cybersecurity and data protection regulations. The regulations are only emerging, and further research is required, particularly regarding addressing the cybersecurity laws. Specifically for the updated version of eIDAS 2.0, while it has the potential to provide trustworthy, interoperable digital identities for smart city services, practical implementations are still a future development. Academic research will require established implementations, concrete use cases, and data for analysis.

A further recurring issue is the shallowness of both technical implementations and regulatory compliance claims. Although many studies propose cybersecurity measures, they often provide limited detail on configuration, integration, or long-term operation. While technical and, to some extent, operational measures are implemented and evaluated (typically in small-scale pilots or controlled environments), only a few solutions, such as the FIWARE–eIDAS gateway and Snap4City, demonstrate deployment in larger-scale infrastructures. In contrast, organisational measures, including DPIAs, role allocation, and training, are primarily discussed at a conceptual level and are rarely translated into concrete solutions. Similarly, many works claim compliance with regulations, particularly the GDPR, without demonstrating how specific legal obligations are implemented, verified, or monitored over time. This imbalance highlights the limited translation of legal requirements into organisational practices, in contrast to more frequently operationalised technical and operational measures, providing a more critical perspective on how regulatory obligations are (or are not) operationalised in practice.

This imbalance is also reflected across application domains. Mature and validated solutions are concentrated in Digital Identity Management and Data Management, where long-standing regulations such as eIDAS and GDPR have enabled the development of concrete frameworks. In contrast, domains such as Smart Governance and Critical Infrastructure remain underrepresented, despite their strategic importance. The lack of a common definition of critical infrastructure across EU regulations may partly explain this gap. Overall, these findings indicate a lag between regulatory development and technical implementation, particularly for newer instruments such as the AIA, NIS 2, CRA, and eIDAS 2.0. Across domains, another recurring gap is the limited depth of demonstrated regulatory compliance: several papers claim alignment with EU regulations, especially the GDPR, without providing sufficient technical detail to verify how specific legal obligations are implemented, monitored, or enforced. Only a small subset of solutions offers publicly available implementations that enable external validation and reuse. Taken together, these findings indicate that while certain regulatory areas have reached a degree of technical maturity, much of the current research remains unevenly distributed across domains and

often stops short of fully operationalising regulatory requirements in implementable and verifiable smart city solutions.

The analysis also reveals gaps in stakeholder representation. Service and technology providers dominate the literature, while municipalities and public authorities are discussed only superficially, despite their central role in governance. Citizens are primarily treated as passive data subjects rather than active participants in system design or decision-making. In addition, stakeholder roles are often framed using regulation-specific categories (e.g., data controllers, processors), which do not fully reflect real-world practices where actors may fulfil multiple roles simultaneously. These ambiguities are acknowledged in some works, such as in the context of automated city shuttles and cloud service provision, but remain largely unexplored.

Finally, ethical considerations remain underexplored. Issues such as function creep and the integrity of stakeholders in interpreting legal provisions receive limited attention. Only a small number of studies highlight broader societal concerns, such as the Clearview case [32] or the limitations of the AIA in addressing private-sector surveillance [35]. Given the potential impact of smart city technologies on fundamental rights, these aspects require stronger consideration in future research. Taken together, these findings suggest that regulatory-driven cybersecurity research for smart cities is still evolving. While certain domains and regulations show signs of maturity, the literature lacks integrated, empirically grounded approaches that effectively bridge legal requirements, technical design, and real-world governance.

5.2. Challenges & Risks

This work highlights several challenges and risks arising from the interaction between legal obligations and technical implementations in smart city solutions. A recurring concern is whether the current EU regulatory “patchwork” effectively strengthens privacy and security, or instead introduces overlapping requirements that complicate compliance and implementation. One key technical challenge relates to the increasing use of blockchain-based Identity and Access Management solutions. While blockchain technologies (e.g., Ethereum and smart contracts) enable decentralised trust and accountability, they create tensions with GDPR requirements, particularly regarding data minimisation, purpose limitation, and the right to erasure. Proposed mitigation strategies, such as data purging, privacy filters, distributed architectures, and off-chain storage, help address these conflicts but introduce additional architectural complexity, highlighting the difficulty of reconciling immutable systems with data protection obligations.

