UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF POLITICAL SCIENCE, LAW,
AND INTERNATIONAL STUDIES

Master's degree in
European and Global Studies

THE EVOLUTION OF PERSONAL DATA PROTECTION FRAMEWORKS:

A COMPARATIVE ANALYSIS OF LEGAL APPROACHES IN THE UNITED STATES, RUSSIA, AND EUROPE

Supervisor: Prof. GUIDO GORGONI

Candidate: ANNA MZHELSKAIA

Matriculation No. 2106504

A.Y. 2025/2026

Abstract

This dissertation examines the effectiveness of contemporary data protection regimes through a historically grounded comparative legal analysis of the United States, Russia, and Europe. Rather than assessing data protection solely as a set of legislative norms, the study examines it as a comprehensive legal system shaped by historical traditions, institutional structures, enforcement mechanisms, resources, and underlying threat perceptions. The central research question is which regulatory model provides the most effective level of personal data protection when assessed as a coherent and functioning system rather than as a formal set of rules.

The study employs a diachronic-synchronous comparative methodology, tracing the evolution of privacy and data protection from their philosophical and constitutional foundations to contemporary regulatory frameworks. The analysis demonstrates that persistent divergence between regulatory models is not primarily the result of insufficient harmonisation, but of deeply embedded legal cultures, governance priorities, and historically conditioned institutional trajectories. Despite technological convergence and increasing global coordination, contemporary reforms largely adapt existing structural logics rather than fundamentally transform them.

The analysis shows that the United States prioritises sectoral regulation and flexible enforcement; Europe emphasises human rights-based coherence and institutional independence; and Russia promotes a state-centric, security-focused model centred on sovereignty and administrative control. Effectiveness is assessed based on legislative coherence, judicial interpretation, enforcement mechanisms, and systemic resilience.

The dissertation concludes that no single model offers a one-size-fits-all solution. Regulatory effectiveness depends on internal coherence, institutional capacity, and the alignment between regulatory guarantees and practical implementation. By integrating historical, doctrinal, judicial, and institutional analysis, the study develops a multidimensional framework for assessing personal data protection regimes and lays the foundation for extending comparative research to other jurisdictions and developing context-sensitive normative guidance.

Table of Contents

Introduction

The essence of personal data legislation is grounded in the relationships between three legal entities: individuals, companies, and intermediaries (Solove, 2006; González Fuster, 2014). This structure is consistent across jurisdictions, as the underlying concepts are rooted in constitutional guarantees of privacy and anonymity, as well as in international legal instruments such as Convention 108 of the Council of Europe (1981) (De Hert & Gutwirth, 2009). In this sense, it is not the law itself that fundamentally differs, but rather the way it is applied or, more precisely, the institutional and historical logic of its application: how the law was initially drafted, subsequently amended, and applied over time (Mahoney & Thelen, 2010).

It is generally accepted that legislation represents the state and society's response to perceived threats (Beck, 1992). Accordingly, the threat model created by a given state largely determines the legal instruments it employs (Bennett & Raab, 2006). Each regulatory approach is shaped by a core value that guides legislative intervention. In the United States, personal data regulation has been predominantly shaped by a market-oriented, competition-based logic, in which data concentration is often viewed as a potential monopolistic threat, whereas in Europe it has been primarily grounded in a human-rights-based constitutional logic (Cohen, 2019). In contrast, Russia is generally characterised as a jurisdiction in which the collection and processing of personal data are perceived primarily as threats to privacy and national or strategic security (Budnitsky & Jia, 2018).

Academics often cite the early 2010s as a turning point in the development of personal data protection (González Fuster, 2014), reflecting two key issues: large-scale data breaches and a growing emphasis on information sovereignty (Solove & Citron, 2018). The 2015 disclosure of highly sensitive data from the servers of the dating platform Ashley Madison, which led to an international wave of personal, political, and legal repercussions, became one of the most illustrative examples of the social impact of data breaches (Greenberg, 2015). Furthermore, after 2014, states increasingly recognised that, beyond land, air, and maritime borders, they faced a new and ill-defined realm, digital space, where the boundaries of jurisdiction and sovereignty remained unclear (Bradford, 2020). This realisation ushered in intensified efforts to establish control over

information flows, commonly referred to as the struggle for information sovereignty (Deibert et al., 2010). In response to these and other challenges identified during the 2010s, modern data protection legislation began to emerge.

By the mid-2020s, data protection had become one of the most complex, controversial, and strategically important issues in modern law and public administration (Zuboff, 2019). The emergence of artificial intelligence, rapid digitalisation, the expansion of algorithmic decision-making, the globalisation of data flows, and the growing reliance of both public authorities and private entities on large-scale data processing have fundamentally changed the relationship between individuals, markets, and the state. Companies can no longer operate without collecting, processing, and storing vast amounts of personal data daily, while individuals increasingly face tangible consequences of such practices. This dynamic is well illustrated by documented cases of digital platforms providing users with extensive records of their personal data, sometimes running to hundreds of pages, detailing their online behaviour and personal preferences (Duportail, 2017).

In 2026, data protection issues will remain at the forefront of the global legal and policy agenda (Fox, 2025). Increased digital surveillance, transnational flows of personal data, repeated large-scale data breaches, rapid advances in artificial intelligence technologies, and growing concerns about national security all require a comprehensive assessment of the resilience and effectiveness of existing legal frameworks (Fox, 2025). Leading experts are increasingly describing this period as the "industrialisation of cybercrime," characterised by the use of artificial intelligence to carry out autonomous, rapid, and often undetected data breaches (Fox, 2025). As states tighten regulatory control over data and companies continue to expand their data collection practices, at least 33 confirmed data breaches occur daily worldwide, more than one every hour (TheBestVPN.com, 2026). These events have exposed the structural vulnerabilities of existing personal data protection regimes, placing data regulation at the intersection of fundamental rights protection, economic development, technological innovation, and state sovereignty.

However, despite growing global attention to these issues, much of contemporary legal research on personal data protection remains narrowly focused on textual analysis of

recent regulations (Javed & Sajid, 2024) such as the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or Federal Law of Russia No. 152-FZ "On Personal Data." While these documents provide the necessary regulatory framework, an exclusive focus on their content risks leading to a fragmented and superficial understanding of how personal data protection systems function in practice (Zaguir et al., 2024). This approach often ignores the deeper legal, institutional, and philosophical foundations that shape legislative decisions, enforcement mechanisms, and judicial interpretation in various legal systems (Ding et al., 2025). Therefore, a meaningful assessment of the effectiveness of data protection regimes requires not only an analysis of current regulations but also an examination of their historical development. This long-term legal and political evolution helps explain why different regions respond differently to similar digital challenges and why even large-scale reforms often fail to change the underlying structural logic of a given system.

In light of this, this dissertation proceeds from the premise that the effectiveness and sustainability of personal data protection regimes cannot be adequately assessed without considering their historical evolution. Modern data protection systems are not entirely new legal constructs. Rather, they represent adaptive responses rooted in earlier legal traditions, constitutional principles, and institutional mechanisms developed before the digital age. The persistence of regional differences in personal data regulation, despite technological convergence and globalisation, suggests that these systems are built on historically entrenched legal frameworks that continue to shape regulatory reform. Understanding why some models prioritise individual autonomy, others emphasise the sectoral nature of enforcement, and still others adopt state-centric or security-focused approaches requires a historically informed and comparative approach.

With this focus, this dissertation offers a comparative legal analysis of the formation and development of personal data protection systems in the United States, Russia, and Europe. These jurisdictions reflect distinct legal traditions and regulatory models: a decentralised and sectoral structure in the United States, a hybrid system characterised by significant state involvement in Russia, and a harmonised regime based on the protection of fundamental human rights in Europe. A comparative analysis of these systems allows us to identify both structural differences and common conceptual

foundations, and to assess their strengths and weaknesses in addressing contemporary data protection challenges.

The relevance of this study is supported by both doctrinal and empirical considerations. Existing scholarly works reveal a significant lack of historically grounded comparative studies tracing the continuity of data protection concepts from their philosophical and legal origins to their contemporary institutional manifestations. Moreover, although legislative provisions are often compared, significantly less attention is paid to the practical application of legal norms through judicial interpretation and regulatory action. This dissertation aims to fill these gaps by integrating legislative analysis, case law, supervisory practice, and expert commentary into a unified analytical framework.

The choice of research topic is also informed by the author's academic and professional experience. With a Bachelor of Laws degree specialising in both Russian and international law, the author approaches legal issues from a comparative perspective, viewing cross-jurisdictional analysis as a key tool for identifying effective legal solutions. This approach is underpinned by four years of professional experience as a legal consultant in the real estate sector, where compliance with personal data protection legislation has become a critical operational and strategic challenge. Ongoing engagement with data protection compliance issues, as well as organising corporate seminars on the development of Russian personal data protection legislation, revealed the practical implications of abstract legal frameworks and emphasised the need for a deeper theoretical understanding of their origins and limitations. Beyond its professional significance, personal data protection is an enduring area of academic interest that the author intends to develop in future PhD research, including by extending the comparative analysis to the Asian legal context.

Methodologically, the dissertation employs a historically grounded comparative legal approach. It explores the evolution of personal data protection from the 18th and 19th centuries to the present, combining a diachronic analysis of legal development with a synchronic assessment of contemporary regulatory frameworks. The study draws on Constitutional provisions, legislative norms, judicial decisions, regulatory practices, and institutional structures to assess personal data protection as an integrated legal system rather than a collection of individual legal norms.

This dissertation reflects this analytical framework. Chapter one presents the theoretical and methodological foundations of the study, including a review of the relevant literature, identification of existing research gaps, and formulation of the research questions and objectives. Chapter two analyses the development of personal data protection in the United States, tracing its evolution from early privacy doctrines to the modern sectoral and law-enforcement-oriented model. Chapter three focuses on Russia, examining the transition from Soviet approaches to the post-Soviet regulatory system shaped by international obligations and state-oriented governance. Chapter four examines the European model, emphasising the recognition of data protection as a fundamental right and the development of a harmonised regulatory regime, culminating in the GDPR, which continues to evolve. Chapter five summarises the results of the comparative analysis, assessing the impact of historical continuities on the effectiveness of modern data protection regulation. The dissertation concludes with an assessment of which model provides the highest level of personal data protection when considered as a comprehensive legal system, and outlines areas for future research.

The primary goal of this dissertation is to demonstrate that more effective and sustainable personal data protection systems can only emerge through a critical comparative analysis of different legal traditions. By identifying successful regulatory practices and institutional mechanisms across different jurisdictions and examining their historical foundations, the study aims to contribute to the development of more balanced, context-sensitive approaches to personal data protection in an increasingly interconnected digital environment.

Chapter 1. Theoretical and Methodological Framework

1.1 Literature review

Academic debates about personal data protection have their origins in broader discussions about the right to privacy. The earliest theoretical foundations are usually associated with Warren and Brandeis' seminal article "The Right to Privacy" (1890), which conceptualised privacy as "the right to be let alone." The authors viewed privacy primarily as protection against intrusion, a view that strongly influenced early legal doctrines in common law jurisdictions. Although this conception did not address data processing and protection per se, it established privacy as a legally recognised interest deserving protection.

Building on these early foundations, the second half of the 20th century saw privacy theory evolve in response to the growing use of information technology and data processing. Prosser (1960) systematised privacy violations into four categories of harm, providing a more operational legal framework. Subsequently, Westin (1967) expanded on the concept by defining privacy as an individual's ability to control the collection, use, and dissemination of personal information. This concept of informational self-determination proved fundamental to early data protection regimes and served as the basis for international documents such as the Council of Europe Convention 108 (1981).

Moving beyond these frameworks, subsequent research has questioned overly abstract or control-based definitions of privacy. Solove (2006; 2008), for example, criticised the conceptual vagueness of traditional theories and proposed a pragmatic taxonomy of privacy harms based on concrete data practices. This approach shifted attention from philosophical definitions to regulatory responses to the actual processes of data processing, storage, and protection.

