SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

The Transformation of Privacy in the Algorithmic Age: A Legal, Technical, and Social Analysis in Light of the KVKK and the GDPR

Ayşe Güngör[1], Filiz Kutluay Tutar[2], Abdallah Abukalloub[3*]

[1]Department of Logistics Management, Kadir Karabaş School of Applied Sciences, Giresun University, Türkiye
[2]Department of Economics, Faculty of Economics and Administrative Sciences, Nigde Omer Halisdemir University, Türkiye
[3]Department of Economics, Institute of Social Sciences, Nigde Omer Halisdemir University, Türkiye

Author Email: ayse.gungor@giresun.edu.tr[1], flztutar51@gmail.com[2], abdkalloub@gmail.com[3]

ORCID: 0009-0006-3916-9657[1], ORCID: 0000-0002-2574-9494[2], ORCID: 0009-0000-1697-5206[3]

Abstract. The rapid expansion of big data, Internet of Things (IoT) systems, and artificial intelligence (AI) has transformed the conditions under which privacy and personal data protection operate. In the algorithmic age, privacy is increasingly challenged not only as an individual right but also as a structural condition of socio-technical systems. This article examines whether privacy is merely adapting to technological change or undergoing a deeper paradigmatic transformation. Focusing on Türkiye's Personal Data Protection Law (KVKK No. 6698) in comparison with the European Union's General Data Protection Regulation (GDPR), the study investigates the changing legal and operational foundations of personal data protection, particularly the declining centrality of explicit consent and the growing role of broader governance mechanisms. Methodologically, the article adopts a qualitative multi-method design combining comparative legal analysis, doctrinal examination, and a socio-technical case study of six smart city applications in Türkiye. The findings reveal a gap between formal regulatory alignment and substantively effective protection, especially in smart city systems characterized by ambient data collection, system interoperability, and limited user contestability. The study concludes that privacy is being restructured from an individual consent-based model toward a more systemic governance condition. Accordingly, sustainable privacy protection requires integrated legal, technical, and societal governance mechanisms.

Keywords: Privacy Transformation, Personal Data Protection, Algorithmic Governance, Smart Cities, Data Justice

1 Introduction

In the algorithmic age, whether privacy will persist, undergo transformation, or gradually erode has become one of the fundamental questions of contemporary governance. The rapid proliferation of the Internet of Things (IoT), big data analytics, and artificial intelligence (AI) technologies has fundamentally transformed the scale, speed, and transparency of personal data processing. These developments place significant pressure on the conceptual and institutional foundations of privacy and data protection law, particularly in environments where digital infrastructures permeate nearly every aspect of everyday life.

At the global level, the most prominent regulatory response has been the European Union's General Data Protection Regulation (GDPR), which seeks to re-establish normative oversight over data-driven systems. Due to its extraterritorial impact, the GDPR has become a transnational reference standard and has influenced legal reform processes in numerous countries. Türkiye's Personal Data Protection Law No. 6698 (KVKK), which entered into force in 2016, can be seen as a reflection of this regulatory diffusion, although it also incorporates distinctive constitutional and institutional characteristics. Nevertheless, achieving formal compliance with international standards does not necessarily guarantee the existence of substantively effective protection in practice.

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

This study examines whether privacy continues to exist in the digital era merely by adapting to technological transformations or whether it is undergoing a deeper paradigmatic restructuring. In this context, the study seeks to address the following questions:

a. How is the regulatory architecture governing personal data protection evolving in the algorithmic age?
b. To what extent does the weakening of the central role of explicit consent reshape the normative foundations of privacy?
c. How are legal principles operationalized within smart city infrastructures in Türkiye?
d. Do existing governance mechanisms adequately mitigate the socio-technical risks produced by data-intensive urban systems?

Smart cities provide a particularly revealing empirical domain for examining these questions. These systems integrate IoT infrastructures, algorithmic data processing mechanisms, and large-scale data integration practices within essential public services such as transportation, public administration, and environmental monitoring. Within such ecosystems, personal data are frequently collected, processed, and subjected to inferential analytics on a continuous basis, often without the meaningful awareness of data subjects. Consequently, privacy risks emerge not as incidental outcomes but as structural characteristics of these systems.

This article adopts a comprehensive analytical framework that combines comparative legal analysis, doctrinal examination, and qualitative case study methods. The study situates Türkiye's Personal Data Protection Law (KVKK) within the broader evolution of global data protection paradigms and evaluates how regulatory norms interact with technological architectures and social practices within Türkiye's smart city ecosystem. By bringing together legal theory and socio-technical practice, this approach aims to contribute to contemporary debates on data justice, algorithmic governance, and the sustainability of privacy in digital societies.

Beyond comparing legal frameworks, the study contributes to contemporary privacy theory by arguing that privacy in the algorithmic age can no longer be adequately understood through an individualist, consent-centered model alone. Instead, it advances a systemic interpretation of privacy in which meaningful legal protection depends on the interaction between regulatory norms, technical architectures, and institutional governance practices. In this perspective, privacy is conceptualized not merely as an individual right to authorize data processing, but as a structural condition of fairness, visibility, accountability, and contestability within data-driven socio-technical systems.

Although the empirical focus of this study is Türkiye, the case is not treated as merely context-specific. Rather, Türkiye provides a theoretically relevant site for examining privacy governance in digitally transforming urban environments because it combines formal regulatory alignment with the GDPR, rapid smart city expansion, and uneven institutional and infrastructural implementation capacities. In this sense, the Turkish case offers broader analytical value for understanding how privacy protection operates in jurisdictions that are formally aligned with global regulatory norms but face socio-technical governance challenges in practice.

2 Theoretical and Analytical Evaluation of the Literature on Personal Data Protection

Privacy is widely recognized as a fundamental right embedded in constitutional orders and international human rights regimes. In contemporary scholarship, privacy is conceptualized not only as a sphere of individual autonomy but also as a structural safeguard against arbitrary exercises of power by both states and corporations [1]. Within the fields of information technology law and cyber regulation, debates on privacy are primarily framed through the concept of personal data protection, focusing on the normative foundations, scope, and governance mechanisms of data processing.

However, the emergence of digital surveillance technologies and algorithmic governance has expanded the scope of privacy debates. In particular, the increasing role of artificial intelligence (AI) has intensified scholarly attention to issues such as data security, automated decision-making, and informational self-determination. In this context, the literature can broadly be categorized into three strands:

a. Legal approaches to personal data protection,
b. Socio-political analyses of digital privacy and surveillance, and
c. Technical and socio-technical studies focusing on data security, artificial intelligence, and privacy-enhancing technologies.

A critical review of these aspects shows that, especially in the Turkish context, research on the dynamics of smart cities remains scarce. Although smart cities are environments where legal, technological, and social factors come together within complex data ecosystems, current studies often focus on isolated applications like transportation systems, biometric surveillance, or digital governance platforms rather than examining these systems as integrated data infrastructures [2]. This fragmented view makes it hard to identify cumulative risks, systemic vulnerabilities, and regulatory gaps.