A second challenge concerns stakeholder complexity in smart city ecosystems. Identifying relevant actors and aligning their differing priorities, particularly across public and private sectors, complicates system design and governance. This is further reinforced by the organisational complexity of cities, where municipalities operate under multiple, often overlapping legal frameworks, sector-specific regulations, and local norms. As a result, deploying smart city technologies requires navigating the complexity of cities as organisational units, combined with the coexistence of multiple, often overlapping legal frameworks and local norms that vary from one municipality to another.

Emerging data-driven technologies also introduce broader societal and ethical risks. AI-based systems, in particular, raise concerns related to surveillance, bias, and lack of transparency. Addressing these risks requires more than technical safeguards alone. The literature highlights the need to translate normative values, such as fundamental rights, into concrete technical and organisational practices. In this context, regulatory bodies play a crucial role in enforcing compliance and limiting harmful practices, thereby fostering trust and enabling citizen participation in smart city environments.

Finally, a persistent challenge is the temporal and technological lag between regulation and innovation. EU regulatory frameworks often struggle to keep pace with rapid technological developments, creating interpretation gaps and uncertainty for developers and operators. This is especially evident in the case of the AIA, which continues to evolve in response to emerging AI capabilities. Taken together, these challenges demonstrate that regulatory-driven cybersecurity in smart cities is not only a technical issue but also a legal, organisational, and societal one. Addressing these risks requires coordinated evolution of legal frameworks, technical architectures, and governance practices.

5.3. Legal Perspective

A key source of ambiguity emerging from the reviewed literature is the lack of precise legal definitions within EU regulatory frameworks, which leads to inconsistent interpretations by technical and legal stakeholders. For instance, the classification of transient data captured and immediately deleted by cameras raises uncertainty as to whether such data qualify as personal data under the GDPR [28]. Similarly, in the context of biometric data, both the GDPR and the LED provide limited clarity on what constitutes “sensitive” data, resulting in ambiguous distinctions between identification and verification, as well as uncertainty regarding the storage and potential reuse of biometric datasets [26]. In the domain of AI governance, additional ambiguity arises from the lack of a precise legal definition of AI in smart city contexts and from the broad classification of “high-risk” systems under the AIA [34,43]. This is further compounded by enforcement mechanisms that may rely on self-assessment, such as provider-based certification of high-risk AI systems, potentially limiting external oversight and accountability [35].

Another source of complexity concerns the interaction and overlap of multiple regulatory frameworks across domains. Smart city systems often operate at the intersection of sector-specific and horizontal regulations, requiring simultaneous compliance with multiple legal instruments. This can lead to conflicting requirements, such as overlapping oversight of cloud service providers under DORA and NIS 2, or tensions between the AIA and GDPR, where the use of sensitive data for bias mitigation under the AIA may conflict with GDPR restrictions [43,44]. Similarly, differences in incident reporting timelines between the CRA and NIS 2 illustrate how regulatory overlaps can create uncertainty for implementers [42].

On top of that, a further limitation lies in the gap between high-level legal principles and their technical implementation. Regulations such as the GDPR establish concepts like data protection by design, pseudonymisation, and the right to erasure, but often lack concrete technical guidance. For example, while pseudonymisation is encouraged, the regulation provides limited direction on appropriate techniques or on mitigating risks such as de-anonymisation over time [36]. Similar challenges arise in reconciling blockchain immutability with the right to erasure, where technical workarounds exist but are not explicitly addressed in legal frameworks [39]. Moreover, requirements such as DPIAs are mandated but not standardised, particularly in complex contexts such as AI-driven systems [43]. Furthermore, there are no specific enforceable standards that can measure and limit GDPR’s proportionality principle in real use cases. Specifically, when collecting large datasets of personal data for training AI models, there is a tendency to bypass GDPR’s principle of data minimisation and potentially also the purpose limitation principle with any subsequent use and transmission [36].