At the same time, critical social theory introduced a structural perspective on the control of data and information. Foucault's analysis of surveillance and disciplinary power (1975) emphasised how information systems function as mechanisms of social control. Building on this tradition, Lyon (2001; 2014) conceptualised surveillance as a defining feature of modern societies, emphasising institutional power asymmetries rather than individual consent. These views have had a significant influence on contemporary

critiques of data protection law, particularly regarding the limitations of consent-based regulation in the context of systemic data collection.

Taken together, these theoretical perspectives—including liberal privacy theory, informational self-determination, pragmatic harm-based approaches, and critical surveillance theory—form the conceptual foundation of contemporary data protection law. Their continued coexistence helps explain both the internal contradictions within current regulatory frameworks and the diversity of legislative responses observed across jurisdictions.

By shifting the focus from broad theoretical debates to national contexts, academic research on personal data protection in the United States highlights the lack of a comprehensive federal privacy protection framework. Scholars widely characterise the U.S. system as fragmented, sector-specific, and enforcement-focused (Schwartz & Solove, 2011). Much of the literature debates whether this fragmentation represents a failure of regulation or a deliberate preference for flexibility, innovation, and market solutions.

Recently, academic research has increasingly focused on state-level developments, particularly the California Consumer Privacy Act (CCPA) and its successors, and has assessed their potential convergence with European standards. However, comparative studies often evaluate the US model primarily through the lens of the GDPR, implicitly viewing the European approach as a normative benchmark. This tendency risks oversimplifying the US system and underestimating the historical, philosophical, social, constitutional, and institutional factors—such as the primacy of economic freedoms, the role of tort law, and ex post facto enforcement mechanisms—that continue to shape US data protection policy.

Turning to the Russian context, the academic literature on personal data protection remains limited and unevenly accessible to the international scholarly community because it is published in Russian. Russian-language studies typically focus on compliance with international instruments, particularly Convention 108, while also emphasising data localisation, state control over information flows, and national security considerations. Data protection is often considered alongside broader discussions of sovereignty, governance, and state capacity.

While some comparative studies analyse the formal compliance of Russian legislation with European standards, far fewer studies critically examine how Soviet legal traditions, centralised administrative control, and post-Soviet institutional transformations have influenced contemporary approaches to regulation. As a result, Russian data protection legislation is often portrayed as a deviation from European norms, rather than as a system shaped by its own historical and institutional logic. This limits the explanatory depth of existing comparative analyses.

In contrast, European legal scholarship has traditionally viewed the protection of personal data as a fundamental right, closely linked to human dignity and privacy. Authors such as Bygrave (2014), González Fuster (2014), and De Hert and Gutwirth (2009) emphasise the constitutionalization of data protection within the EU legal system, particularly since the adoption of the Charter of Fundamental Rights of the European Union (2000). The adoption of the General Data Protection Regulation (GDPR) has sparked extensive academic debate regarding its regulatory structure, enforcement mechanisms, accountability requirements, and extraterritorial scope (Voigt & von dem Bussche, 2017). Most studies adopt a doctrinal perspective, focusing on issues of interpretation and implementation. While historical continuity with earlier European data protection instruments is often acknowledged, it is rarely examined in detail as a structuring factor shaping contemporary regulatory decisions.

Methodologically, the literature on personal data protection can be divided into three dominant approaches. First, doctrinal legal analysis remains the most common, particularly in studies of the GDPR and national implementing legislation. Although essential for understanding legal norms, this approach often pays limited attention to enforcement practices and institutional behaviour. Second, comparative studies often employ a synchronic perspective, comparing regulatory frameworks at a fixed point in time. While such analysis is useful for identifying formal differences, it often ignores historical evolution and dependence on prior development. Third, interdisciplinary studies often lack detailed legal analysis, limiting their applicability to legal system design and reform. The absence of a systematic, historically grounded comparative methodology that integrates legal doctrine, institutional development, detailed legal analysis, and threat perception represents a significant gap in the literature.

Despite the breadth of scholarly work, several critical gaps persist in the literature on personal data protection. First, comparative studies rarely consider modern data protection regimes as the result of long-term historical and institutional evolution. Second, Russian data protection legislation is underrepresented in comparative analyses and is rarely considered on an equal analytical footing with US and European systems. Third, although economic risks and national security concerns are frequently mentioned in the literature, they are rarely analysed as factors that determine threat perceptions and influence regulatory development over time. Addressing these gaps will provide a more accurate understanding of why fundamentally different regulatory models persist despite technological convergence and increased international coordination.

1.2 Thesis statement

The evolution of personal data protection systems in the United States, Russia, and Europe is the result of a long historical development, where the key principles and institutional approaches were laid down long before the advent of modern privacy laws. Regional differences in personal data protection are not driven by current political or technological factors, but by fundamental legal traditions, human rights concepts, government structures, and historical precedents (Kohl, 2023; Phang & Kaabi, 2025). Despite new challenges, such as cyber threats, national security, and digital technologies, current reforms merely adapt existing models rather than fundamentally change them. Comparative analyses, for example, Lim and Oh (2025) show that the security and effectiveness of personal data protection are determined by the integrity of the entire legal system, from the original concepts of the 18th and 19th centuries to modern judicial practice and practical guidelines, and not merely by the text of current laws.

1.3 Gap in the literature

Despite the extensive body of research in the field of personal data law and regulation, there are several significant gaps that this paper addresses:

1. Insufficient historical and legal analysis. Most comparative studies focus on contemporary regulations, ignoring their deep historical roots. There are virtually no works that systematically trace the development of approaches from the 18th and 19th

centuries to the present day, analysing the continuity of ideas and institutions. Some specialists, for example, Ruihua (2025), state that research often treats legislation as a static norm, ignoring judicial practice, regulatory commentary, supervisory guidance, real-world cases of norm application, and expert assessments—that is, the actual mechanisms by which the system functions.

2. Within comparative scholarship focusing on the United States, Russia, and Europe the academic literature lacks a comprehensive theory explaining the resilience of distinct regional data-protection models despite global challenges, technological pressures, and economic integration.

3. Within legal scholarship, analyses of data-protection "security" remain largely doctrinal and comparative. Legal researchers rarely attempt to assess which system provides a higher overall level of data protection, often focusing on statutory design rather than the effectiveness of mechanisms, institutional practices, or their long-term sustainability.

1.4 Aim of the study

The purpose of this study is to conduct a historically grounded comparative analysis of the legal, institutional, and judicial frameworks for personal data protection in the United States, Russia, and Europe. The study aims to determine the extent to which these systems have developed to effectively ensure the right to personal data protection and to determine which regional model demonstrates the highest level of protection in both historical and contemporary contexts.

1.5 Research question

The main research question is:

- Which regulatory model provides the most effective protection for personal data when assessed as a comprehensive legal system rather than merely as a set of formal rules?

The supporting research questions are:

- How have historical legal traditions and institutional structures shaped contemporary data protection regimes in the United States, Russia, and Europe?
- Why do fundamentally different regulatory models persist despite technological convergence and increasing international coordination?
- To what extent do underlying threat perceptions influence legislative development, enforcement mechanisms, and judicial interpretation in data protection law?

1.6 Object and subject

This study examines the legal, institutional, and judicial systems governing personal data protection in the United States, Russia, and Europe. It examines the evolution, structure, and practical functioning of legal, regulatory, and judicial mechanisms ensuring the protection of personal data within these three regional models.

1.7 Objectives of the study

To achieve this goal, the study pursues the following objectives:

1. To trace the historical evolution of personal data protection concepts and institutions in the United States, Russia, and Europe from their inception to the present day.

2. To analyse the development of the main legal approaches to personal data protection and privacy in each region, identifying the fundamental principles, political factors, and legal traditions that influenced their development.

3. To examine contemporary legal frameworks, including legislative norms, constitutional guarantees, regulations, case law, and enforcement mechanisms, to understand how each system functions in reality.

4. To identify the degree of continuity between historical developments and contemporary regulatory models, demonstrating how early legal and philosophical foundations continue to influence contemporary approaches.

5. To compare the effectiveness and reliability of the United States, Russian, and European systems in ensuring personal data protection, drawing on legal analysis, case law, expert commentary, and actual law enforcement practice.

6. To determine which of the three regional models provides the highest level of personal data protection when viewed as a comprehensive system rather than through the lens of individual laws.

1.8 Research Design

This study utilizes a qualitative and historically informed comparative design to analyse the long-term evolution of personal data protection systems in the United States, Russia, and Europe. The study is structured around a cross-jurisdictional comparison that examines how each region's legal and institutional approaches have evolved over time and how these trajectories have shaped contemporary data protection regimes. The design integrates both diachronic and synchronic dimensions: diachronic, tracing the development of privacy and data protection concepts from their early intellectual and legal origins in the 18th and 19th centuries to the present day; and synchronic, assessing the current structure and functioning of each system as of 2025.

The comparative research architecture is built on an analysis of three different models: the U.S. sectoral regulation, the European system based on fundamental rights, and the Russian hybrid state-centric model. Each model is examined through the same analytical lenses: historical foundations, legislative frameworks, institutional structures, judicial and administrative practice, and actual law enforcement practice. The overall concept of the study deliberately goes beyond a static textual comparison of laws and seeks to view each system as an evolving structure, dependent on previous developments, shaped by political, legal, and institutional factors. This concept allows the study to answer the central question: which model provides the highest level of protection when viewed as a holistic system, rather than simply as a set of contemporary laws.

1.9 Methodology

This research utilises a methodology that combines several complementary legal and analytical methods to provide a comprehensive understanding of the evolution and functioning of three distinct data protection systems.

1. Comparative Legal Method

The primary method is a comparative legal analysis of the US, Russian, and European systems. This includes a comparison of legislative norms, constitutional principles, institutional competencies, regulatory frameworks, and enforcement mechanisms. This method is used to identify both structural similarities and differences between the three models.

2. Historical-Legal Method

Building on the legal-historical approach developed in my previous work and inspired by the traditions of historical jurisprudence and comparative legal history, this study uses a legal-historical method to examine the long-term development of approaches to data protection. Methodologically, it follows the logic of legal-historical analysis formulated by Wieacker (1995), which emphasizes the importance of tracing the continuity of legal concepts, institutions, and normative structures over time, rather than analyzing legal norms in isolation. This approach is complemented by González Fuster's (2014, 2022) genealogical analysis of personal data protection, which demonstrates how contemporary data protection regimes are rooted in earlier legal, philosophical, and constitutional traditions. Together, these perspectives allow us to view data protection as a historically rooted legal institution, rather than as a purely modern or technologically driven normative response.

3. Doctrinal and Legal Analysis

The study conducts an in-depth analysis of legal texts, including constitutions, statutes, regulations, guidelines, commentaries, and treatises. This doctrinal method helps clarify how laws are interpreted, how concepts are defined, and the normative foundations underlying each regional approach.

4. Judicial Analysis

Judicial practice is studied to understand how rights are interpreted and applied in practice. This includes decisions of courts of various levels (from the supreme courts to lower courts) in the United States, Russia, and Europe. Judicial analysis is necessary to assess the actual, rather than purely textual, level of protection.

5. Regulatory and Institutional Practice Analysis

The methodology includes a study of decisions, reports, and enforcement guidance from key supervisory authorities, such as the Federal Trade Commission (FTC), the European Data Protection Board (EDPB), and Roskomnadzor. This provides insight into the functioning and effectiveness of enforcement mechanisms.

6. Expert and Academic Analysis

This study analyses academic literature, expert commentary, and policy analysis to contextualize legal changes, interpret key controversies, and assess the effectiveness of various regulatory models.

Taken together, these methods allow for a multidimensional assessment of personal data protection systems, allowing the study to go beyond legislative acts and assess the full systemic functioning of each model in both historical and contemporary contexts across three different regions.

Chapter 2. Formation and development of the right to personal data protection in the U.S.