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

Accordingly, this study conceptualizes smart cities as interconnected socio-technical ecosystems and examines how legal frameworks, technological infrastructures, and societal risks interact in shaping digital privacy governance.

2.1 Legal Approaches to Personal Data Protection

The global spread of data protection legislation reflects an emerging normative convergence aimed at balancing the legitimate use of personal data with the protection of fundamental rights. Türkiye's Personal Data Protection Law No. 6698 (KVKK), which entered into force in 2016, represents one example of this trend. The KVKK is frequently compared with the European Union's General Data Protection Regulation (GDPR), and comparative analyses highlight both similarities and differences, particularly regarding enforcement mechanisms, data subject rights, and cross-border data transfer rules [3] [4] [5].

Through administrative practice and judicial interpretation, the KVKK has gradually evolved within the framework of Turkish administrative law [6]. Recent regulatory discussions concerning cross-border data transfers illustrate the tension between data sovereignty and the facilitation of international data flows [7].

From a doctrinal perspective, privacy is widely recognized as a fundamental right, while data protection law functions as a balancing mechanism between individual rights and legitimate public or commercial interests [1] [8]. Although explicit consent has traditionally been considered a central legal basis for data processing, contemporary scholarship increasingly highlights the structural limitations of consent-based models, particularly in contexts characterized by power and information asymmetries. As a result, recent debates advocate a contextual evaluation of alternative legal bases for data processing while preserving the core essence of the right to privacy.

2.2 Digital Privacy, Surveillance Society, and Social Implications

The expansion of digital technologies has contributed to the emergence of what is often described as a "surveillance society," characterized by pervasive data collection, algorithmic monitoring, and the normalization of visibility [9]. Surveillance practices are frequently justified through narratives of national security, counter-terrorism, and crime prevention [10]. Technologies such as CCTV systems, facial recognition tools, and drone-based monitoring have therefore generated significant debates regarding proportionality, legality, and democratic accountability [11].

Despite official claims that surveillance technologies enhance public security, empirical evidence regarding their effectiveness remains contested. Critical scholarship suggests that expanding surveillance infrastructures may normalize exceptional governance practices rather than substantially improving security outcomes [12] [13]. At the same time, the politicization of digital infrastructures and cybersecurity debates demonstrates that privacy discussions are increasingly intertwined with geopolitical and ideological dynamics [14] [15].

In parallel, scholarly attention has increasingly focused on AI-driven systems and data security. Technologies such as predictive analytics and algorithmic profiling raise concerns regarding transparency, accountability, and the "black-box" nature of automated decision-making [16]. While Privacy-Enhancing Technologies (PETs) offer potential mechanisms for risk mitigation, their uneven implementation across digital infrastructures highlights the persistent gap between regulatory aspirations and practical application.

2.3 Data Security, Artificial Intelligence, and Privacy-Enhancing Technologies

Legal and technical scholarship increasingly emphasizes the interdependence between data security and privacy. While security mechanisms aim to prevent unauthorized access and data breaches, privacy frameworks regulate the legitimacy and proportionality of data processing. These dimensions intersect particularly within artificial intelligence systems, where risks may arise throughout the entire data lifecycle—from collection to model deployment [17].

The principle of privacy by design has emerged as a central normative and technical approach advocating the integration of privacy considerations into system architecture from the earliest stages of development. Nevertheless, empirical research suggests that implementation frequently remains limited due to regulatory uncertainty, institutional capacity constraints, and commercial priorities [18].

Sector-specific studies focusing on healthcare systems and IoT ecosystems highlight the increasing sensitivity of personal data within interconnected infrastructures [19]. Although technological solutions such as blockchain architectures and secure communication protocols aim to strengthen privacy protection [20], technical measures alone cannot fully address challenges related to algorithmic bias, transparency, and accountability. These concerns have strengthened calls for broader data justice frameworks capable of addressing structural inequalities embedded in digital infrastructures [21].

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

2.4 Gaps in the Literature and the Positioning of This Study

The existing literature on privacy and personal data protection reveals a persistent fragmentation across legal, socio-political, and technical lines of inquiry. A structured reading of the literature indicates that existing scholarship tends to cluster around three partially disconnected strands. First, legal and doctrinal studies primarily focus on regulatory principles, lawful bases for processing, consent, compliance mechanisms, and comparative legal frameworks such as the GDPR and the KVKK. Second, socio-political studies emphasize digital surveillance, visibility, algorithmic governance, and the implications of data-driven systems for autonomy, rights, and power. Third, technical and socio-technical studies concentrate on privacy-enhancing technologies, cybersecurity, IoT infrastructures, AI risks, and system design. While each strand provides important insights, they rarely converge within a single analytical framework.

This fragmentation is particularly visible in the context of smart cities. Studies on digital surveillance provide valuable critiques of monitoring practices, but often do not examine how these practices are embedded within the operational architecture of urban digital infrastructures. Similarly, research on artificial intelligence, IoT security, and data protection technologies frequently addresses privacy as a technical or engineering challenge, without sufficiently engaging with its legal and normative dimensions. Conversely, legal scholarship often remains focused on doctrinal interpretation and regulatory alignment, without systematically analysing how legal norms operate within data-intensive socio-technical systems.

In the Turkish context, this fragmentation is even more pronounced. Existing studies provide important analyses of the KVKK and its doctrinal structure, while separate strands of scholarship discuss smart city implementation, municipal digitalization, or specific technological applications. However, a comprehensive and integrated analysis of how legal frameworks, surveillance infrastructures, algorithmic systems, and technical safeguards interact within Turkish smart city ecosystems remains largely absent. This is particularly significant given the rapid expansion of urban digital infrastructures and the increasing use of data-intensive systems in public administration and service delivery.

This study addresses that gap by conceptualizing smart cities as interconnected data ecosystems and examining personal data protection through a holistic analytical framework that integrates legal, socio-political, and technical dimensions. By doing so, the study aims to identify systemic risks, regulatory inconsistencies, and governance challenges that may remain invisible when these dimensions are analysed in isolation.

In addition, this study treats the transformation of privacy not merely as a rhetorical description of digital change, but as an analytically distinguishable shift in the normative and operational conditions of personal data protection. For analytical purposes, three possible states are identified. First, privacy persistence refers to situations in which fundamental data protection principles—such as lawfulness, purpose limitation, data minimization, transparency, and the meaningful exercise of data subject rights—remain functionally effective despite technological change. Second, privacy transformation refers to cases in which privacy is not eliminated but reconfigured: protection shifts from an individual-control model centered on explicit consent toward a broader governance model based on accountability, risk assessment, privacy by design, and institutional oversight. Third, privacy erosion refers to conditions in which legal protections continue to exist formally but lose substantive effectiveness due to opaque data flows, ambient data collection, secondary use, weak contestability, and structural asymmetries of power and information. This distinction provides the conceptual basis for evaluating whether smart city data practices in Türkiye reflect continuity, restructuring, or weakening in privacy protection.