Furthermore, the temporality dimension of the law introduces additional complexity. Legal frameworks often lag behind rapid technological developments, creating uncertainty for both developers and regulators [48]. Although the GDPR acknowledges this challenge—for example, by linking identifiability to the “state of the art” (Recital 26)—

practical mechanisms for continuous adaptation remain limited. Proposed approaches, such as continuous compliance management or adaptive regulatory frameworks, highlight the need for more dynamic governance models [9].

Finally, the literature suggests that regulatory compliance is often perceived by technical stakeholders as a burden, largely due to the complexity, ambiguity, and cross-referencing of legal texts. This perception may lead to superficial or inconsistent interpretations of legal requirements. Ensuring accurate and context-aware interpretation of legal instruments, including understanding their hierarchy and interactions (e.g., *lex specialis* vs. *lex generalis*), is therefore essential for translating regulatory provisions into effective technical and organisational measures. Overall, these findings highlight that legal ambiguity, regulatory overlap, and the gap between legal principles and technical implementation remain significant barriers to achieving effective regulatory-driven cybersecurity in smart city systems.

5.4. Implications and Recommendations

The findings of this review suggest that the successful evolution of smart cities requires a shift from fragmented, local implementations towards more integrated and multidisciplinary governance approaches. As urban systems increasingly rely on interconnected infrastructures and AI-driven data processing, public trust and technical robustness emerge as essential prerequisites for long-term sustainability. A key implication concerns the need for stronger interdisciplinary collaboration. While privacy and security are widely addressed, the literature pays limited attention to trade-offs with other objectives such as sustainability, utility, cost, and safety. Addressing these trade-offs requires closer cooperation between technical experts and legal professionals, as well as mechanisms to balance the interests of multiple stakeholders. However, concrete examples of successful cross-disciplinary and cross-stakeholder collaboration remain relatively scarce in the literature, with Chhetri et al. [37] providing a rare example of such cross-disciplinary collaboration.

The findings also highlight the importance of public trust and societal acceptance. In particular, the deployment of surveillance and AI-based systems in public spaces requires stronger transparency, oversight, and citizen involvement. Mechanisms such as citizen panels, public consultations, and participatory digital platforms can support alignment between technological solutions and community needs, thereby enhancing legitimacy and accountability [34].

Another important implication relates to scalability and interoperability. The prevalence of highly localised solutions contributes to fragmentation and limits reuse across cities. The results suggest that improving the scalability and interoperability of existing frameworks, rather than continuously developing new isolated solutions, may better support long-term sustainability. At the same time, such approaches must remain adaptable to local contexts. The FIWARE-based identity management integration [27] illustrates how standards-aligned architectures can support reuse while allowing contextual adaptation.

Finally, the findings underline the importance of strengthened multi-stakeholder and cross-regional collaboration. Cooperation between industry, academia, public authorities, and regulators can facilitate knowledge exchange on regulatory compliance and trustworthy AI development. Clear definition of roles and responsibilities, combined with effective cross-border collaboration, is therefore essential for improving governance, accountability, and cybersecurity resilience in smart city ecosystems. Overall, these implications highlight the need for more integrated, collaborative, and scalable approaches that bridge technical design, regulatory requirements, and societal considerations.

6. Related Work

This section reviews existing surveys and literature reviews at the intersection of smart cities, privacy and security, and EU regulations. While prior work has examined security threats, enabling technologies, and privacy challenges in smart city environments, most reviews focus on technical solutions or on individual regulations, particularly the GDPR. Consequently, there is limited analysis of how cybersecurity solutions are shaped by the broader and evolving EU regulatory landscape, or how legal requirements are translated into concrete technical, organisational, and operational measures. This section positions our work in relation to prior reviews and highlights its distinct contribution.