2.1 Early legal and philosophical foundations of the U.S. personal data protection before 1974

2.1.1 The formation of the U.S. personal data protection framework from implicit privacy to explicit data protection

The emergence of personal data protection in the United States can be traced back to the adoption of the Constitution of 1789. Although the right to privacy was not explicitly stated, the Supreme Court later grounded it in several constitutional amendments (specifically the First, Third, Fourth, and Fifth Amendments), adapting foundational legal principles to address evolving privacy risks. This understanding developed from the English common law notion that a person's home is his or her castle (University of Michigan Information and Technology Services, 2025). The development of technologies such as the telegraph and Morse code in the 19th century sharply increased both the opportunities and threats to privacy, compelling lawmakers and society to reconsider and expand traditional protections (Clarip, 2026). Early solutions, including confidentiality agreements and message encryption, set critical precedents, laying the groundwork for modern approaches in personal data regulation. The invention of the telegraph led to an intensified debate in Congress about "whether telegrams should be given the same privacy protection as letters." (Solove, 2006) Thus, telegraph messaging became a "brand new concept," unleashing a wave of previously unknown privacy concerns (McMullan, 2015). Along with the emergence of such innovative technology, fundamental risks of privacy invasion also arose: telegraph operators read and transmitted other people's messages; telegraph companies could store, copy, or disclose the contents of telegrams. The state began requesting access to telegraph messages for investigations, and telegraph lines could be tapped and signals intercepted. Cable workers were required to sign confidentiality agreements, but even they could be bribed to divulge messages. Thus, a person's personal information ended up in the hands of third parties and was transmitted in digital (encoded) form. Initially, a certain level of privacy existed because users had to understand Morse code to read telegraph messages,

but later users began encrypting their messages using ciphers to further protect them and limit eavesdropping (McMullan, 2015; Clarip, 2026).

In the late 19th century, the core of US privacy law emerged as lawyers and philosophers defined the main argument for personal data protection: safeguarding the individual's autonomy amid technological advances. The pivotal 1890 article by Warren and Brandeis reframed privacy as a vital right interconnected with modern life, justifying legal recognition of personal data protection as a crucial extension of this right. Their work established the foundation for treating personal information as needing robust legal protection against evolving threats, and is considered the first milestone in the history of privacy in the USA (Palmer, 2011). However, certain elements of protection already existed in American judicial practice before this, and even the phrase "right to be let alone" had already been uttered by Thomas Cooley (Cooley, 1888). In the Harvard Law Review, Judge Louis Brandeis and a lawyer, Samuel Warren, first used this term and asked whether the then-existing law could properly be applied to protect an individual's privacy. They directly addressed how new communication technologies (including the telegraph, telephone, and camera) threatened privacy (Solove, 2006). Warren and Brandeis (1890) presented this right as a unifying theme to various common law protections of the "right to be left alone," including the developing laws of nuisance, libel, search and seizure, and copyright. According to the authors, "the right to life has come to mean the right to enjoy life,—the right to be let alone... This development of the law was inevitable... Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterises the common law enabled the judges to afford the requisite protection, without the interposition of the parliament." Moreover, Warren and Brandeis (1890) emphasize that "instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life," meaning that our "intense intellectual and emotional life" also requires guarantees of legal protection and sanctions for its breaking.

In the first half of the 1900s, there was a gradual formation of the institution of personal data protection: in order to protect it, in 1914, the Federal Trade Commission (FTC), a specialized body, was created in the United States based on The Federal Trade

Commission Act (FTCA), which, in addition to the establishment of such a body, also prohibited unfair or deceptive commercial practices (Federal Trade Commission Act, 1914). Although not immediately, by the late 1960s, the FTC began to play a key role in privacy, regulation, and enforcement in the field of personal data protection (Conolly-Smith, 2009).

During the mid-20th century, public concern over privacy intensified as Americans perceived a growing threat from widespread surveillance and data collection. A series of books and reports starkly revealed the breadth of data collection by both public and private entities, exposing the scale of dossiers maintained on ordinary citizens: The Eavesdroppers (1959), Privacy: The Right to Be Let Alone (1962), The Privacy Invaders (1964), The Naked Society (1964), The FBI Nobody Knows (1964), The Intruders (1966), Privacy and Freedom (1967), The Death of Privacy (1969). This growing unease crystallized the need for robust personal data protection law, connecting social anxiety over data banks with clear legislative urgency. As Igo (2015) points out, areas of private life subject to surveillance and spying "seemed limitless, and the threat emanated not from one specific direction but from every corner of American society." The government and the military, corporations and workplaces, universities and hospitals, the media and marketers—all without exception were "intruders." For Senator Edward Long (1967) of Missouri, this amounted to "an undeclared war on privacy." Public anxiety is beginning to coalesce more and more around the specter of the "data bank," a term defined by New Scientist and Science Journal in 1971 as a "generalized collection of data not linked to one set of…questions" (Malik, 1971). The 1966 survey estimated that the government possessed "more than 3 billion records on individuals, including 27.2 billion names, 2.3 billion addresses, 264 million criminal histories, 280 million mental health records, 916 million profiles on alcoholism and drug addiction, and 1.2 billion financial records" (United States Congress, 1967). As a Life magazine writer wrote in 1964: "Most Americans who have served in the armed forces, taken out mortgage purchases or insurance, made large purchases on credit or worked in defence industries know that, somewhere, dossiers on them are maintained. But few people have any notion of the extent of this dossier-keeping or of the number of facts (and gossip and lies) on file…on virtually every adult US citizen" (Wallace, 1964).

The next key milestone in the development of privacy law was the article "Privacy" by the well-known legal scholar Prosser (1960), in which he outlined four offences that violate a person's privacy, one of which is to sue the violator for damages. He names the following violations: "Intrusion upon seclusion or solitude, or into private affairs; public disclosure of embarrassing private facts; publicity which places a person in a false light in the public eye; and appropriation of one's name or likeness." Thus, the nature of the right to the protection of personal data begins its active development, not only as a human right but also as a guarantee that the violator can be held accountable for the damage caused (Palmer, 2011).

Until the mid-20th century, personal data was mainly stored in paper archives, limiting risks. However, with advances in computerization, especially in the 1960s, businesses and government agencies began storing and processing data at unprecedented scales. These changes heightened the central legal challenge: ensuring that increasing data collection did not undermine individuals' rights. In response, the US Office of Management and Budget proposed creating a centralized database to consolidate information on all citizens, reducing costs and simplifying management. In response, Senator John McCarthy introduced the "Bill of the Computer and the Rights of Citizens" in 1966, which proposed enshrining citizens' rights to know what data is collected about them and to correct errors in that data. It marked a clear turning point, shifting the legal debate from technical data management to the fundamental protection of personal rights in the digital age.

2.1.2 Institutionalization of the U.S. personal data protection (1960–1974)

Although not initially conceived as a theory of personal data protection, Alan Westin's Privacy and Freedom was later retrospectively identified as a foundational contribution to the modern understanding of privacy and personal data protection in the United States (González Fuster, 2014). In this context, "privacy" refers to what Westin (1960) defined as "the claim of individuals … to determine for themselves when, how, and to what extent information about them is communicated." In this framework, any information a person considers confidential is confidential. "Personal information," as discussed in the article, is defined as information that is both true (not defamatory or false) and confidential, such as health, salary, or sexual orientation (Pazyuk & Sokolova,

2015). This article is seen as the institutional birth of the American concept of data protection (Harrington, 2015). Westin also introduced the concept of the "electronic shadow,"—the countless electronic records about each person stored in systems such as banking, insurance, medical, and government. Westin was first to show that data is an extension of one's personality; that control over it is a civil liberty; and that losing control threatens democracy and privacy (Westin, 1960). In March 1968, Westin testified before Congress, warning about uncontrolled credit bureau data collection, errors that could harm reputations, and the need to restrict the use of personal data (U.S. Congress, 1968). His arguments influenced the Fair Credit Reporting Act (1970), the first US federal law regulating private-sector personal data (Garfinkel, 2004).

At the same time as Westin's influential work, according to Andruss (2022), many government agencies (such as Social Security, Medicare, and Medicaid) were already collecting and storing vast amounts of personal data to provide essential services to Americans. Recognizing the need to securely collect, store, preserve, and use this data for the purposes for which it was collected, they began developing fundamental frameworks to assess the risks associated with data storage and use. To this end, the US Department of Health and Human Services developed the Initial Privacy Impact Assessment (IPIA) to identify data-related risks, and such assessments have become standard practice for measuring the impact of data collection on individuals (U.S. Department of Health and Human Services, 2025).

By the late 1960s and early 1970s, public and scholarly awareness of the risks of digital surveillance and their link to civil liberties was increasing. For instance, in 1970, Malcolm Warner and David Stone, a behavioral scientist and a computer scientist, respectively, noted that organisations now had "the technical power available" to implement George Orwell's "chilling vision of a society under surveillance and control" (Warner & Stone, 1970). In line with these concerns, several surveys showed that the public was becoming increasingly aware of the privacy threats posed by computer databases. For example, a 1971 survey reported that 53 percent of respondents believed that "computerized information files might be used to destroy individual freedoms," and 58 percent thought that "computers will in the future be used to keep people under

surveillance" (American Federation of Information Processing Societies & Time, Inc, 1971).

In the 1970s, a special group of data concerning the private lives of specific individuals emerged from the vast amount of processed information. This data was collected, processed, stored, and disseminated by various organisations, services, and individuals. This information became known as "personal information," "personal data," or "personal information." As a result, the problem of legally protecting personal data was first formulated in the United States (Pazyuk & Sokolova, 2015).

Legislative recognition of citizen rights in personal data processing shifted as criticism and public pressure mounted. This shift was motivated by growing criticism (particularly Packard's 1967 article "Don't Tell It to the Computer") and concern over the large-scale monitoring and exploitation of personal data by governments and corporations (Packard, 1967). Congressional hearings and public pressure led to the development of privacy safeguards, marking a foundational shift: the US Congress held hearings on the risks of privacy invasion, and the Subcommittee on Invasion of Privacy recommended suspending the project until data protection safeguards were developed, thus beginning the development of privacy principles applicable to automated databases. However, concerns about individual control over personal data were articulated by sociologists such as Baker (1973), who argued that "ownership and control" of "record identities" rested primarily with organisations, not individuals." He explained that the individual in such systems was conceived of as an object rather than as a "citizen-with-rights," and was therefore "a poor candidate for self-protection where record privacy problems are concerned." Baker (1973) pinpointed the tremendous mismatch between the capacity of the record system and the citizen's ability to keep track of even personal data. On these grounds, Baker (1973) believed that solutions would "have to be accomplished primarily for, not by, the individual..."

Later, the creation of personal data protection institutions accelerated with proposals such as Elliott Richardson's Advisory Committee on Automated Personal Data Systems (1970–1972), which led to the Code of Fair Information Practices. The landmark 1973 Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems was developed by the Department of

Health, Education, and Welfare (HEW) Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS) (United States. Congress. House. Committee on Government Operations. Special Subcommittee on Invasion of Privacy, 1966). These FIPPs codified early policy thought on privacy and data protection before any official legislation was formed. It is the first systematic set of principles for the protection of personal data, which served as the basis for future legislation. It was then that the concept of "Fair Information Practices" was born, becoming the true foundation of all modern US personal data legislation (Gellman, 2025). The Code of Fair Information Practices (1973) defined the following principles: (1) No secret records — there should be no secret databases of personal data; people should know what data is being collected about them. (2) Access — individuals should be able to find out what information about them is stored and how it is being used; citizens should have access to their own information. (3) Use limitation — data collected for one purpose cannot be used for another without consent; data cannot be used for other purposes without consent. (4) Participation — individuals have the right to correct or supplement their own information; error correction mechanisms must be in place. (5) Data quality/security — organisations are required to ensure the accuracy and security of data, and organisations collecting data are responsible for its protection.

By 1977, further refinement of Fair Information Practice Principles occurred through the Privacy Protection Study Commission report, which added new principles (Privacy Protection Study Commission, 1977): (6) Collection restrictions — organisations must not collect excessive data. (7) Use and disclosure restrictions — data must not be distributed or used for purposes other than those stated. (8) Accountability — organisations must be transparent in their policies and disclose to the public how data is processed.