The theoretical contribution of this study lies in extending contemporary privacy debates beyond the conventional consent-based paradigm. While existing legal frameworks such as the GDPR and the KVKK continue to rely, at least partially, on the logic of individual authorization, this study argues that such an approach is increasingly insufficient in data-intensive environments characterized by ambient collection, inferential analytics, and infrastructural integration. In these settings, privacy risks are not produced solely by discrete acts of unlawful data processing but by the structural organization of socio-technical systems. Accordingly, the study advances a systemic interpretation of privacy in which meaningful protection depends not only on consent or individual control, but also on institutional accountability, architectural design, and the equitable governance of data relations. In doing so, the article positions privacy as a structural and governance-based condition rather than merely a transactional legal entitlement.

3 Methodology

This study adopts a qualitative multi-method research design integrating comparative legal analysis, doctrinal examination, and a socio-technical case study. The aim is to evaluate both the normative framework of personal data protection and its practical implementation within smart city infrastructures in Türkiye.

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

To operationalize the concept of privacy transformation, the study evaluates each regulatory and empirical domain through three analytical criteria: (i) the continued effectiveness of core legal safeguards, including lawfulness, purpose limitation, data minimization, transparency, and the meaningful exercisability of data subject rights; (ii) the extent to which privacy protection is reconfigured from an individual consent-based model toward systemic governance mechanisms such as accountability, risk-based regulation, privacy by design, and institutional oversight; and (iii) the degree to which data subjects experience a loss of visibility, control, and contestability over personal data processing.

These criteria are assessed through observable indicators within both legal texts and smart city applications, including the presence and quality of consent mechanisms, the transparency of data flows, the availability of user control and opt-out options, the clarity and limitation of processing purposes, the existence of secondary data use, and the presence of oversight, accountability, and redress mechanisms. Accordingly, privacy is considered persistent where legal guarantees remain substantively functional and observable in practice; transformed where protection continues but through altered institutional and technical mechanisms; and eroded where formal safeguards exist without meaningful practical effectiveness due to structural opacity, asymmetries of power, or limitations in user agency. This operationalization provides the basis for comparing formal legal provisions with their practical manifestation in socio-technical systems.

The methodological strategy consists of three complementary stages:

a. Comparative legal analysis of the KVKK and the GDPR,
b. Doctrinal assessment of the regulatory structure of the KVKK, and
c. Qualitative analysis of personal data processing practices in selected smart city applications.

These methods are applied in a sequential and integrated manner. First, the comparative legal analysis establishes the broader regulatory framework by identifying convergences and divergences between the KVKK and the GDPR, particularly in relation to lawful bases for processing, data subject rights, accountability, and governance mechanisms. Second, the doctrinal examination focuses more closely on the internal legal logic of the KVKK, clarifying how its principles, exceptions, and regulatory structure shape the normative conditions of personal data protection in Türkiye. Third, the qualitative case study translates these normative insights into the empirical domain by examining how smart city applications operationalize, mediate, or undermine these legal principles in practice. In this way, the research design moves from the normative level to the institutional-legal level and finally to the socio-technical implementation level, allowing the study to address both the formal and practical dimensions of privacy governance.

This sequencing also aligns with the research questions: the first two questions are primarily addressed through comparative legal and doctrinal analysis, while the latter two are examined through the socio-technical case study of smart city infrastructures.

The analytical framework integrates three interdependent dimensions: the legal, technical, and social dimensions. The legal dimension evaluates whether data processing practices are compatible with applicable legal norms, including lawful basis, proportionality, purpose limitation, and data subject rights under the KVKK and the GDPR. The technical dimension examines how personal data are collected, processed, stored, transferred, and potentially combined across digital infrastructures, with particular attention to ambient data collection, interoperability, and automated processing. The social dimension assesses how these legal and technical arrangements affect autonomy, visibility, accountability, contestability, and broader concerns of fairness and data justice.

These dimensions are not treated as separate or parallel layers of analysis, but as mutually constitutive components of a single socio-technical governance framework. In this framework, legal norms are assessed not only as formal rules but as principles whose effectiveness depends on technological architectures and institutional practices; similarly, technical infrastructures are analysed not merely as neutral tools but as systems that shape legal compliance and social outcomes. The social dimension, in turn, captures how these interactions produce differential implications for individuals and communities. This integrated approach enables the study to move beyond parallel disciplinary discussion and instead examine how privacy is structured, mediated, and contested across legal, technical, and societal domains.

Within this framework, algorithmic governance and data justice are employed as explicit analytical lenses rather than merely descriptive references. Algorithmic governance is used to examine how smart city infrastructures increasingly rely on automated, data-driven, and inferential mechanisms to shape administrative practices, public services, and forms of urban oversight. Data justice, in turn, is used to evaluate the distributive and relational implications of these systems, particularly with regard to visibility, asymmetries of power, contestability, and unequal exposure to surveillance or data-related harms. Concepts such as privacy by design and privacy by default serve as bridging analytical principles across these dimensions, allowing the study to assess whether regulatory norms are meaningfully embedded into technological systems and governance arrangements.

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

The comparative legal analysis examines the scope of regulation, legal bases for data processing, data subject rights, obligations of controllers and processors, supervisory mechanisms, and cross-border data transfer rules under the KVKK and the GDPR. Primary sources include statutory provisions, regulatory decisions, official guidance documents, and relevant academic literature.

The empirical phase focuses on six widely used smart city applications in Türkiye. Case selection is based on prevalence of use, integration with public services, and the intensity and sensitivity of personal data processing. Türkiye is selected not only for contextual relevance, but also as a strategic analytical case for examining the relationship between formal legal harmonization and practical socio-technical implementation. As a jurisdiction shaped by GDPR-oriented legal reform while simultaneously undergoing rapid urban digitalization, Türkiye offers a useful lens for understanding privacy governance challenges that are increasingly visible across many non-EU and emerging digital governance contexts.

The cases were selected through a purposive analytical sampling strategy rather than for statistical representativeness. The objective was not to produce an exhaustive inventory of smart city applications in Türkiye, but to identify cases that capture different configurations of data-intensive urban governance. In this respect, the selected applications represent distinct but recurring socio-technical modalities within smart city ecosystems, including citizen participation platforms, location-based monitoring systems, digital municipal service portals, public safety and geofencing infrastructures, urban surveillance networks, and smart mobility platforms.