Three papers [6,49,50] give an overview of existing security and technological solutions for smart cities, explore threats and vulnerabilities in several smart city domains (i.e., smart mobility, smart healthcare, smart economy, etc.), and give recommendations for improving the security of smart urban environments. For instance, while Ali et al. [49] explore security strategies for AI-assisted smart cities, and assess the role of federated learning in helping to comply with GDPR for data exchanges, Selwe et al. [50] review several proposals for the integration of GDPR into smart city technologies, such as the protection of personal data via access control mechanisms, the use of user location data for authentication and data management, or exploiting the security attributes of systems to achieve GDPR compliance. However, none of these reviews explain how GDPR compliance can be achieved. The study by Ismagilova et al. [6] is a systematic review with a fully-reported formal methodology. Different from our scope, their work covers the prior period of 2010–2019. Their study addresses operational and technological challenges, and various technological solutions (i.e., encryption, authentication protocols, privacy-preserving frameworks, among others). Unlike our review, the authors acknowledge this limitation of the lack of coverage of EU regulations, noting that their focus is solely on technological solutions and suggesting future research on how legal systems can address trust challenges within smart cities. The majority of related works offer very limited discussion on EU regulations, addressing only the GDPR in a smart city context.

In contrast, papers [51–53] have a more narrow focus on enabling technologies in smart cities. Wang et al. [51] review the challenges of crowdsensing in smart cities, categorising sensing entities into human-oriented, vehicle-oriented, and infrastructure-oriented sensing, as well as introducing the various crowdsensing applications and approaches. Collecting data is an integral part of crowdsensing, and GDPR is introduced as one of the regulations applied in that field. Although the authors reference GDPR-compliant projects, they provide no analysis of compliance mechanisms, enforcement challenges, or implementation details—mentioning the regulation in passing rather than actively analysing it. In contrast, the review by Asghar et al. [52] explores the GDPR in the context of video surveillance by giving an overview of the articles within the first four chapters of the GDPR relevant for the CCTV surveillance industry and reviewing existing smart city surveillance solutions, some of which are GDPR-compliant. It reviews GDPR-compliant video redaction techniques in terms of anonymisation (irreversible) and pseudonymisation (reversible), as well as existing market-based data protection-by-design solutions. Lane [53] takes a different approach in which the author bridges the discourse on smart cities, AI, and human rights by critically analysing the AIA from the perspective of preventive corporate responsibility that applies to private AI businesses. The review categorises long-term risks to human rights in a smart city context, and discusses the role of private AI developers, the unpredictability of AI technologies, and unforeseen uses of high-risk AI systems.

On the other hand, the reviews in [54,55] provide an overview of the cybersecurity challenges facing smart cities and the mitigation strategies to address them. Abdulghani et al. [54] propose a framework that links security and privacy guidelines, attacks, stake-

holders, and mitigation techniques for IoT data at rest. The authors discuss GDPR in relation to several of their guidelines, such as minimisation of data storage, data retention, post-informing customers, and proper data destruction. Oliha et al. [55] explain how the heavy reliance on IoT devices, interconnected systems, and large-scale data flows creates significant risks, and highlight key mitigation measures such as encryption, access control, and multi-factor authentication. The paper discusses real-world examples and emphasises the importance of collaboration among governments, industry, and citizens to build secure and resilient smart urban environments. GDPR is only mentioned in passing as an example of a data protection and privacy regulation for smart city systems.

In contrast to previous works, this review is based on an updated corpus of publications from 2018 to 2025 and follows a formal (structured and reproducible) methodology. We take a more general smart city approach and present the state of the art of cybersecurity measures in smart cities, contextualised by the emerging EU regulatory framework. By filling the research gaps, our work addresses several EU regulations on cybersecurity and data protection in a smart city context, combined with technological, organisational, and operational measures, including existing smart city solutions compliant with EU regulations.