The 1973 Report established the framework for Fair Information Practice Principles (FIPPs), which became central to subsequent privacy laws in the US and globally. These principles subsequently became the core of the entire system of Fair Information Practice Principles (FIPPs), which later form the basis of the Privacy Act (1974), American industry regulations (HIPAA, COPPA, Gramm-Leach-Bliley), as well as international standards: the OECD International Guidelines for data protection (1980);

the EU Directive 95/46/EC (1995); and the GDPR (2016), which directly dates back to the American principles of the 1970s. Thus, Westin's concept of the "electronic shadow" transformed the problem of technical automation of data into a socio-legal category and laid the foundation for the formation of a legal institution to protect personal data in the United States (Garnett, 2014; Eskens et al., 2016). Moreover, thanks to his work, the perception of privacy changed: from the "private sphere of the individual" to control over information about oneself (Westin, 1968).

Subsequent privacy legislation expanded rapidly in the years following these foundational steps. Even though there still was not a codified act guaranteeing data protection, there was a continued trend towards industry-specific laws addressing data privacy issues. For instance, in 1974, the Family Educational Rights and Privacy Act (FERPA), also known as the Buckley Amendment, was enacted, a federal law that safeguards the privacy of student education records. This law still applies to all educational organisations, from schools to universities, that directly receive funding from the US Department of Education (U.S. Department of Education, 2000). It provides parents and students with the right to inspect their information, request corrections, and control the disclosure of some personally identifiable information (Family Educational Rights and Privacy Act of 1974, 1974).

In this way, it is possible to state the US legislation has recognized privacy in a heterogeneous manner, and the institution of data protection has gradually developed, based on the philosophically rooted principle of the "right to be let alone" (Warren & Brandeis, 1890) and the concept of freedom, and on the Fourth and Fourteenth Amendments of the Constitution as a legal basis. Throughout this time, there was no general law or clearly formulated constitutional provision on "data protection", but the Warren-Brandeis approach and the developing case law paved the way for subsequent legislative action, namely the adoption of the Privacy Act in 1974, which would become a turning point in the development of the institution of personal data protection (Covington & Burling, 1974).

2.2 Evolving policy landscape: data protection in the U.S. from the 1974 to the 2020s

2.2.1 From Watergate to the Privacy Act of 1974: a milestone in the U.S. federal data protection.

The evolution of privacy law and data protection in the United States during the 1970s and 1980s was shaped by technological advancements and significant political scandals, most notably the Watergate scandal. The proliferation of large-scale electronic databases in both government and private sectors has transformed information storage and processing. The exposure of the Nixon administration's illicit surveillance and unauthorized collection of personal data during the Watergate scandal (1972–1974) revealed the vulnerability of citizens to governmental abuse. This convergence of political misconduct and technological change eroded public trust and highlighted the urgent need for comprehensive legal protections to safeguard privacy and prevent data misuse by both governmental and private actors (Boyne, 2018).

In 1974, President Nixon publicly addressed privacy concerns, stating: "As technology has advanced in America, it has increasingly encroached on... the right of personal privacy. Modern information systems, data banks, credit records, mailing list abuses, electronic snooping, the collection of personal data for one purpose that may be used for another — all these have left millions of Americans deeply concerned about the privacy they cherish (Brady, 2007). The time has come for a major initiative to define ... privacy and to erect new safeguards to ensure those rights are respected... We will make a historical beginning on the task of defining and protecting the right of personal privacy for every American" (Nixon, 1974; Hughes, 2023).

The US Congress enacted the Privacy Act of 1974 after technological advances and political abuses heightened public concern about privacy. This was especially evident following the Watergate scandal (Boyne, 2018). The Act established privacy as a legally protected right. It marked a major shift in US policy by positioning data protection as both a civil rights safeguard and a regulatory tool for emerging technologies. The law served two main purposes: protecting civil liberties and overseeing technological development.

The Privacy Act of 1974 aimed to address fears about personal data privacy and the growing use of computers and Social Security numbers as federal identifiers. Its main goal was to create a Code of Fair Information Practice to guide federal agencies in collecting, maintaining, using, and sharing personal information. Called the "American Bill of Rights on data," (Zang, 2024), the Act was driven by widespread fears about government surveillance. Congressional hearings, reports, and scandals like Watergate and Counter Intelligence Program exposed illegal surveillance and increased public distrust. Congress moved to restore confidence by limiting what information federal agencies could collect about individuals (U.S. Department of Justice, Office of Privacy and Civil Liberties, 2020). Senator Sam Ervin argued that Watergate proved the necessity of limits on government access. President Nixon, as noted by Zweifel-Keegan (2024), publicly endorsed privacy rights to rebuild trust.

The law lets citizens know what data the government collects and allows them to request corrections. Agencies must keep this data secure and use it properly. Main impacts include: (1) agencies must publish any "system of records" with personal data; (2) collect records only for lawful, relevant purposes; (3) allow people to access and amend their data; and (4) require consent before using data for unrelated purposes. The Privacy Act (1974) restricts sharing records without written consent (5 U.S.C. § 552a(b)). Some exceptions allow use for routine activities, archives, law enforcement, and congressional investigations.

Igo (2015) argues that, though the Privacy Act was meant to empower citizens, its value for privacy rights is unclear. Ironically, it increased fears of a surveillance society. The case *Doe v. Chao* shows this: the Supreme Court interpreted the Privacy Act to limit damages for rights violations (*Doe v. Chao,* 2004). The Act provides rights to see and amend records, get notifications of use, limit disclosures, and seek recourse for willful violations (U.S. Department of Justice, Office of Privacy and Civil Liberties, 2020). However, *Doe v. Chao* revealed important limits to these protections. The Act also requires agencies to state the authority for requesting information and whether disclosure is mandatory or voluntary (5 U.S.C. § 552e). So, while citizens have mechanisms for access and corrections, limits in case law reduce the law's power.

Angwin (2025) says that, though groundbreaking, the law was heavily criticized early on. Critics argued that it applied only to federal agencies and lacked the teeth for enforcement. The United States still lacks a data protection agency to enforce privacy laws. Iga (2015) notes that the law ignored massive data collection by private employers, banks, insurers, telecom companies, and marketers. Myron Brenton called this threat "Big Brother in civilian clothes" (Brenton, 1964). Iga (2015) says the Act's authors wanted broader privacy protection, but this did not happen. The U.S. Privacy Protection Study Commission, created in 1974, was meant to review the Act and make recommendations (U.S. Congress, 1975). When it considered expanding the Act, those efforts failed (Iga, 2015).

A main criticism of the Privacy Act is that it excludes non-U.S. citizens without permanent residency. This affects the exchange of passenger ticket data with the EU (Statewatch, 2012). Zang (2024) says courts have weakened the Act by requiring claimants to prove "actual harm," not reputational or emotional damage. Renewed scrutiny followed President Trump's 2017 executive order, which removed ADA protections for foreign nationals. Section 14 of the "Enhancing Public Safety" order told agencies to exclude non-citizens and non-residents from Privacy Act protections for personal information, when permitted by law (Burgess, 2017).

The main argument centers on the Privacy Act's enduring foundational influence despite criticisms that it is outdated. Although the Act was amended in 1988 to extend its reach, its core terms remained intact, leading to claims that it cannot address evolving technological and societal changes. Yet, the Department of Justice contends that the Act's "basic principles of fair information practices" have maintained public trust in government for over 45 years (U.S. Department of Justice, Office of Privacy and Civil Liberties, 2020). The DOJ further explains that, while later statutes such as the E-Government Act (2002) and FISMA (2014) supplemented the Act, its original language has proven adaptable. Furthermore, the Act's core principles of transparency, access, and consent have informed subsequent U.S. and international privacy laws, providing a durable framework for protecting personal data (U.S. Department of Justice, Office of Privacy and Civil Liberties, 2020). For example, the Gramm-Leach-Bliley Act (1999) and HIPAA Privacy Rule (1996) both draw on these concepts. In sum, the

Privacy Act of 1974 has shaped U.S. policy and established a lasting national "privacy framework" (U.S. Department of Justice, Office of Privacy and Civil Liberties, 2020).

2.2.2 Patchwork privacy: the evolution of sector-specific privacy regulation in the U.S. (1974–2000s)

The Law Institute (2023) in its research observes that, following the enactment of the Privacy Act of 1974, personal data protection in the United States evolved into a patchwork of sector-specific laws and regulations. As the Privacy Act applied exclusively to government records, U.S. privacy policy became sectoral after 1974, with each law addressing a distinct area. The main argument is that this sectoral approach, originally intended to guarantee privacy and give individuals more control over their data, has raised persistent concerns about whether these protections are sufficient during the collection, processing, and storage of personal data. The prevailing view is that the sectoral system creates inconsistencies and gaps in privacy protections.

Igo (2015) observes that efforts to increase transparency in personal records often resulted in more data being created. Miller (1970) called the US a "surveillance society," due to the systematic collection and analysis of personal data. After the 1974 Privacy Act, the Los Angeles Times reported large-scale government monitoring, describing an unprecedented scope and giving examples like lists of New Jersey driving examiners, Kentucky tollbooth operators' performance, and Cincinnati firemen's hearing tests (Igo, 2015).

In the 1970s and 1980s, Congress passed laws to address privacy concerns (Bhoumik, 2005). The Fair Credit Reporting Act (1970) required credit-reporting services to ensure data accuracy but did not restrict data collection. The 1984 Cable Communications Policy Act limited monitoring risks from interactive cable systems, prohibiting the collection of personal data without consent, except as needed for service or to stop interception. Amendments to the Electronic Communications Privacy Act (1986) modernized wiretap laws to cover e-mail and cellular calls, but did not grant a broad privacy right for such communications, and allowed data collection unless expressly refused. The Video Privacy Protection Act of 1988 barred the disclosure of video rental records but permitted the sharing of names and addresses for marketing unless the

consumer objected (Mukherjee & Samarajiva, 1993). These laws reflect a sectoral approach, resulting in unequal privacy protections. After 2010, regulations began requiring explicit, informed consent before data collection or sharing. The Driver's Privacy Protection Act (1994) addressed motor vehicle records, while the Telephone Consumer Protection Act (TCPA) and the National 'Do Not Call Registry' (1991) targeted solicitation calls, sanctioned opt-outs, and authorized fines for violations. Although not specific to online data, the TCPA remains a prominent U.S. privacy law (Clarip, 2026).

The 1990s and 2000s saw many new industry-specific privacy regulations. Specifically, in 1991, the Department of Health and Human Services introduced extra protections in healthcare under Title 45 CFR 46 (Public Welfare) Subparts A–D. Subpart A, known as The Common Rule, updated a 1981 research ethics regulation (Privacy of Genetic Information in the United States, 2021). The Common Rule sets minimum federal privacy standards for health data, but states may set stricter policies (Capital Health, 2026). It applies to most federally funded research and many NGOs. These regulations have since been revised several times, most recently in 2018.

A 1997 U.S. National Research Council report identified five main threats to personal data in medical systems: errors and leaks, access violations, abuse, unauthorized physical access, and intentional harm by disgruntled or terminated staff. Responding to these risks, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA), also known as the Kennedy-Kassebaum Act (Stevens, 2003). HIPAA aimed to standardize records, improve the security of sensitive data, and create a federal privacy framework. Specifically, the Act governs how health insurers, employer plans, and certain providers handle protected health information (PHI)—any medical or healthcare data about an individual (Clarip, 2026). However, critics argue HIPAA is bureaucratic and expensive, possibly shifting resources from care (Solove, 2008).

Since the late 1990s, the Federal Trade Commission (FTC) has been the main U.S. data protection authority, especially through Section 5 of the FTCA, which bars unfair or deceptive practices (Solove, 2014). This let the FTC address privacy issues as the internet and e-commerce grew. The FTC counted undisclosed or deceptive practices involving personal data as violations. Companies that do not honor data protection

promises break the law. The FTC later gained the power to levy fines and address spam, spyware, behavioral ads, mobile apps, and social media privacy. These steps made the FTC central to U.S. data protection (Clario, 2026).