These cases were chosen because they vary across key analytical dimensions central to this study: the type of personal data processed, the legal basis invoked or implied, the technical infrastructure involved, the degree of automation and ambient data collection, and the nature of privacy and governance risks produced. Taken together, the six cases provide a structured cross-section of how personal data are collected, processed, and governed within Türkiye's smart city environment. They are therefore treated not as isolated examples, but as analytically selected instances that illuminate broader socio-technical patterns of privacy governance. In this sense, the case study design follows a logic of analytical generalization rather than statistical generalization.

The empirical analysis employs Data Flow Mapping (DFM) to identify data collection points, categories of personal data processed, purposes of processing, relevant actors, consent mechanisms, and data transfer pathways. Each case is evaluated in relation to KVKK provisions and Data Protection Impact Assessment (DPIA)-inspired risk indicators in order to identify high-risk processing activities, ambiguous consent practices, secondary data use, and automated or inferential decision-support mechanisms.

For the purposes of this study, socio-technical risks are operationalized as structurally recurring conditions that may weaken meaningful privacy protection within smart city systems. These risks are identified through qualitative indicators derived from the interaction between legal safeguards, technical infrastructures, and governance arrangements. More specifically, the analysis evaluates whether a given application exhibits one or more of the following conditions: continuous or ambient data collection, opaque or weakly informed consent mechanisms, secondary or functionally expanded data use, limited user visibility and control, cross-system interoperability and data aggregation, retention and access uncertainty, and the presence of automated or inferential decision-support mechanisms.

These indicators are assessed through publicly observable features of each application, including privacy notices, user interfaces, declared processing purposes, data categories, infrastructural design, and institutional context. Risks are interpreted as systemic where they arise not merely from isolated legal non-compliance, but from the structural organization of data flows, technological architectures, or governance practices that reduce transparency, contestability, and meaningful user agency. The study therefore does not attempt to quantify risk numerically, but to evaluate whether particular applications reproduce recurring socio-technical conditions associated with heightened privacy vulnerability.

The study relies on publicly available documents and observable system structures. While this approach limits access to internal compliance procedures, it enables the identification of externally verifiable governance patterns within Türkiye's emerging smart city ecosystems. To ensure alignment between findings and claims, the study does not infer privacy restructuring from normative theory alone. Instead, this conclusion is based on the combined evaluation of doctrinal developments and empirical socio-technical patterns. At the doctrinal level, the analysis examines whether the legal framework for data protection increasingly shifts from an explicit consent-centered model toward broader governance mechanisms such as accountability, risk-based oversight, and privacy by design. At the empirical level, the study assesses whether smart city applications exhibit recurring patterns such as ambient data collection, weakly meaningful consent, interoperability, limited contestability, and infrastructural opacity, which indicate a practical reconfiguration of how privacy is protected. Accordingly, claims about privacy persistence, transformation, or erosion are grounded in the observed relationship between formal legal norms and their actual implementation in practice.

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

4 Findings: Data Protection Governance in Smart City Ecosystems

4.1 Paradigm Shift in Data Protection Law

The concept of a "transformation of privacy" employed in this study pertains to a shift in the underlying logic of privacy protection, rather than a mere binary distinction of presence or absence. Consequently, the findings are analyzed within the frameworks of persistence, transformation, and erosion, contingent upon whether privacy safeguards continue to be effective, are institutionally restructured, or are substantially diminished in practice.

Contemporary data protection law is undergoing a significant paradigmatic transformation at both national and supranational levels. This shift is particularly visible in the changing role of legal bases governing personal data processing and the evolving relationship between constitutional privacy guarantees and regulatory governance models.

A comparative assessment of Türkiye's Personal Data Protection Law No. 6698 (KVKK) and the European Union's General Data Protection Regulation (GDPR) reveals substantial convergence in core principles such as lawfulness, transparency, purpose limitation, data minimization, and accountability. These similarities reflect Türkiye's regulatory alignment with European Union data protection standards [22]. However, important differences remain regarding enforcement culture, supervisory authority independence, and the institutional mechanisms through which rights are realized.

Historically, explicit consent has been regarded as the primary legal foundation for data processing. However, recent regulatory changes suggest a gradual move toward alternative legal bases such as legitimate interest and statutory authorization. This shift highlights the limitations of consent-based models in complex digital environments marked by information asymmetries and behavioral manipulation techniques. In AI-driven systems and large-scale data infrastructures, relying on consent becomes increasingly problematic. Algorithmic profiling, predictive analytics, and collective data processing challenge the idea that individuals can effectively control the use of their data through consent mechanisms. As a result, modern data protection regimes are increasingly dependent on broader governance frameworks rather than solely on individual authorization models [23] [24].

Cross-border data governance further illustrates this transformation. The Schrems II decision of the Court of Justice of the European Union significantly reshaped the global regulatory landscape by emphasizing that adequate data protection requires not only formal commitments but also effective safeguards against disproportionate surveillance [25]. For Türkiye, these developments highlight the need to balance data sovereignty concerns with participation in global digital markets.

4.2 Socio-Technical Dynamics of Smart City Data Ecosystems

Smart cities operate through dense infrastructures of sensors, mobile applications, and interconnected platforms that continuously generate and process data. Within these environments, personal data circulate across multiple actors, including municipalities, private technology providers, and platform intermediaries.

This architecture blurs traditional data boundaries and often reduces the visibility of data processing activities for citizens. Personal data may be collected through ambient infrastructures such as cameras, sensors, and IoT devices, frequently without direct interaction between data subjects and the system. As a result, smart city environments increasingly resemble pervasive surveillance infrastructures with significant implications for privacy and fundamental rights [26] [27].

The literature suggests that technical security measures and regulatory compliance alone are insufficient to address these governance challenges. Instead, effective privacy governance requires integrated approaches that combine institutional oversight, transparency mechanisms, and citizen participation [28].

Within this context, principles such as privacy by design and privacy by default have emerged as key governance tools. These principles aim to integrate privacy protections directly into system architectures. However, empirical studies show that implementation often remains superficial when these principles are treated solely as compliance requirements rather than as broader socio-technical governance commitments [29].

From the perspective of algorithmic governance, these infrastructures do not merely facilitate service delivery; they also participate in shaping how individuals are rendered visible, categorized, and governed within urban environments. As such, smart city systems function not only as technological tools but also as administrative architectures of governance.

4.3 Artificial Intelligence, Algorithmic Governance, and Structural Privacy Risks

The growing integration of artificial intelligence systems into digital infrastructures introduces additional governance challenges. AI-driven decision-making systems rely on large-scale datasets and complex

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

computational models that are often difficult to interpret. This "black-box" character raises concerns regarding transparency, accountability, and the ability of individuals to contest automated decisions [30].

Transparency mechanisms such as algorithmic explanations are frequently proposed as safeguards. However, the literature cautions that transparency alone may not ensure meaningful accountability, particularly in complex or adversarial decision environments [31]. As a result, the governance of AI systems increasingly requires institutional oversight mechanisms that extend beyond technical transparency.