7. Conclusions

As cities become increasingly digitalised, their exposure to cybersecurity risks grows accordingly. Smart city viability is dependent on the ability to preserve citizen data privacy and ensure that digital services are implemented securely. However, given that smart cities are still in the early stages of deployment, building them on a foundation of privacy and security as prerequisites for trust is imperative for their sustainability. This comprehensive review has discussed the state-of-the-art research of 21 scientific publications with the goal of analysing cybersecurity solutions for smart cities that address EU regulatory requirements. We scrutinised the publications in terms of application domains, stakeholder groups, cybersecurity and data protection measures (technical, organisational, and operational), smart city solutions (validated implementations compliant with regulations), and EU regulations. This review has also identified trends and gaps, challenges and risks, legal perspectives (in terms of ambiguity, overlapping oversight, and gaps), and lastly, key recommendations. Finally, our work has also generated valuable insights that encourage further reflection. In one sense, the results from this work highlight the importance of the interplay between cybersecurity laws in the EU and technical smart city deployments, as well as contribute to a better understanding of various aspects crucial to be considered, such as legal, technical, social, and ethical. Practitioners and researchers could benefit from the results presented here as a basis to start from. There is no doubt that the near future research needs to focus on the multidisciplinary aspect in the conduct of the work for effective implementation of smart city applications that also reach successful legal compliance.

Author Contributions: Conceptualisation, all; methodology, M.P., M.G.V., M.G., and L.I.; formal analysis, all; writing—original draft preparation, all; writing—review and editing, M.P., M.G.V., M.G., and L.I.; editing, M.P., M.G.V., M.G., and L.I.; visualisation, M.P., M.G.V., M.G., and L.I.; supervision, M.P., L.I., and L.S.; project administration, M.P. and L.I.; funding acquisition, L.I. All authors have read and agreed to the published version of the manuscript.

Funding: This study was co-funded by the Innovations and Technology (InnoTech) Task Force project under the Interreg Öresund–Kattegat–Skagerrak (Interreg ØKS) programme, project NYPSID (No. 20358659).

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: During the preparation of this manuscript, the authors used ChatGPT (OpenAI, GPT-4 model, December 2025 version) for the purposes of language editing, including grammar correction, spelling, and improvement of text clarity and structure. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

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

Abbreviations

The following abbreviations are used in this manuscript:

ABAC	Attribute-Based Access Control
ACS	Automated City Shuttles
AES	Advanced Encryption Standard
AES-OFB	Advanced Encryption Standard-Output Feedback Mode
AFR	Automated Facial Recognition
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
API	Application Programming Interface
ASFA	Attack-Situation-Focused Analysis Framework
CCTV	Closed-Circuit Television
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CCSP	Critical Cloud Service Provider
CSP	Cloud Service Provider
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
DORA	Digital Operational Resilience Act
DPbD	Data Protection by Design
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECCF	European Cybersecurity Certification Framework
eIDAS	electronic Identification, Authentication and Trust Services
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUDI	European Union Digital Identity
FIWARE	Future Internet Ware Security Framework
FOI	Features-of-Interest
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
ICT	Information and Communication Technology
IoT	Internet of Things
ISO	International Organisation for Standardisation
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
LED	Law Enforcement Directive
NIS 2	Network and Information Security Directive 2
oAuth	Open Authorization protocol
PKG	Private Key Generator
RBAC	Role-Based Access Control
RSA	Rivest-Shamir-Adleman algorithm
SAML	Security Assertion Markup Language
SPID	Italy's Public Digital Identity System
SSL	Secure Sockets Layer

TLPT	Threat Led Penetration Testing
TLS	Transport Layer Security
TOMs	Technical and Organisational Measures