FTC v. GeoCities (1998) was a landmark in online privacy. Specifically, GeoCities collected user data, including from children, supposedly for internal use. However, the FTC charged that GeoCities misled users by sharing the data with advertisers. As a result, the settlement required GeoCities to allow users to delete their data and to inform parents about disclosures regarding their children. Notably, the case affected over 2 million users, including about 200,000 children under 16 (Federal Trade Commission, 1998). Moreover, it reinforced the FTC's power to hold internet companies accountable for privacy promises. Finally, GeoCities had to clarify disclosures, enable data deletion, and alert parents to their rights (Federal Trade Commission, 1998).

This case also helped strengthen protections for children's data collection and storage in the U.S. and abroad. In 1998, the Children's Online Privacy Protection Act (COPPA) was passed. The law sets rules for website privacy policies, parental consent, and protections for children's online safety. COPPA applies to sites or services for children under 13 and to operators knowingly collecting such data. These companies must post privacy policies on their data practices, notify parents, get parental consent before collecting, using, or sharing data, and allow parents to review or delete their child's data (Clarip, 2026).

In a 1999 address, President Clinton warned of rising privacy risks from electronic medical records, saying, "As more of our medical records are stored electronically, the threats to all our privacy increase. Because Congress has given me the authority to act if it does not do so by August, one way or another, we can all say to the American people, ‘We will protect the privacy of medical records, and we will do it this year’" (Hughes, 2023; Malik, 2023). The following year, Clinton shifted his focus from medical to financial records, again stressing the importance of privacy: "We've … taken the first steps to protect the privacy of bank and credit card records and other financial statements. Soon, I will send legislation to you to finish that job" (Hughes, 2023).

Later in 1999, the Financial Modernization Act, or Gramm-Leach-Bliley Act (GLBA), required all financial institutions to disclose their data-sharing and protection practices. The law set strict rules for handling nonpublic financial information (NPI)—that is, any customer data not publicly available. Firms must explain how they share data, offer customers opt-out choices, and protect personal data through a security plan. For finance, GLBA became a privacy standard, similar to HIPAA in healthcare, and brought the principle of "privacy by design" into financial services (Harrington, 2025).

In the same year, two new positions were established in the United States: the Chief Counselor for Privacy in the Federal Government and the Chief Privacy Officer (CPO), the latter being "the senior executive responsible for managing risks associated with information privacy laws and ensuring compliance with them." Today, the CPO role exists in most government agencies and corporations, influenced in part by the experience of AllAdvantage, an online advertising technology company that employed privacy lawyer Ray Everett.

Overall, the U.S. privacy laws have been shaped not only by technological developments but also by significant historical events, such as the terrorist attacks of September 11, 2001. In response, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, which expanded government authority to monitor telephone and electronic communications for national and homeland security purposes (U.S. Department of Justice, 2007). Fourteen original provisions formed the foundation of the current USA Patriot Act Improvement and Reauthorization Act. Legislative updates also addressed the growing use of information technology to enhance government services, exemplified by the E-Government Act of 2002. The USA Patriot Act (2001) mandates that all federal agencies conduct a Privacy Impact Assessment (PIA) for any new technology that "collects, maintains, or disseminates personally identifiable information (PII), or for a new aggregation of information that is collected, maintained, or disseminated using information technology."

2.2.3 Crisis-driven evolution: how data leaks, re-identification, and the redefinition of data protection in the U.S. (2006–2017)

A series of high-profile cases in the early 2000s fundamentally altered public and governmental perceptions of personal data. These incidents introduced significant challenges and threats to the American government, while also revealing the extensive amounts of personal information stored on private company servers.

In 2006, a pivotal moment occurred when the illusion of "data anonymity" was shattered, marking the beginning of new challenges to American personal data protection in the digital era. This era, shaped by mass data, online identity, and human-factor threats, was highlighted in August 2006, when AOL published anonymized user search queries for research purposes (Arrington, 2006). Despite removing personal data such as names and IP addresses, researchers and journalists were able to de-anonymize users based on their queries. The AOL case showed that anonymization does not guarantee privacy (Ohm, 2010). Data sets can be compared, and identities can be reconstructed, meaning non-personally identifiable data can still reveal private lives. This incident spurred the development of ethical norms and regulations for Big Data and began discussions about corporate liability for data leaks or careless data use.

In academic and legal circles, this case symbolized the dawn of the Big Data era. Here, the main challenge became re-identification—the ability to deduce an individual from indirect digital traces. The AOL case demonstrated that digital technologies were creating new risks and challenges (Jesdanun, 2006). These required a comprehensive approach that combined legislation, technical protections, and ethical data processing standards. As a result, the United States began to shift during this period. The idea changed from "privacy as a right" to privacy as the management of personal information in a digital society. This shift led to the modern understanding of data protection.

The AOL case, as well, showed that banks and hospitals, which handle large amounts of personal information, pose special risks. This sparked talks about limiting automatic government database mergers (United Kingdom Parliament, 2024). It also led to calls for strict rules for data access and sharing. The main concern involved the Social

Security Number (SSN). Originally, agencies used the SSN for pensions, but it became a universal ID in banking, taxes, schools, and healthcare (Puckett, 2009). For US citizens, leaking an SSN meant complete exposure to identity theft. The federal government then attempted to restrict SSN use. The Privacy Act (1974), 5 U.S.C. §552a, requires agencies to inform people why they need an SSN and on what grounds. But the Tax Reform Act of 1976 relaxed these limits for some agencies, such as Social Security and transportation. As a result, widespread SSN use continues to create a weakness in US data security (U.S. Department of Justice, Office of Privacy and Civil Liberties, 2020).

Shortly after the governmental and corporate debates catalyzed by the AOL case, the WikiLeaks project emerged in 2006 as a new chapter in the evolution of data protection. Initially serving as a transparency tool and "digital inbox" for whistleblowers, WikiLeaks quickly became central to discussions on personal data protection in the United States (Lozano, 2010). However, following the publication of classified Pentagon and State Department documents (2010–2011), the issue escalated into a global conflict. This escalation triggered a direct clash between freedom of information and data protection. The published materials included not only political documents, but also sensitive data on employees, diplomats, and Afghan and Iraqi informants—names, addresses, and locations (Reals, 2010). This exposure placed lives at risk and provoked a strong reaction from US authorities, who viewed WikiLeaks' actions as an abuse of digital data and a violation of information security principles. Thus, the WikiLeaks case demonstrated for the first time that a digital leak can undermine national security, violate privacy, and upset the balance between the public's right to information and the individual's right to data protection.

Before 2010, observers largely regarded data leaks in the United States as journalistic occurrences. After the WikiLeaks disclosures, people started to view such leaks as global threats to both national and personal security (Myre, 2019). In response, the government implemented comprehensive reforms, strengthened internal protocols for accessing classified information (Obama, 2011), enhanced oversight of federal agency personnel, and initiated modern data governance frameworks to manage data access, storage, and transmission (Obama, 2011).

These measures later served as the basis for subsequent legislative initiatives, including the Cybersecurity Information Sharing Act (2015) and the National Cybersecurity Protection Advancement Act (2015). Lawmakers also drew on these measures in recent cybersecurity laws, such as those addressing foreign threats (for example, the Protecting Americans' Data from Foreign Adversaries Act, 2024). The Assange case publicly demonstrated for the first time that "Data is a form of power. Control over information equals control over government and society." In response to this incident, the United States began systematically developing the concept of data accountability. Authorities significantly reformed this concept after the Snowden and Equifax cases in 2013 and 2017 respectively.

The WikiLeaks affair became a symbol of the internal conflict of American democracy. Tension exists between the public's right to know and the state's responsibility to protect data, security, and privacy. This dilemma directly shaped the development of personal data protection as a legal institution. At that time, Americans began a public debate: Should data on government activities be public? Where is the line between whistleblowing and crime? How can we ensure whistleblowers' safety without undermining data protection? This case led people to view the concept of "privacy" more broadly. Now, privacy means protecting against unauthorized access in any form, including hacking, publishing, and digital leaks (BBC News Russian, 2024).

As public and governmental debates about state-driven data breaches continued, the focus of privacy debates in the 2010s began to shift toward the commercial sector. A prominent example of this transition was the Cambridge Analytica case. An ordinary user was unaware that, by sharing data on Facebook through a fun "quiz," it could be shared with third parties (Cadwalladr & Graham-Harrison, 2018). The app collected data from 87 million Facebook profiles (Meredith, 2018). The Cambridge Analytica scandal revealed that Facebook user data was shared with a political consulting firm. The firm used the data to improperly target users in political advertising without their knowledge (Andruss, 2022). Furthermore, Cambridge Analytica used this data to provide analytical support for the 2016 presidential campaigns of Ted Cruz and Donald Trump (Confessore, 2018).

As part of its settlement with the Federal Trade Commission (FTC), Facebook agreed to pay a $5 billion fine. It also had to implement substantial changes to its privacy practices (Harrington, 2015). This penalty represented one of the largest fines ever imposed by the US government for regulatory violations (Fair, 2019). The FTC cited Facebook's repeated breaches of its 2012 privacy regulations. These included sharing user data with third-party applications accessed by friends, enabling facial recognition by default, and using users' phone numbers for advertising. Facebook then became subject to a new 20-year settlement agreement (Federal Trade Commission, 2019).

The public responded very strongly to the breach, starting the #DeleteFacebook campaign. The campaign sought to organize a boycott of Facebook, but this did not lead to significant changes (Guynn, 2020). Then the #OwnYourData campaign began, calling on Facebook to be more transparent about its rules. It asked Facebook to give users more control over their data, calling user data an asset or property (Lozano, 2010). The Own Your Data Foundation was also created to teach digital skills (Own Your Data Foundation, 2020).

Finally, broadening the perspective beyond corporate misuse to include state surveillance, it would be difficult to discuss the history of privacy in the U.S. without mentioning the revelations in June 2013. These concerned the National Security Agency's domestic collection of intelligence from internet and communications companies. While an employee of the government contractor Booz Allen Hamilton, Snowden disclosed to the media that the NSA collected daily phone records of millions of Verizon customers (Greenwald, 2013). Snowden also revealed details about the American surveillance program PRISM. This program monitors and stores internet data, including search engine and social media activity, in collaboration with American intelligence agencies and European partners, under the guise of jointly combating international terrorism (Ehrenfreund, 2013). According to Snowden, American companies such as Facebook and Microsoft provided data to the National Security Agency. He also claimed the CIA and NSA can bypass all forms of cryptographic protection of internet information. As a result, intelligence agencies gain access to the commercial secrets of many companies and to private online correspondence (Biryukov, 2015; Gellman & Poitras, 2013). Most importantly, the Snowden case disclosures have

been analysed not merely as leaks of secret programs but as phenomena that reconfigure global surveillance, human rights, democracy, and state power, involving both state intelligence agencies and private corporations across borders (Bauman et al., 2014). This challenges traditional understandings of surveillance as purely national or state-centric. Bauman et al. (2014) state that the impact cannot be understood simply as "the U.S. vs the rest of the world" or as privacy against surveillance — the issues are much broader and deeper. Instead of seeing surveillance as isolated within nation-states, the authors frame it as a global phenomenon shaped by networks of private and public actors collaborating across borders.

In response to these challenges, President Obama (2014, 2015) emphasized in his 2014 and 2015 State of the Union addresses that "the intelligence community's activities must be based on public trust, and the privacy of ordinary people must not be violated." He proposed reforms to surveillance programs and increased transparency for intelligence agencies. He also called for the establishment of additional oversight mechanisms and the adoption of new federal data protection legislation, including measures addressing cyberattacks, identity theft, and child data protection. These proposals were formalized through a series of initiatives, most notably the USA Freedom Act (2015), which restricted the mass collection of telephone metadata (Office of the Director of National Intelligence, 2015). New standards for transparency and accountability in intelligence agencies were also implemented. Efforts began to develop a Consumer Privacy Bill of Rights, although this was ultimately not enacted.