Another major concern relates to algorithmic discrimination. Machine learning models are trained on historically embedded datasets and may reproduce or amplify existing social inequalities. Empirical studies demonstrate that algorithmic systems can generate discriminatory outcomes in domains such as employment, credit scoring, and public service allocation [32] [33].

These dynamics highlight the growing importance of data justice frameworks, which seek to ensure the equitable distribution of risks and benefits arising from data-driven systems. In this perspective, privacy is no longer viewed solely as an individual right but as a structural component of fair digital governance.

These findings also highlight the relevance of data justice as an analytical framework. The risks generated by AI-driven systems are not evenly distributed across populations; rather, they may disproportionately affect individuals and groups who are more exposed to monitoring, less able to understand data processing practices, or less capable of contesting automated outcomes. In this respect, privacy protection must be evaluated not only in terms of formal legality, but also in terms of fairness, visibility, and the equitable distribution of digital risks.

4.4 Case Study: Socio-Technical Mapping of Personal Data Processing in Turkish Smart Cities

Smart city initiatives implemented in Türkiye increasingly rely on digital infrastructures that collect and process personal data in order to provide urban services, enhance public safety, and facilitate citizen participation. While some smart city technologies primarily process technical or environmental data, many applications directly involve the processing of citizens' personal information. In such cases, the lawfulness of these practices must be evaluated within the framework of the Turkish Personal Data Protection Law No. 6698 (KVKK). In particular, determining whether these applications process personal data in accordance with the legal principles established by the KVKK requires careful legal and socio-technical analysis.

In the Turkish context, several smart city applications illustrate how personal data are processed under different legal bases. These applications operate in areas such as citizen participation, digital municipal services, location-based monitoring, urban surveillance systems, and smart transportation platforms. Examining these systems provides important insights into how personal data protection principles are implemented in practice.

4.4.1 Citizen Participation Platforms

One example of participatory governance within smart city infrastructures is the "Trabzon İçin Bir Fikrim Var" application developed by the Trabzon Metropolitan Municipality. The system enables citizens to submit opinions, complaints, and suggestions regarding urban governance through physical kiosks installed in public spaces. These interactions are recorded through audio and video technologies in order to document citizen feedback.

From a data protection perspective, the system processes audiovisual data belonging to individuals. According to Article 5(1) of the KVKK, personal data may be processed if the data subject provides explicit consent. In this application, individuals voluntarily interact with the system while being aware that their voices and images are recorded. Therefore, the processing of personal data occurs based on informed participation and explicit consent of the data subjects. At the same time, the application demonstrates how participatory smart city mechanisms may involve the processing of personal data as part of democratic engagement processes [34].

4.4.2 Location-Based Monitoring Systems

Another example is the "Sevgi Çipi" application, which enables family members to monitor individuals suffering from Alzheimer's disease or similar cognitive disorders. The system operates through a device carried by the individual, allowing real-time location tracking and information sharing with relatives. Because location data can directly identify an individual's position in space, such data constitute personal data under the KVKK.

Under Article 5 of the Turkish Personal Data Protection Law (KVKK No. 6698), the processing of personal data generally requires the explicit consent of the data subject. However, Article 5(2)(b) provides a key exception by allowing personal data to be processed without consent when it is necessary to protect the life or physical integrity of a person who cannot give valid consent due to factual impossibility or legal incapacity. This includes individuals with severe cognitive impairments—such as those with advanced dementia or similar conditions—who may fall within this exception. Consequently, processing location data to ensure their safety

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

can typically be justified on this legal basis. However, simply having a legitimate aim does not automatically make such processing lawful. Following the principles outlined in Article 4 of the KVKK, personal data must be processed in a manner that is lawful, fair, accurate, relevant, limited, and proportional to the purpose. Therefore, systems like the Sevgi Çipi may only be considered compatible with the KVKK if they adhere to the principles of necessity and proportionality, minimize data collection, and include appropriate technical and organizational safeguards. Additionally, even without an explicit consent requirement, the obligation to inform (aydınlatma yükümlülüğü) under Article 10 of the KVKK still applies, requiring transparency about the purposes and conditions of data processing. In conclusion, while Article 5(2)(b) provides a valid legal basis for processing personal data in emergency or protective situations, the legality of location tracking systems depends on a comprehensive assessment of compliance with the broader data protection principles established by Turkish law [35] [36] [37] [38].

Similar legal reasoning also applies to related systems such as panic button applications, safety monitoring platforms, and digital health monitoring tools designed to protect individuals who cannot provide legally valid consent.

4.4.3 Digital Municipal Services and Cookie Technologies

Digital municipal service platforms represent another important area where personal data processing occurs within smart city ecosystems. The Balıkesir e-Municipality system enables citizens to access a variety of municipal services online, including tax payments, debt inquiries, and administrative record checks. In order to perform these services, users must provide personal information such as identification numbers and telephone numbers. In addition to these inputs, the platform also relies on cookies that record user activity on the website. These cookies may store information about visited pages, access times, and authentication credentials. Such data are stored within internet browsers and remain active unless manually deleted by the user. Because these data can be linked to identifiable individuals, they fall within the scope of personal data under the KVKK. Although users are typically informed about cookie policies through pop-up notifications, questions remain regarding whether users fully understand the implications of such data processing mechanisms. When users accept the cookie policy after being informed, the processing of personal data can be considered lawful based on explicit consent under Article 5 of the KVKK. However, if cookies continue to operate despite the rejection of consent or without meaningful user awareness, such practices may raise concerns regarding unlawful data processing [34].

4.4.4 Public Safety Monitoring Systems

Another category of smart city applications concerns location-based safety systems such as the “Güven Çemberi” project. This system operates through wearable devices that transmit location information to mobile applications used by parents or guardians. Sensors installed in public areas create a digital boundary, and users receive notifications if the individual wearing the device leaves the designated safe zone. The project is primarily designed for children, individuals with cognitive impairments, and even pets. Since these individuals may not possess legal capacity to provide valid consent, the legal evaluation of the system relies on Article 5(2)(b) of the KVKK, which allows the processing of personal data when necessary to protect life or physical integrity. Therefore, the processing of location data within this system is generally considered lawful when it serves protective purposes [34].

4.4.5 Urban Surveillance Systems

Urban surveillance systems such as MOBESE (Mobile Electronic System Integration) or the Urban Security Management System (KGYS) constitute one of the most debated aspects of smart city governance. These camera networks are widely deployed in urban areas in order to monitor traffic, enhance public security, and provide evidence in criminal investigations.

The legal status of such systems has been subject to debate in the literature. One perspective argues that images recorded in public spaces do not necessarily violate personal data protection principles because individuals are already visible to others in public environments. Another perspective argues that the systematic recording and storage of visual data may constitute an interference with privacy rights.