References

- Spensky, C.; Stewart, J.; Yerukhimovich, A.; Shay, R.; Trachtenberg, A.; Housley, R.; Cunningham, R.K. Sok: Privacy on mobile devices—it's complicated. *Proc. Priv. Enhancing Technol.* **2016**, 2016, 96–116. [CrossRef]
- European Parliament and Council of the European Union. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Off. J. Eur. Union* **2022**, L 333, 80–156.
- European Parliament and Council of the European Union. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending certain Union legislative acts (Cyber Resilience Act). *Off. J. Eur. Union* **2024**, L 2847. Available online: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> (accessed on 23 March 2026).
- European Parliament and Council of the European Union. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act). *Off. J. Eur. Union* **2022**, L 333, 1–142.
- European Parliament and Council of the European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act). *Off. J. Eur. Union* **2024**, L 1689. Available online: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (accessed on 23 March 2026).
- 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.* **2022**, 24, 393–414. [CrossRef]
- Serrano, M.; Griffor, E.; Wollman, D.A.; Dunaway, M.; Burns, M.; Rhee, S.; Greer, C. *Smart Cities and Communities: A Key Performance Indicators Framework*; NIST Special Publication 1900-206; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2022. [CrossRef]
- Buccafurri, F.; Labrini, C.; Musarella, L. Smart-contract based Access Control on Distributed Information in a Smart-City scenario. In *Proceedings of the 3rd Distributed Ledger Technology Workshop (DLT 2020)*; Chiaraluce, F., Mostarda, L., Eds.; CEUR-WS.org: Aachen, Germany, 2020; Volume 2580.
- Hacker, P.; Neyer, J. Substantively smart cities: Participation, fundamental rights and temporality. *Internet Policy Rev.* **2023**, 12, 1–30. [CrossRef]
- Singh, P.; Sweksha, M. Role of Right to Privacy in Criminal Justice System. *Int. J. Multidiscip. Res.* **2024**, 6, 22378. [CrossRef]
- Hulok, M. The EU model of AI governance: Regulating artificial intelligence through law and policy. *ERA Forum* **2025**, 26, 527–547. [CrossRef]
- European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* **2016**, L 119, 1–88.
- Laux, J.; Wachter, S.; Mittelstadt, B. Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk. *Regul. Gov.* **2024**, 18, 3–32. [CrossRef] [PubMed]
- European Parliament and Council of the European Union. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Off. J. Eur. Union* **2022**, L 277, 1–163.
- European Parliament and Council of the European Union. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). *Off. J. Eur. Union* **2022**, L 265, 1–66.
- European Parliament and Council of the European Union. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). *Off. J. Eur. Union* **2022**, L 152, 1–44.