In 2015, the United States faced not only intelligence leaks but also large-scale cyberattacks, including the breach of the Office of Personnel Management (OPM), which compromised the data of over 21 million federal employees (Guzman, 2015). This development underscored emerging threats posed by both governmental and private-sector data collection and storage practices. It also exposed the inadequacy of the Privacy Act of 1974 in addressing the complexities of Big Data, Web 2.0, geolocation, health, and children's information (United States House Committee on House Administration, 2022). Consequently, President Obama advocated for a unified federal data protection standard during 2015–2016, emphasizing corporate responsibility over consumer burden.

President Obama's address marked the onset of a new era in data protection in the United States, highlighting that privacy is not a private issue for the user, but a public obligation and a corporate responsibility (Obama, 2015). This signaled a shift in personal data policy from reactive measures against technological threats in the 1960s and 1970s, through the commercialization of data and the rise of the internet in the 1990s and 2000s, toward a comprehensive national digital policy in which data protection is integral to national security and social justice (Boyne, 2018).

Despite these policy shifts, large-scale data breaches at American companies persisted. In 2017, the Equifax breach marked a significant turning point for data protection in the United States. Equifax, one of the nation's three largest credit bureaus (Culnan, 2019), reported a breach affecting the personal data of 143 million Americans (Haselton, 2017). The compromised information included credit card numbers for approximately 209,000 consumers and certain documents containing personally identifiable information for about 182,000 individuals (Equifax Inc, 2017). The attack resulted in the theft of names, addresses, dates of birth, Social Security numbers, driver's license details, and credit card information. Notably, many victims were not direct Equifax clients, as the company collected data for credit ratings without their explicit involvement (Equifax Inc, 2017). This incident raised critical questions about citizens' ability to control their data when unaware of its collection. The media labeled the breach "digital Watergate," and bipartisan calls emerged for a federal consumer data protection law, mandatory national breach notification, and stricter information security requirements. Several bills were introduced, including the Data Breach Prevention and Compensation Act (2018), the Consumer Privacy Protection Act, and the Data Care Act (2018), but none passed Congress due to partisan disagreements over federal regulation and corporate liability (U.S. Congress, 2018).

The Equifax breach is widely regarded as a catalyst for significant institutional reforms in the United States. The incident spurred the development of state-level initiatives and resulted in substantial financial penalties for Equifax. The settlement included $300 million for a victim compensation fund, $175 million to participating states and territories, and $100 million in fines to the Consumer Financial Protection Bureau (CFPB), as filed by the FTC, CFPB, and 50 states (Federal Trade Commission, 2019).

This outcome signaled to major corporations that inadequate data protection could result in severe financial and reputational consequences. In the aftermath, the FTC was granted expanded authority to oversee data security, and discussions commenced regarding the establishment of a unified federal data protection agency (Federal Trade Commission, 2024).

The Equifax incident fundamentally altered the philosophy underlying the American privacy model. Prior to 2017, the prevailing approach emphasized "opt-out" mechanisms, whereby companies could collect and share data by default unless individuals actively opted out, and relied on voluntary self-regulation. The Equifax breach demonstrated that this model was insufficient for safeguarding personal data in the digital era. Consequently, the United States has begun to transition toward a framework centered on accountability and data responsibility, requiring companies not only to notify individuals of breaches but also to proactively prevent them, implement robust cybersecurity measures, and monitor the entire data lifecycle.

These developments have contributed to a gradual erosion of public trust in both American companies and the government, prompting international debate regarding the boundaries between national security and privacy rights. Ultimately, this has led to reforms in intelligence practices and increased regulation of data collection.

2.3 The contemporary U.S. framework for personal data protection

2.3.1 Shaping privacy through case law: the judicial evolution of personal data protection in the U.S.

The concept of personal data in the United States has evolved primarily through judicial practice, particularly regarding the "reasonable expectation of privacy." Court decisions have established and redefined foundational principles, shifting the focus from property-based privacy to a broader understanding of informational privacy. Legal precedents continue to shape federal laws governing personal data protection, reflecting this ongoing transformation.

One of the key decisions of the 20th century was *Roberson v. Rochester Folding Box Co* (1902). In this case, the plaintiff alleged that the defendant used her image in one of his

advertising posters without her permission. She claimed this caused her "serious nervous shock," which left her bedridden. The court dismissed the claim. It stated that the so-called right to privacy has no basis in practice and cannot be incorporated into law without seriously violating existing legal principles. This sparked public outrage and led to rapid change (Kornstein, 2006). In 1903, the New York State legislature, dissenting from the court's position in the Roberson case, passed the Privacy Protection Act. However, the law understood privacy in a narrow sense: the right to prevent or stop the use of one's image for commercial purposes and to recover damages for such use. This initial legal acknowledgment of privacy rights regarding personal images can be seen as a precursor to today's debates over data brokering and biometric data, where issues of consent and commercial use remain highly relevant (Kornstein, 2006; Spears, 2008).

Olmstead v. United States (1928) significantly shaped the field of personal data protection. The case examined whether warrantless wiretapping of private telephone conversations by federal agents violated the Fourth and Fifth Amendments. Justice Brandeis argued that the Fourth Amendment protected Americans' beliefs, thoughts, and sensations, conferring "the right to be let alone—the most comprehensive of rights" (*Olmstead v. United States*, 1928). This case established a philosophical basis for informational privacy, highlighting a pre-digital gap in constitutional protections for personal data. The absence of specific legislation or explicit constitutional guarantees underscored the need for legal evolution. The Olmstead case demonstrates that concerns about personal data protection predate digital technology and encompass broader aspects of individual privacy beyond computer-stored information.

By the mid-20th century, the Supreme Court began to address privacy more explicitly. In *Griswold v. Connecticut* (1965), the Court invalidated a state ban on contraceptives, finding that the statute infringed a "non-textual penumbral right" derived from various constitutional provisions. Justice Douglas described privacy as emerging from the "penumbras" of explicit guarantees, while Justices Harlan and White identified alternative constitutional foundations for privacy (*Griswold v. Connecticut*, 1965). This decision significantly broadened the right to privacy and established a precedent for applying constitutional principles to the protection of personal data.

Later, in the landmark decision *Katz v. United States* (1967), the Supreme Court extended the Fourth Amendment's protection against illegal searches and seizures. This protection moved beyond a person's home and property. It covered any place where a person has a reasonable expectation of privacy. After recording the phone calls of a sports bettor who used a phone booth outside his apartment, FBI agents arrested Katz and charged him with eight counts of knowingly transmitting interstate betting information by telephone—a federal crime. They listened and recorded his conversations without his knowledge by using a hidden device on the outside of a phone booth. The Katz case set a significant precedent because technological advances continue to raise new questions about privacy and government surveillance of personal data. The court in *Katz v. United States* (1967) held that "the Government's activities in electronically listening to and recording the petitioner's words violated the privacy on which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment." Law enforcement agencies, especially the FBI, continue to use the Katz precedent in modern disputes over electronic surveillance (Smith, 2013). However, some are concerned that the Katz test is being rendered obsolete by advances in surveillance technology (Arcila, 2012). A vivid example of this tension is the use of geofence warrants, in which law enforcement requests location data from all devices within a specific area over a specific period. This tool challenges the "reasonable expectation of privacy" standard established in Katz, as it potentially captures data on individuals not suspected of any wrongdoing, thus stretching the original framework to accommodate modern digital surveillance capabilities.

These cases did not create a general "informational self-determination" doctrine—a term later coined abroad. However, they affirmed that certain personal data and communications are protected by constitutional principles. In other cases, such as *Eisenstadt v. Baird* (1972), the right to privacy is viewed as "protected from governmental intrusion." In contrast, *United States v. U.S. District Court* (1972), well known as Keith Case, reflects the Court's careful balance between individual autonomy and national security. The court upheld and strengthened the right to privacy. It decided whether wiretapping violated the Fourth Amendment and what exceptions were allowed for wiretapping and privacy violations. The court said such exceptions were only

justified in situations involving a "clear and present danger to the structure or existence of the government" (*United States v. U.S. District Court*, 1972). The Court found the case did not fall within this exception and set the precedent that a warrant must be obtained before electronic surveillance, even in cases involving domestic security. The Court reinforced this even for government cases, where the defendants were members of organisations trying to subvert the government. The Court again found that the exception did not apply. This established that a warrant is required before electronic surveillance, even for domestic security (Conyers, 2003).

Whalen v. Roe (1977) addressed the constitutionality of a New York State program requiring centralized storage of prescription records for certain controlled substances. Plaintiffs contended that this collection violated their right to privacy. The Supreme Court recognized two dimensions of privacy: personal autonomy and informational privacy, defined as an individual's interest in controlling the collection and dissemination of personal information. Although the law was upheld, the decision affirmed that personal data protection is integral to constitutional privacy rights. Justice Brennan referenced the Fourth Amendment, emphasizing limits on government data collection and the risks posed by advances in computer technology (*Whalen v. Roe*, 1977). His concerns about the vulnerability of centralized health records anticipated later legislative responses, such as the Health Insurance Portability and Accountability Act of 1996. The prevalence of healthcare data breaches (500+ records in 2005 and 725 incidents reported in 2024; the number of individuals impacted has exploded, and according to the average cost of a healthcare data breach in 2025, the average cost for a healthcare breach is $7.42 million (Khalil, 2025) highlights the ongoing risks associated with centralized storage of sensitive information.

United States v. Miller (1976) established that individuals lack a "reasonable expectation of privacy" in bank records held by third parties. Later, *Smith v. Maryland* (1979) extended this principle to telephone data, ruling that information voluntarily provided to a telephone company is not protected by the Fourth Amendment. These rulings formed the basis of the "third-party doctrine," which holds that data shared with third parties is not constitutionally protected. This doctrine underpins the regulation of

digital surveillance and continues to influence debates over internet data and digital communications in the era of big data.

However, the foundational decision was *NASA v. Nelson* (2011). In this case, NASA contract employees challenged a background check that included questions about drug addiction and personal life. The question before the Supreme Court was whether these background checks violated the right to informational privacy. In two previous cases, *Whalen v. Roe* (1977) and *Nixon v. General Services Administration* (1977), the Supreme Court hinted that such a right might exist. However, it had never clearly resolved the question. The Supreme Court found that the government has a legitimate interest in such checks. It ruled that they do not violate informational privacy because the data is protected by confidential storage mechanisms (*NASA v. Nelson*, 2011). This case confirmed that government collection of personal information can be justified if there are adequate protections against its disclosure and abuse.

That same year, *Sorrell v. IMS Health* (2011) raised the issue of a Vermont law restricting the sale and use of prescription-identifiable data by pharmaceutical companies for marketing. The Supreme Court held that these restrictions violated the First Amendment because the sale and use of data constitute speech, and the law unlawfully discriminates against speech based on its content and source. The decision set an important precedent for regulating data flows and the commercial use of personal data, holding that restrictions on information flows could constitute a violation of freedom of expression. The quantitative and qualitative scope of data is radically different from that of pockets and wallets. The court explicitly recognized that phones are "portals" to extensive personal data (photos, messages, locations, apps). This precedent established a high standard of judicial review of police access to digital information.

Spokeo, Inc. v. Robins (2016) and *TransUnion LLC v. Ramirez* (2021) addressed the issue of damages for violations of federal data protection laws, such as the Fair Credit Reporting Act, in cases where harm was purely formal rather than actual. The Supreme Court ruled that Art. III standing requires a "concrete injury"—a specific and tangible harm, not merely an abstract legal violation. These decisions substantially limited the

scope for private lawsuits in data protection cases, mandating proof of real adverse effects or clear invasions of privacy, even when companies breached consumer rights.