The distinction between observation and recording is therefore crucial. Observing individuals in public spaces may not raise legal concerns; however, recording, storing, and processing visual data introduce additional legal obligations. Questions regarding where the recorded data are stored, how long they are retained, and who has access to them are central to assessing compliance with personal data protection principles.

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

The European Court of Human Rights addressed a similar issue in the case of Peck v. United Kingdom (2003), where it stated that while camera observation in public spaces may not necessarily violate privacy rights, the recording and dissemination of such footage may constitute an infringement of the right to private life [39].

4.4.6 Smart Mobility Platforms

Smart transportation platforms represent another important component of urban data ecosystems. The iTaksi application, developed under the supervision of the Istanbul Metropolitan Municipality, enables users to locate nearby taxis, track journeys, evaluate drivers, and plan travel routes. In order to enhance passenger safety, the system includes in-vehicle security cameras that record visual data without audio. These recordings are stored locally within the device for a limited period of time and are accessible only in cases where legal authorities request them during criminal investigations. According to the information provided by the platform, recorded footage is retained for approximately one week before being automatically deleted. Under the KVKK framework, the recorded video images constitute personal data. However, the application clearly informs users about the existence of in-vehicle cameras and the conditions under which the recordings may be used. Because users are informed and voluntarily choose to use the service, the processing of these data is generally considered compatible with the explicit consent principle [34].

The examples discussed above demonstrate that personal data processing in Turkish smart city applications occurs across multiple technological and institutional contexts. These systems illustrate how digital infrastructures designed for urban governance may simultaneously generate complex data protection challenges.

First, many smart city applications rely on continuous or automated data collection mechanisms that reduce the visibility of data processing activities for individuals. Second, the integration of multiple technological systems increases the possibility of data aggregation and secondary data use. Third, certain surveillance technologies operate in regulatory environments where legal frameworks remain ambiguous or incomplete.

Consequently, effective data protection in smart city environments requires not only legal compliance with the KVKK but also broader governance mechanisms that address the interaction between technological infrastructures, institutional practices, and societal expectations regarding privacy.

Table 1. Socio-Technical Analysis of Personal Data Processing in Turkish Smart City Cases

Case Study Application	Data Category	Primary Legal Basis (KVKK)	Technical Infrastructure	Identified Privacy Risk
1. Citizen Participation (Trabzon)	Audiovisual	Art. 5(1) - Explicit Consent	Physical Kiosks, Audio/Video	Informed participation vs. permanent storage risks.
2. Sevgi Çipi (Vulnerable Monitoring)	Real-time Location	Art. 5(2)(b) - Vital Interests	IoT Wearables, GPS	Data security for sensitive vulnerable populations.
3. e-Municipality (Balıkesir)	ID, Finance, Cookies	Art. 5(1) - Explicit Consent	Web/Cloud Portals, Cookies	Lack of meaningful awareness in cookie tracking.
4. Güven Çemberi (Safety Zones)	Geofencing Data	Art. 5(2)(b) - Vital Interests	Wearables, Proximity Sensors	Potential for long-term behavioral profiling.
5. Urban Surveillance (MOBESE/KGYS)	Visual/Biometric	Statutory Authorization	AI-integrated CCTV Networks	Function creep and lack of individual opt-out.
6. iTaksi (Smart Mobility)	Video (In-vehicle)	Art. 5(1) - Explicit Consent	On-board Cameras, Cloud	Ambient sensing in private-public hybrid spaces.

Source: [34] [39].

4.5 Challenges and Opportunities in Personal Data Processing for Smart City Applications in Türkiye

The integration of personal data processing within smart city applications in Türkiye presents both substantial challenges and promising opportunities. Local governments face multiple obstacles, including data security concerns, inadequate infrastructure, and legal ambiguities, which complicate the effective implementation of smart city strategies. Nevertheless, advancements in technology and innovative governance frameworks have the potential to improve data management and privacy, thereby facilitating more efficient urban solutions.

SAGA: Journal of Technology and Information Systems
Vol 4, Issue 1, February 2026, Page 551-564
ISSN: 2985-8933 (Media Online)
DOI: 10.58905/SAGA.v4i1.598

A. Challenges in Personal Data Processing
   a. Data Security: Safeguarding personal data remains a primary concern, as breaches may erode public trust and undermine citizen engagement [40].
   b. Infrastructure Limitations: Many municipalities lack the technological and physical infrastructure necessary to support advanced smart city initiatives [40].
   c. Legal and Bureaucratic Barriers: Ambiguous regulations and bureaucratic resistance hinder the adoption of data-driven governance approaches [40].
   d. Human Resource Constraints: High staff turnover and insufficiently trained personnel further impede effective data management [40].

B. Opportunities for Improvement
   a. Privacy-Preserving Frameworks: Innovative methodologies for data collection and processing can maintain privacy while effectively leveraging real-world data [41].
   b. Technological Integration: The deployment of big data analytics and the Internet of Things (IoT) can enhance service delivery, urban management, and decision-making processes [42].
   c. Public-Private Partnerships: Collaborative initiatives between government and private actors can support innovative financing models and accelerate infrastructure development [42].

Despite these opportunities, the risk of personal data misuse remains a critical concern, necessitating robust privacy protections to ensure citizen trust and participation in smart city initiatives [43]. Achieving a balance between innovation, legal compliance, and ethical data governance is therefore essential for the sustainable development of smart cities in Türkiye. These challenges demonstrate that the governance of personal data in smart cities is not only a matter of legal compliance, but also of algorithmic governance capacity and data justice.

5 Conclusion

The algorithmic age has fundamentally transformed the conditions under which privacy and personal data protection operate. The expansion of big data infrastructures, Internet of Things (IoT) ecosystems, and artificial intelligence (AI)-driven decision systems has turned personal data processing into a structural feature of digital governance. In this context, privacy can no longer be understood solely as an individual right; it must also be interpreted as a socio-technical governance challenge embedded within digital infrastructures.

This study demonstrates that contemporary privacy challenges cannot be addressed through legal regulation or technological innovation alone. Instead, they emerge from the interaction of multiple structural dynamics, including the gradual decline of explicit consent as the dominant legal basis for data processing, the increasing reliance on alternative legal grounds, the normalization of ambient data collection, and the growing opacity of algorithmic decision-making systems. These developments collectively reshape the normative foundations of data protection law.

The comparative analysis of Türkiye's Personal Data Protection Law No. 6698 (KVKK) and the European Union's General Data Protection Regulation (GDPR) reveals a high degree of formal convergence between the two regimes. Nevertheless, significant differences remain regarding enforcement practices, cross-border data governance, and the institutional capacity of supervisory authorities. In particular, the declining centrality of explicit consent reflects a broader transition from an autonomy-centered privacy model toward a systemic governance approach focused on regulating large-scale data flows.