17. European Parliament and Council of the European Union. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive). *Off. J. Eur. Union* **2016**, L 119, 89–131.
18. European Parliament and Council of the European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Off. J. Eur. Union* **2016**, L 194, 1–30.
19. European Parliament and Council of the European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Off. J. Eur. Union* **2019**, L 151, 1–94.
20. European Parliament and Council of the European Union. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Off. J. Eur. Union* **2014**, L 257, 73–200.
21. European Parliament and Council of the European Union. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. *Off. J. Eur. Union* **2024**, L 1183. Available online: <https://eur-lex.europa.eu/eli/reg/2024/1183/oj> (accessed on 23 March 2026).
22. Webster, J.; Watson, R.T. Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.* **2002**, 26, xiii–xxiii. [[CrossRef](#)]
23. Kitchenham, B.; Brereton, P. A systematic review of systematic review process research in software engineering. *Inf. Softw. Technol.* **2013**, 55, 2049–2075. [[CrossRef](#)]
24. El Majdoubi, D.; El Bakkali, H.; Sadki, S. Towards smart blockchain-based system for privacy and security in a smart city environment. In *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*; IEEE: New York, NY, USA, 2020; pp. 1–7.
25. Christofi, A.; Verdoodt, V.; Bertels, N.; Ziegler, S.; Quesada Rodriguez, A.; Radócz, R. IoT and Data Protection. In *Springer Handbook of Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 341–383.
26. Kindt, E. Having yes, using no? About the new legal regime for biometric data. *Comput. Law Secur. Rev.* **2018**, 34, 523–538. [[CrossRef](#)]
27. Alonso, Á.; Pozo, A.; Choque, J.; Bueno, G.; Salvachúa, J.; Diez, L.; Marín, J.; Alonso, P.L.C. An Identity Framework for Providing Access to FIWARE OAuth 2.0-Based Services According to the eIDAS European Regulation. *IEEE Access* **2019**, 7, 88435–88449. [[CrossRef](#)]
28. George, D.; Reutimann, K.; Tamò-Larrieux, A. GDPR bypass by design? Transient processing of data under the GDPR. *Int. Data Priv. Law* **2019**, 9, 285–298. [[CrossRef](#)]
29. Buccafurri, F.; De Angelis, V.; Lax, G.; Musarella, L.; Russo, A. An Attribute-Based Privacy-Preserving Ethereum Solution for Service Delivery with Accountability Requirements. In *Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES '19, Canterbury, UK, 26–29 August 2019*. [[CrossRef](#)]
30. Buccafurri, F.; Lax, G.; Musarella, L.; Russo, A. Ethereum Transactions and Smart Contracts among Secure Identities. In *Proceedings of the Second Distributed Ledger Technology Workshop (DLT 2019)*; Mori, P., Bartoletti, M., Bistarelli, S., Eds.; CEUR-WS.org: Aachen, Germany, 2020; Volume 2334.
31. Badii, C.; Bellini, P.; Difino, A.; Nesi, P. Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. *IEEE Access* **2020**, 8, 23601–23623. [[CrossRef](#)]
32. Rezende, I.N. Facial recognition in police hands: Assessing the ‘Clearview case’ from a European perspective. *New J. Eur. Crim. Law* **2020**, 11, 375–389. [[CrossRef](#)]
33. Asghar, M.N.; Ansari, M.S.; Kanwal, N.; Lee, B.; Herbst, M.; Qiao, Y. Deep Learning based Effective Identification of EU-GDPR Compliant Privacy Safeguards in Surveillance Videos. In *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDDCom/CyberSciTech)*; IEEE: New York, NY, USA, 2021; pp. 819–824. [[CrossRef](#)]
34. Schwemer, S.F.; Tomada, L.; Pasini, T. Legal AI Systems in the EU’s proposed Artificial Intelligence Act. In *Proceedings of the Joint Proceedings of the Workshops on Automated Semantic Analysis of Information in Legal Text (ASAIL 2021) & AI and Intelligent Assistance for Legal Professionals in the Digital Workplace (LegalAIIA 2021)*; Conrad, J.G., Pickens, J., Baron, J.R., Henseler, H., Linna, D.W., Jr., Vinjumur, J.K., Eds.; CEUR-WS.org: Aachen, Germany, 2021; Volume 2888, pp. 51–58.
35. Veale, M.; Borgesius, F.Z. Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Comput. Law Rev. Int.* **2021**, 22, 97–112. [[CrossRef](#)]