In *Carpenter v. United States* (2018), the court recognized that obtaining historical location data (CSLI) from a telecom operator constitutes a "search" and generally requires a warrant. Prior to Carpenter, government agencies could obtain cellphone location data from service providers without a search warrant, arguing that the information was necessary for an investigation, but this decision changed that practice (Squire Patton Boggs, 2018). The court created a significant crack in third-party doctrine by recognizing that long-term location histories are so sensitive that they retain constitutional protection even when stored by third parties. The decision became a pillar for subsequent arguments regarding the protection of digital metadata and behavioral traces. However, the Supreme Court's decision in Carpenter was narrow and failed to fundamentally alter the third-party doctrine applicable to other business records that might inadvertently reveal location information, nor did it overturn previous decisions regarding traditional surveillance methods and tools, such as security cameras (Ng, 2018). The Ninth Circuit Court of Appeals held that collecting publicly available data (web scraping) does not constitute unauthorized access under the law because the data is publicly available (*Carpenter v. United States*, 2018). This decision is pivotal for the regulation of "public" personal data, confirming that information posted publicly is not subject to the criminal protections of the CFAA, although it may still be subject to privacy and data protection laws.

The recent case of *TikTok, Inc. v. Garland* (2025) saw the Supreme Court uphold the constitutionality of legislation authorizing the banning or transfer of a foreign-controlled application. This decision raised critical questions regarding the collection, storage, and transfer of American user data by foreign entities, as well as the judiciary's approach to national security. While the Court acknowledged the heightened sensitivity of digital data, such as geolocation and metadata, it remained cautious in revisiting the established third-party doctrine, thereby allowing continued government and corporate access to data.

These judicial decisions underscore the growing tension between the openness of public data and the necessity for legal protection, illustrating that traditional concepts of

"access" must be reconsidered in the digital era. A discernible shift toward prioritizing national security over personal data protection is also evident. Collectively, these cases highlight the central challenge for personal data protection in the United States: balancing freedom, security, innovation, and constitutional privacy guarantees amid rapid technological change. The proposed American Data Privacy Protection Act (ADPPA) represents a forward-looking solution, offering a unified framework for data regulation and protection. If enacted, the ADPPA could address existing inconsistencies in privacy law and guide future policy toward effective outcomes.

2.3.2 Fragmentation, federal inertia, and emerging national security concerns: U.S. data protection challenges in the 2020s

Since the early 2020s, US data privacy legislation has been deteriorating (IncFine, 2025). There are growing calls for a federal, unified law. This is especially evident in the wake of *Dobbs v. Jackson Women's Health Organization* (2022). This ruling stated that the US Constitution does not guarantee the right to abortion. It overturned *Roe v. Wade* (1973) and *Planned Parenthood v. Casey* (1992), which previously enshrined this right at the federal level (*Dobbs v. Jackson Women's Health Organization*, 2022). This decision heightens concerns that US constitutional protections for privacy and liberty can be unexpectedly overturned. As a result, the lack of a robust, unified, and secure legal framework for data protection creates risks. Personal and medical information, including reproductive data, is left to state regulation. Concerns have grown about how data brokers and app developers blatantly track users, such as visits to abortion clinics or the use of menstruation apps. These records could be used to prosecute users in states where abortion is criminalized (Xavier et al., 2025). This situation once again highlights the urgent need for comprehensive federal legislation. Lawmakers must urgently act to unify personal data protection and build a resilient legal framework that safeguards all Americans, proactively addressing threats before more rights are compromised.

Amid urgent demands for federal action, the American Data Privacy and Protection Act (ADPPA) emerges as a critical proposed federal online privacy bill. If enacted, it would fundamentally regulate how organisations store and use consumer data. The bill focuses sharply on data minimization, individual ownership, and private right of action (Dumiak, 2022). To comply, data collectors must only gather data that is "necessary,

proportionate, and limited to" their stated purpose, such as operating a product or enabling communication. Importantly, the ADPPA would specifically restrict the transfer and processing of certain sensitive data types. For example, urgent restrictions would apply to Social Security numbers, precise geolocation, biometric and genetic data, passwords, browsing history, and physical activity tracking (Dumiak, 2022; Skadden, 2022). In addition, individuals would gain the right to know how their data is used and to whom it is given, as well as the immediate ability to correct or download their user data. Organisations are required to process these requests within up to 90 days, depending on their size.

Certain "large data holders" must urgently comply with extra oversight. These include those with gross revenues above $250 million in the last year and who process either five million personal data items or 100,000 sensitive individual records (Dumiak, 2022; Mayfield, 2023). In contrast, "small data holders"—organisations with gross revenue of less than $41 million over the past three years—face fewer demands. They process data for fewer than 100,000 people per year, do not mainly transfer data, and are exempt from some requirements. Small data holders may promptly delete records rather than handle corrective requests. They remain exempt from most other requirements, except the user's right to request deletion of data no longer in use (Dumiak, 2022).

Another notable aspect of the proposed federal bill is its intended scope. The federal bill was intended to include nonprofits (while many state privacy laws do not), although nonprofits would largely fall under the exemptions provided for "small data holders." However, as of fall 2025, it remains pending, in part because many experts believe the law does not provide a truly high degree of personal data protection and "might nullify stronger protection from several state laws" (Morrison, 2022). Addressing these shortcomings is not just necessary, but urgent.

While federal efforts address privacy domestically, international data transfers are subject to separate frameworks. In 2023, the Data Privacy Framework (DPF) came into force to facilitate the transfer of personal data between the European Union and the United States. The DPF replaces two defunct EU-US agreements. First, the Safe Harbor Privacy Principles (2000-2015) ended after the Court of Justice of the European Union overturned them, citing the broad powers of US law enforcement to access personal

data. Second, the EU-US Privacy Shield (2016-2020) was also invalidated by the Court. As a result, the DPF aims to address the urgent issues raised in these previous decisions (Manancourt et., 2022; U.S. Department of Commerce, 2023). Under the General Data Protection Regulation (GDPR), the transfer of personal data to the US is a "transfer of personal data to a third country" (a cross-border transfer) and is regulated by Chapter V of the GDPR (2016). The level of protection provided by the receiving country's government and practice determines the transfer's legal basis. Transfers may rely on an adequacy decision (Art. 45) or one of the appropriate safeguards listed in Art. 46.

For organisations managing transatlantic data flows, experts believe that adequacy decisions make the transfer of personal data much simpler. No extra steps are needed for transfers outside the EU (Data Privacy Office, 2023; European Commission, 2017). These transfers are similar to those within the EU. GDPR (2016) enshrines that a contract is concluded between controller and processor (Art. 28). This contract does not contain special conditions for transferring data to non-GDPR countries Without an adequacy decision, transferring personal data is more difficult (Data Privacy Office, 2023). First, a high level of data protection on the recipient side is required, using "appropriate safeguards." The recipient must comply with rules comparable to those of the GDPR, even if local law is less strict. Because so much personal data flows to the US—often due to US-developed software—making transfers easier was urgent (Data Privacy Office, 2023; European Commission, 2017).

The mechanics of the DPF are as follows: The new mechanism requires self-certification by US companies wanting to receive personal data from the EU under a simplified scheme. This is similar to the Safe Harbor Privacy Principles and the EU-US Privacy Shield. GDPR (2016) enshrines that the adequacy decision (Art. 45) applies only to companies that declare their participation in the DPF, take additional steps, and submit documents for listing in the DPF database (European Commission, 2023). The EDPB's explanatory note (2023) states that the DPF can only be used for transfers from the EU. If a company outside the EU is subject to the GDPR under Art. 3(2) data transfers from such a company to the US must use an appropriate safeguard in Art. 46 or the exception in Art. 49. These companies cannot rely on an adequacy

decision (Art. 45), even if transferring data to a US company in the DPF (European Data Protection Board, 2023).

Despite these official mechanisms, the DPF has faced repeated criticism from experts (NOYB, 2023). Many see it as a political decision by the US and the EU, hastily created and in a rough form. Max Schrems, chair of NGO NOYB (2023), says, "Just like "Privacy Shield," the latest deal is based not on material changes, but on political interests." The DPF is seen as a copy of the Privacy Shield (2016), which itself copied Safe Harbor (2000). Other experts criticize its implementation. They often cite the lack of secrecy and the inefficiency of the Data Protection Review Court (DPRC). The DPRC is a three-judge panel that hears appeals from decisions of the Civil Liberties Protection Officer at the Office of the Director of National Intelligence. Its decisions are binding (The White House, 2022). As of spring 2025, the independence and effectiveness of the PCLOB—the body that appoints DPRC judges—are under question. President Trump dismissed the Democratic PCLOB members, leaving only one Republican on the five-member panel. This falls short of the required three-person quorum (Wold, 2025). The lack of independent oversight and the PCLOB's paralysis undermine the legitimacy of the appeals system in the EU–U.S. Data Privacy Framework (2023). This also raises doubts about the DPRC's secrecy, accountability, and effectiveness, given that its decisions are binding but its independence from the executive is questioned (Wold, 2025).

In 2024, the Protecting Americans' Data from Foreign Adversaries Act was passed. This controversial law now bans data brokers from transferring sensitive personal data of US citizens, such as biometric and genetic information, Social Security numbers (SSN), health data, or precise geolocation, to foreign "adversaries" (China, Russia, Iran, North Korea). Feiner (2024) argues that this law marks the first time that personal data protection is directly linked to geopolitics and digital sovereignty (U.S. Congress, 2024). Furthermore, he discusses the bill and its adoption, noting the implications of this linkage. While the act addresses national security concerns, it may inadvertently shift focus from domestic misuse of personal data. The framing of foreign adversaries could overshadow urgent issues within the United States, where similar data could be exploited by local entities in ways that also threaten individual privacy. Balancing

external geopolitical threats with internal risks demands a nuanced policy approach that invites stakeholders to critically examine all potential vulnerabilities.

These laws reflect important changes and trends in the American data protection system. First, they emphasize national security as a component of privacy, as traditionally, US data protection laws have focused either on individual rights (data access, correction, notification) or on specific sectors (finance, healthcare). However, this law emphasized that data protection is not only a personal and commercial issue, but also a matter of national security. Preventing the sale of data to "foreign adversaries" demonstrates that the government sees risks in the widespread commercial processing and international transfer of data. Furthermore, the law significantly expanded the definition of sensitive data, for example, by including categories such as genetic information and precise geolocation, raising the bar for data security and governance requirements. Second, the law strengthened the role of private-sector regulation by imposing obligations on data brokers, not just government agencies. This reflects a shift from the idea of "access and control over government agencies" to "governance and responsibility in the private sector." Furthermore, Feiner (2024) points out that the law was viewed as "an important complement to the broader data protection law we still plan to enact," meaning that the US data protection institution could shift from a "mosaic" industry model to a more integrated federal framework, where new regulations would reflect the challenges of the digital age.

Furthermore, the FTC announced its closure on October 1, 2025, due to the lapse in government funding (Shoop, 2025). Formally, the FTC's suspension (due to lack of funding) is the result of a "government shutdown," a situation in which Congress failed to approve a budget. However, 2025 coincides with a time when the US data protection institution is undergoing reform, particularly amid rising leaks, cyberattacks, and international threats. The FTC is the central authority responsible for overseeing privacy and data security: it uses Section 5 of the FTC Act to curb unfair or deceptive practices (Federal Trade Commission Act, 1914); it hears cases against major companies (Facebook, Google, Equifax, Snapchat); and it sets precedents that effectively replace the lack of a general data protection law in the US. Thus, when the FTC's role as a regulator is most critical, the agency effectively ceases to function: user complaints are

not addressed; leak investigations are not conducted; regulatory guidelines and penalties are not updated; and interaction with international regulators (in particular, with the EU under the EU–US Data Privacy Framework) is disrupted.

Shoop (2025) and The Guardian (2025) point out that the closure of the FTC represents nothing less than a new institutional challenge and a threat to trust in the data protection system. After all, if the main oversight body effectively "disappears," the public loses confidence that personal information is under control. Furthermore, as Congress has been debating the need to create a unified federal data protection standard since 2024, the closure of the FTC—a key player without which reform effectively stalls—has been announced. Moreover, the situation with the FTC's closure repeats the story of 1980, when the commission first ceased its work due to political disagreements over its powers (Brown, 1980). Thus, the closure of the FTC once again underscores the weakness of the American data protection model, which is based on fragmented legislation (an industry-specific approach) and on regulators' dependence on Congress's political decisions (Shoop, 2025).