The empirical analysis of smart city applications in Türkiye highlights a substantial gap between formal regulatory frameworks and socio-technical practices. Data Flow Mapping indicates that in many cases consent mechanisms function primarily as formal interface requirements rather than as meaningful safeguards. In IoT-based infrastructures where data collection occurs through ambient sensing and interconnected systems, privacy risks become structurally embedded within technological architectures.

From a theoretical perspective, the findings suggest that privacy in the algorithmic age should be reconceptualized as a systemic and infrastructural condition rather than solely as an individual right exercised through consent. In smart city ecosystems, where data processing is ambient, continuous, and often inferential, the meaningful protection of privacy depends less on isolated moments of authorization and more on the governance quality of the surrounding socio-technical environment. This shifts privacy theory from an individual-control paradigm toward a structural governance perspective centered on accountability, visibility, institutional safeguards, and data justice.

Although this study is grounded in the Turkish context, its implications extend beyond Türkiye. The case demonstrates how formal legal convergence with global data protection standards does not automatically translate into substantively effective privacy protection within complex digital infrastructures. In this respect, Türkiye represents a broader category of rapidly digitalizing governance environments in which regulatory

modernization coexists with institutional asymmetries, infrastructural opacity, and uneven implementation. The findings are therefore analytically transferable to wider discussions on privacy governance in smart cities, particularly in jurisdictions situated between global regulatory diffusion and context-specific governance constraints.

These findings suggest that effective privacy protection in data-driven societies requires a multi-layered governance approach. Legal frameworks remain necessary but insufficient without complementary technical safeguards, institutional oversight mechanisms, and societal awareness regarding data-related risks.

The study also shows that concepts such as algorithmic governance and data justice are analytically necessary for understanding privacy in data-driven societies. Privacy risks in smart city ecosystems are not produced only through unlawful data collection, but through the governance logics and unequal power relations embedded in socio-technical systems. Accordingly, effective privacy protection requires not only legal compliance, but also fair, transparent, and contestable forms of digital governance.

Three broader implications emerge from this analysis. First, regulatory reforms should prioritize not only legal harmonization but also stronger enforcement capacity, particularly in areas such as cross-border data transfers and high-risk data processing activities. Second, principles such as privacy by design and privacy by default must move beyond abstract policy commitments and become operational governance standards integrated into technological infrastructures. Third, sustainable privacy governance requires greater attention to data justice, including mechanisms that address algorithmic discrimination, information asymmetries, and unequal exposure to surveillance risks.

Ultimately, the future of privacy in the algorithmic age will depend on the degree to which legal norms, technological architectures, and institutional practices can be aligned. Smart city ecosystems illustrate both the opportunities and the risks of data-driven governance. Ensuring that privacy remains a meaningful value therefore requires embedding privacy protections not only in legal frameworks but also in technological design, institutional oversight, and civic awareness.

References

[1] Allen, Anita L., and Christopher Muhawe. "Is Privacy Really a Civil Right?." Berkeley Tech. LJ 40, 2025.

[2] B. F. G. Fabrègue and A. Bogoni, “Privacy and Security Concerns in the Smart City,” *Smart Cities*, vol. 6, no. 1, pp. 586–613, Feb. 2023, doi: 10.3390/smartcities6010027.

[3] B. Kinikoglu, “Implementing a new data protection law: lessons from the Turkish experience,” *International Data Privacy Law*, vol. 13, no. 1, pp. 25–46, Mar. 2023, doi: 10.1093/idpl/ipad001.

[4] F. Tanrikulu, “Comparative Evaluation of Selected Elements of Data Protection Regulations: Türkiye’s KVKK and the EU’s GDPR,” *Comparative Law Review*, no. 31, pp. 205–243, Dec. 2025, doi: 10.12775/CLR.2025.008.

[5] E. Küzeci, “Turkish data protection law: GDPR alignment and key 2024 amendment,” *Journal of Data Protection & Privacy*, vol. 7, no. 4, p. 372, Jun. 2025, doi: 10.69554/FOTQ9875.

[6] F. S. Doğan, “RECENT AMENDMENTS AND JUDICIAL REVIEW OF DECISIONS BY THE TURKISH DATA PROTECTION AUTHORITY,” *Law and Justice Review*, vol. 28, pp. 57–76, 2024.

[7] L. Keser Berber and A. Atabey, “Turkey · Evaluation of the Recent Developments in Laws and Policies Relating to Cross-Border Data Transfers in Turkey,” *European Data Protection Law Review*, vol. 8, no. 2, pp. 302–310, 2022, doi: 10.21552/edpl/2022/2/19.

[8] S. S. Siryon, “PRINCIPLES AND APPLICATIONS OF THE RIGHT TO PRIVACY: EVALUATING INTERNATIONAL PERSPECTIVES AND LAWS,” *LawFoyer International Journal of Doctrinal Legal Research*, vol. 3, no. 3, pp. 897–909, Oct. 2025, doi: 10.70183/lijdlr.2025.v03.116.

[9] C. Aradau and E. Mc Cluskey, “Making Digital Surveillance Unacceptable? Security, Democracy, and the Political Sociology of Disputes,” *International Political Sociology*, vol. 16, no. 1, Apr. 2022, doi: 10.1093/ips/olab024.

[10] C. Mohan, “Surveillance and National Security: Balancing Privacy and Public Interest for a Safer Society,” 2025, pp. 537–561. doi: 10.2991/978-2-38476-426-6_26.

[11] P. Königs, “Government Surveillance, Privacy, and Legitimacy,” *Philos Technol*, vol. 35, no. 1, p. 8, Mar. 2022, doi: 10.1007/s13347-022-00503-9.

[12] J. Duncan, *National Security Surveillance in Southern Africa*. Bloomsbury Publishing Plc, 2022. doi: 10.5040/9780755640256.

[13] K. Nishat, “Human Rights Protections in Digital Surveillance: Balancing Security Needs and Privacy Rights.,” *Mayo Communication Journal*, vol. 1, no. 1, pp. 83–92, 2024.