36. Benyahya, M.; Kechagia, S.; Collen, A.; Nijdam, N.A. The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis. *Appl. Sci.* **2022**, *12*, 4413. [\[CrossRef\]](#)
37. Chhetri, T.R.; Kurteva, A.; DeLong, R.J.; Hilscher, R.; Korte, K.; Fensel, A. Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. *Sensors* **2022**, *22*, 2763. [\[CrossRef\]](#) [\[PubMed\]](#)
38. Neroni Rezende, I. Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces. In *Investigating and Preventing Crime in the Digital Era: New Safeguards, New Rights*; Bachmaier Winter, L., Ruggeri, S., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 67–98. [\[CrossRef\]](#)
39. Stach, C.; Gritti, C.; Przytarski, D.; Mitschang, B. Can blockchains and data privacy laws be reconciled? a fundamental study of how privacy-aware blockchains are feasible. In Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, SAC '22, Virtual Event, 25–29 April 2022; pp. 1218–1227. [\[CrossRef\]](#)
40. Tauqeer, A.; Kurteva, A.; Chhetri, T.R.; Ahmeti, A.; Fensel, A. Automated GDPR Contract Compliance Verification Using Knowledge Graphs. *Information* **2022**, *13*, 447. [\[CrossRef\]](#)
41. Anedda, M.; Fadda, M.; Girau, R.; Pau, G.; Giusto, D. A social smart city for public and private mobility: A real case study. *Comput. Netw.* **2023**, *220*, 109464. [\[CrossRef\]](#)
42. Eckhardt, P.; Kotovskaia, A. The EU's cybersecurity framework: The interplay between the Cyber Resilience Act and the NIS 2 Directive. *Int. Cybersecur. Law Rev.* **2023**, *4*, 147–164. [\[CrossRef\]](#)
43. Fabregue, B. Artificial intelligence governance in smart cities: A European regulatory perspective. *J. Auton. Intell.* **2023**, *7*, 1–17. [\[CrossRef\]](#)
44. Kun, E. Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. *Comput. Law Secur. Rev.* **2024**, *52*, 105931. [\[CrossRef\]](#)
45. Seid, E.; Blix, F.; Popov, O. Cyber Resilience Using ASFA: DORA-Compliant Threat-Led Penetration Testing. In *Critical Information Infrastructures Security*; Oliva, G., Panzieri, S., Hämmerli, B., Pascucci, F., Faramondi, L., Eds.; Springer: Cham, Switzerland, 2025; pp. 269–288.
46. Bradley, E.H.; Curry, L.A.; Devers, K.J. Qualitative data analysis for health services research: Developing taxonomy, themes, and theory. *Health Serv. Res.* **2007**, *42*, 1758–1772. [\[CrossRef\]](#)
47. Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Inf. Softw. Technol.* **2015**, *64*, 1–18. [\[CrossRef\]](#)
48. Bennett Moses, L.; Zalnieriute, M. Law and Technology in the Dimension of Time. In *Time, Law and Change: An Interdisciplinary Study*; UNSW Law Research Paper; Hart Publishing: Oxford, UK, 2020.
49. Ali, J.; Kumar Singh, S.; Jiang, W.; Alenezi, A.M.; Islam, M.; Ibrahim Daradkeh, Y.; Mehmood, A. A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks. *Comput. Commun.* **2025**, *229*, 108000. [\[CrossRef\]](#)
50. Selwe, K.; Hofisi, C. Exploring the Role of Innovative Technologies in Smart Cities. *J. Educ. Learn. Technol. (JELT)* **2024**, *5*, 568–582. [\[CrossRef\]](#)
51. Wang, Z.; Cao, Y.; Jiang, K.; Zhou, H.; Kang, J.; Zhuang, Y.; Tian, D.; Leung, V.C.M. When Crowdsensing Meets Smart Cities: A Comprehensive Survey and New Perspectives. *IEEE Commun. Surv. Tutor.* **2025**, *27*, 1101–1151. [\[CrossRef\]](#)
52. Asghar, M.N.; Kanwal, N.; Lee, B.; Fleury, M.; Herbst, M.; Qiao, Y. Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective. *IEEE Access* **2019**, *7*, 111709–111726. [\[CrossRef\]](#)
53. Lane, L. Preventing long-term risks to human rights in smart cities: A critical review of responsibilities for private AI developers. *Internet Policy Rev.* **2023**, *12*, 1–14. [\[CrossRef\]](#)
54. Abdulghani, H.A.; Nijdam, N.A.; Collen, A.; Konstantas, D. A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. *Symmetry* **2019**, *11*, 774. [\[CrossRef\]](#)
55. Oliha, J.S.; Biu, P.W.; Obi, O.C. Securing the smart city: A review of cybersecurity challenges and strategies. *Eng. Sci. Technol. J.* **2024**, *5*, 496–506. [\[CrossRef\]](#)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.