[14] Q. Bu, "Behind the Huawei sanction: national security, ideological prejudices or something else?," *International Cybersecurity Law Review*, vol. 5, no. 2, pp. 263–300, Jun. 2024, doi: 10.1365/s43439-024-00112-6.
[15] A. Krysovatyy, O. Desyatnyuk, and O. Ptashchenko, "Digital Innovations and their Ramifications for Financial and State Security," *AFRICAN JOURNAL OF APPLIED RESEARCH*, vol. 10, no. 1, pp. 431–441, Jul. 2024, doi: 10.26437/ajar.v10i1.713.
[16] Mosa, M. J., Barhoom, A. M., Alhabbash, M. I., Harara, F. E., Abu-Nasser, B. S., & Abu-Naser, S. S. "AI and Ethics in Surveillance: Balancing Security and Privacy in a Digital World," *International Journal of Academic Engineering Research (IJAER)* , vol. 8, no. 10, pp. 8–15, 2024.
[17] S. Shahriar, S. Allana, S. M. Hazratifard, and R. Dara, "A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle," *IEEE Access*, vol. 11, pp. 61829–61854, 2023, doi: 10.1109/ACCESS.2023.3287195.
[18] L. Kisselburgh and J. Beever, "The Ethics of Privacy in Research and Design: Principles, Practices, and Potential," in *Modern Socio-Technical Perspectives on Privacy*, Cham: Springer International Publishing, 2022, pp. 395–426. doi: 10.1007/978-3-030-82786-1_17.
[19] A. López Martínez, M. Gil Pérez, and A. Ruiz-Martínez, "A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare," *ACM Comput Surv*, vol. 55, no. 12, pp. 1–38, Dec. 2023, doi: 10.1145/3571156.
[20] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review," *Sensors*, vol. 23, no. 2, p. 788, Jan. 2023, doi: 10.3390/s23020788.
[21] S. Sannon, B. Sun, and D. Cosley, "Privacy, Surveillance, and Power in the Gig Economy," in *CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, Apr. 2022, pp. 1–15. doi: 10.1145/3491102.3502083.
[22] A. G. Evren, "Comparative Analysis of the European Union and Turkish Personal Data Protection Laws: Basic Principles, Legal Grounds, and Rights of Data Subjects," *Kişisel Verileri Koruma Dergisi*, vol. 5, no. 2, pp. 39–64, 2023.
[23] A. J. Andreotta, N. Kirkham, and M. Rizzi, "AI, big data, and the future of consent," *AI Soc*, vol. 37, no. 4, pp. 1715–1728, Dec. 2022, doi: 10.1007/s00146-021-01262-5.
[24] G. Malgieri and G. González Fuster, "The Vulnerable Data Subject: A Gendered Data Subject?," *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3913249.
[25] D. S. Guamán, D. Rodriguez, J. M. del Alamo, and J. Such, "Automated GDPR compliance assessment for cross-border personal data transfers in android applications," *Comput Secur*, vol. 130, p. 103262, Jul. 2023, doi: 10.1016/j.cose.2023.103262.
[26] S. E. Bibri and Z. Allam, "The Metaverse as a Virtual Form of Data-Driven Smart Urbanism: On Post-Pandemic Governance through the Prism of the Logic of Surveillance Capitalism," *Smart Cities*, vol. 5, no. 2, pp. 715–727, May 2022, doi: 10.3390/smartcities5020037.
[27] A. Solow-Niederman, "Information Privacy and the Inference Economy," *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3921003.
[28] E. Morozov, "Critique of Techno-Feudal Reason," *New Left Rev*, vol. 2, no. 133, pp. 89–126, Jan. 2022, doi: 10.64590/13n.
[29] S. Barth, D. Ionita, and P. Hartel, "Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines," *ACM Comput Surv*, vol. 55, no. 3, pp. 1–37, Mar. 2023, doi: 10.1145/3502288.
[30] K. Wach *et al.*, "The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT," *Entrepreneurial Business and Economics Review*, vol. 11, no. 2, pp. 7–30, 2023, doi: 10.15678/EBER.2023.110201.
[31] S. Bordt, M. Finck, E. Raidl, and U. von Luxburg, "Post-Hoc Explanations Fail to Achieve their Purpose in Adversarial Contexts," in *2022 ACM Conference on Fairness Accountability and Transparency*, New York, NY, USA: ACM, Jun. 2022, pp. 891–905. doi: 10.1145/3531146.3533153.
[32] A. Kelly-Lyth, "Algorithmic discrimination at work," *European Labour Law Journal*, vol. 14, no. 2, pp. 152–171, Jun. 2023, doi: 10.1177/20319525231167300.
[33] A. C. B. Garcia, M. G. P. Garcia, and R. Rigobon, "Algorithmic discrimination in the credit domain: what do we know about it?," *AI Soc*, vol. 39, no. 4, pp. 2059–2098, Aug. 2024, doi: 10.1007/s00146-023-01676-3.
[34] Y. Hayta, "Akıllı Kent Uygulamalarında Kişisel Verilerin Gizliliği ve Güvenliği," *Firat University Journal of Social Sciences*, vol. 31, no. 2, pp. 929–941, 2021.
[35] Kişisel Verileri Koruma Kurumu, "Personal Data Protection Law ." Accessed: Mar. 31, 2026. [Online]. Available: https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

[36] Kişisel Verileri Koruma Kurumu, “Obligation to Inform (Aydınlatma Yükümlülüğü).” Accessed: Mar. 31, 2026. [Online]. Available: https://www.kvkk.gov.tr/Icerik/6637/Communique-On-Principles-And-Procedures-To-Be-Followed-In-Fullfillment-Of-The-Obligation-To-Inform

[37] Kişisel Verilerin Korunması Kanunu, “KİŞİSEL VERİLERİN KORUNMASI KANUNU.” Accessed: Mar. 31, 2026. [Online]. Available: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5

[38] Kişisel Verileri Koruma Kurumu, “Principles on Processing of Personal Data.” Accessed: Mar. 31, 2026. [Online]. Available: https://www.kvkk.gov.tr/Icerik/6639/Principles-of-Processing-Personal-Data

[39] C. Gallagher, “CCTV and Human Rights: the Fish and the Bicycle? An Examination of Peck V. United Kingdom (2003) 36 E.H.R.R. 41,” *Surveill Soc*, vol. 2, no. 2/3, Sep. 2002, doi: 10.24908/ss.v2i2/3.3378.

[40] A. ÖZDEMİR, “DATA- AND KNOWLEDGE-DRIVEN SMART CITY STRATEGIES: RESEARCH ON IMPLEMENTATION CHALLENGES OF LOCAL GOVERNMENTS IN TURKEY,” *Yönetim ve Ekonomi Araştırmaları Dergisi*, vol. 20, no. 3, pp. 152–169, Oct. 2022, doi: 10.11611/yead.1162186.

[41] Y. Sei, “Privacy-Preserving Data Collection and Analysis for Smart Cities,” in *Human-Centered Services Computing for Smart Cities*, Singapore: Springer Nature Singapore, 2024, pp. 157–209. doi: 10.1007/978-981-97-0779-9_5.

[42] A. Erbey, “Akıllı Şehirlerde Teknoloji ve Veri Yönetimi: Geleceğin Şehir Yaşamı,” in *Yönetim Bilişim Sistemleri Alanında Yenilikçi Çözümler ve Güncel Yaklaşımlar*, Özgür Yayınları, 2025. doi: 10.58830/ozgur.pub700.c2986.

[43] Lioudakis, Georgios V., Dimitra I. Kaklamani, and Iakovos S. Venieris. "Personal data protection under the InfoCity lights." *2009 European Wireless Technology Conference*. IEEE, 2009.