2.3.3 Decentralized data protection: state-level legislation and enforcement practices in the field of personal data protection in the U.S.

Personal information in the United States is protected by a patchwork of industry-specific federal laws and state legislation that vary in scope and jurisdiction. The key debate over U.S. personal data laws centers on the conflict between state regulations and the need for unified national standards. States set their own requirements for obtaining and using confidential data, leading to inconsistent practices nationwide.

California leads the country in personal data protection regulations (Pittman et al., 2025). It was the first to implement data breach notification laws in 2003, requiring companies to disclose security breaches involving residents' personal data (California Senate Bill 1386, 2003), thereby increasing transparency and prompting improved cybersecurity practices. The California Electronic Communications Privacy Act (CalECPA) of 2015 requires law enforcement to get a warrant before accessing electronic data (California Electronic Communications Privacy Act, 2015), protecting

individuals' digital privacy from unwarranted searches. The California Consumer Privacy Act (CCPA) of 2018 regulates how companies handle residents' personal information and allows individuals to control data collection and processing, understand how their data is used, and opt out. These rights rest on transparency and accountability (California Consumer Privacy Act, 2018), fostering consumer trust and business compliance. Many jurisdictions have followed these standards. A recent study found that compliance with these laws raises corporate costs by about 40%, indicating a significant compliance burden. The California Privacy Rights Act (CPRA) of 2023 expands individual rights, clarifies business obligations, limits the use of sensitive information, and requires additional risk assessments (California Privacy Rights Act, 2023), enhancing both consumer protections and regulatory expectations for businesses. The new California Privacy Protection Agency (CPPA) enforces these rules and conducts audits (California Privacy Rights Agency, 2025), increasing regulatory oversight and ongoing accountability for organsations.

The CCPA and CPRA are founded on three core principles: disclosure, control, and protection. Disclosure grants individuals the right to request information regarding their processed personal data and its sources. Control enables individuals to restrict the transfer of their data, including through online opt-out mechanisms. Protection mandates heightened security measures for sensitive information, such as biometric data, health records, and personal preferences.

Amendments to the California data breach notification law take effect on January 1, 2026 (California Legislature, 2025). The new law requires businesses to notify affected California residents within 30 days of discovering a data breach (Senate Bill No. 446, 2025). This replaces the older, flexible standard of notifying individuals "as soon as practicable and without undue delay" (California Senate Bill 1386, 2003). Notification may be delayed to meet law enforcement needs, determine the scope of the breach, or restore data integrity. Companies must notify the Attorney General within 15 days if a breach affects more than 500 Californians (California Senate Bill 1386, 2003).

Giblin and Medeiros (2025) notes that some states already set notification deadlines of 30 to 60 days. These include New York (30 days), Texas (30 days), Colorado (30 days), Florida (30 days), and Delaware (60 days). The requirement in some states to notify the

Attorney General at the same time or before notifying individuals imposes a higher compliance burden than California's new rule, which only requires Attorney General notification within 15 days after notifying individuals (California Senate Bill 1386, 2003). Giblin and Medeiros (2025) further explains that, in practice, many companies immediately issue all necessary notices after individual notification, helping them comply with these varying legal obligations.

California's privacy laws serve as a model for other states and countries. The Delaware Online Privacy and Protection Act, in effect since January 1, 2016, follows California's approach. The law limits advertising to children, increases privacy for digital book readers, and requires clear privacy policies (Clarip, 2026). California also passed stricter laws than federal standards, such as Shine the Light SB 2 (2005), which requires companies to disclose data sharing practices, and the Reader Privacy Act (2011), which limits access to reading data without a court order (Cohn & Jeschke, 2011). The California Privacy Rights Act (2020) created the US's first data protection agency and strengthened access, deletion, and data-use limits. Together, these laws focus on transparency and consumer protection, setting a benchmark for privacy protection like Europe's GDPR (Fazlioglu, 2025).

In the 2020s, Colorado, Connecticut, Maryland, Massachusetts, New York, and Virginia enacted broad data privacy reforms (Sabin, 2023). This weakened California's dominance in data protection and moved the country toward a decentralized, diverse set of standards. State legislatures are now addressing data protection gaps through their own statutes.

Virginia was the second state to pass a general privacy law, enacting the Consumer Data Protection Act on March 2, 2021. The law covers businesses that process data from at least 100,000 Virginia consumers or get over half of their revenue from selling such data. Residents can access and correct their data (Virginia Consumer Data Protection, 2021). California's laws cover companies with over $25 million in revenue or those handling data from 50,000 or more consumers (California Privacy Protection Agency, 2024). Virginia centers on data practices; California emphasizes company revenue and data transactions. Colorado passed a similar law on July 8, 2021 (Rosenkoetter, 2021).

In Colorado, the law requires companies to inform consumers about data collection and sharing, echoing Virginia's focus on transparency and control (Colorado Privacy Act, 2023). Colorado and Virginia use data-processing or sales thresholds, not broad ones like California. Colorado residents have opt-out rights for personal data sales, and the attorney general enforces strict penalties for violations (Colorado Privacy Act, 2023). In 2023, Connecticut required all companies collecting resident data to maintain privacy protections and reasonable security (Connecticut Data Privacy Act, 2023).

Harrington (2025) calls the New York State Privacy Act one of the US's most comprehensive privacy laws, dubbing it "the GDPR of the East Coast." The law creates strict requirements for data collection, use, and sharing, and introduces new consumer rights, including mandatory disclosure of data categories and uses, so people can better understand and control their data. Maryland's Online Consumer Protection Act addresses cyber threats such as data breaches, theft, phishing, and spyware by requiring all businesses, regardless of size, to protect personal data. The law covers any business that collects information on Maryland residents, including those out of state, and allows consumers to opt out of the collection, use, or sale of their data (Maryland Online Consumer Protection Act, 2024).

The Massachusetts Privacy Act requires companies to get consent before collecting or using a consumer's data, giving people control over their data. It requires transparent disclosure on data use, builds in opt-out rights, and demands that businesses keep information accurate to reduce personal data errors (Massachusetts Privacy Act, 2024).

Many states, such as Utah, California, Delaware, Illinois, Maryland, Michigan, and New Jersey, restrict employers' access to employees' social media accounts (Lein, 2013). Utah's Internet Employment Privacy Act bans employers from requesting social media usernames or passwords. This trend reflects growing privacy concerns. Businesses in multiple states now face greater compliance demands. Nevada and Minnesota require internet service providers to protect certain customer information. After federal ISP data restrictions were repealed, many states set their own data-use limits, adding complexity. Many states mandate secure disposal of records with personal information (Lein, 2013). As of December 2016, at least 31 states and Puerto Rico require that information be unreadable (Dunlap et al., 2017). Some states, including

Arkansas, require reasonable security measures to safeguard personal data from unauthorized access or use (Griffin, 2026).

As for October 2025, a total of twenty states have passed comprehensive data privacy laws in the United States: California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Florida, Montana, Oregon, Delaware, New Hampshire, New Jersey, Kentucky, Nebraska, and Rhode Island. Of those twenty, the laws of California, Colorado, Connecticut, Virginia, Utah, Florida, Texas, Oregon, Montana, Delaware, Iowa, Nebraska, New Hampshire, and New Jersey are currently effective, while Tennessee, Minnesota, and Maryland's privacy laws will become effective later in 2025 (Pittman et al., 2025). The number of such laws continues to grow, reflecting the expanding data privacy landscape.

However, one of the most interesting cases is Oklahoma substantial changes to its data breach notification framework, reflecting a broader national trend toward enhanced cybersecurity and consumer protection (Senate Bill 626, 2025). The new amendments will expand the definition of personal information subject to disclosure to include unique government-issued identification numbers (such as state identification card or passport numbers); electronic identifiers and credentials authorizing access to financial accounts (such as routing codes combined with passwords or access codes); and biometric data (Senate Bill 626, 2025). Furthermore, organisations that implement "reasonable security measures" appropriate to their size, activities, and the sensitivity of the data they store may be able to rely on an affirmative defence to civil penalties. Peretti and Austin (2025) indicate that organisations that fail to implement such safeguards but comply with notification requirements may be fined $75,000 plus actual damages, while organizations that fail to implement safeguards or provide adequate notification may be subject to civil penalties of up to $150,000 per violation.

However, as of April 2025, only three states (California, Colorado, and Utah) have laws governing AI use (Taylor et al., 2025). California's AB 2013 requires AI developers to "publish information about the data used to train their AI systems" (California Generative Artificial Intelligence Training Data Transparency Act, 2013). Colorado's AI law, which is set to take effect in 2026, focuses on high-risk AI systems and "is designed to protect against algorithmic discrimination in AI systems" (Colorado's

Artificial Intelligence Act, 2024). Utah's AI policy law "imposes disclosure requirements on companies using generative AI tools" (Utah Artificial Intelligence Policy Act, 2024). Also, as of April 2025, more than 15 other states have proposed AI laws, signaling the U.S. system's commitment to streamlining AI regulation nationwide (University of Michigan, 2025).

In California, financial penalties of $2,500 are imposed for each detected CCPA violation, and penalties of up to $7,500 are imposed for willful violations (California Privacy Protection Agency, 2024). For comparison, the GDPR allows fines of up to €20 million, 4% of annual global turnover, or $750 per affected user (Irwin, 2022). If confidential information is disclosed due to inadequate security, users may sue (Scarcella, 2025). This framework encourages organisations to invest in robust security measures, as compliance is essential for financial stability and reputation. In other states, liability is often handled by prosecutors. It is commendable that states are striving to protect their citizens' personal data independently (Shatz & Lysobey, 2024). However, it is important to understand that differences in state regulations can lead to confusion and chaos. For example, Illinois now has the Biometric Information Protection Act in place to protect individuals' biological characteristics when those characteristics are used in systems that use biometric information (Illinois Biometric Privacy Act, 2008). Thus, while the state has no specific privacy law, it does have restrictions on a specific subset of personal data. Additionally, the New York Department of Financial Services (NYDFS) section 500.3 has requirements for data obligations, including policies for customer data privacy policies (N.Y. Comp. Codes R. & Regs. Tit. 23 § 500.3, 2023): "Virginia, Colorado, Connecticut, Utah... the list of US states with privacy obligations continues to proliferate" (Margolis, 2026; New York State Department of Financial Services, 2023). Furthermore, the author emphasizes that, in addition to other privacy or personal data protection laws in many US states, laws relating to breach notification and data security are moving through the legislative process in each state or are already established: "One of the commonalities in these regulations is a negative use case: many provide exemptions for financial services and health care in deference to industry-specific federal laws. Another instance of uneven application of privacy regulation depends on region and/or industry," (Margolis, 2026). The costs associated with this regulatory fragmentation can be significant for companies

operating across multiple states: "a growing patchwork of state privacy laws threatens to impose rising compliance costs on businesses as they are increasingly subject to multiple, duplicative rules not just from their home states but from others, too. The out-of-state costs of 50 such laws could exceed $1 trillion over 10 years, with at least $200 billion of that burden falling on small businesses..." (ITIF, 2024). For instance, duplicating audit processes and increasing legal fees can create substantial financial burdens, thereby validating Margolis's claim of confusion and chaos (Castro et al., 2022).

Harrington (2025) also believes that the practice is very fragmented and problematic. For example, the laws of California, New York, and Massachusetts apply to any company doing business in those states, regardless of whether it has an office there. By comparison, Maryland's laws apply only to organisations with a physical presence in the state. Furthermore, California and Maryland's privacy laws apply to companies with annual revenues exceeding $25 million, while other states have no such restrictions (Charfoos et al., 2022). Furthermore, the degree of regulatory protection for data privacy in the United States varies significantly from state to state. Despite support for federal privacy laws from both public and private organisations, it is unlikely that the U.S. Congress will pass any such legislation (Warburton, 2024). In response, many states and companies continue to seek other solutions (Andruss, 2022). This will likely lead to further fragmentation of privacy laws and requirements for companies. Many companies simply choose to adhere to the strictest versions of these laws, as this approach inevitably ensures their compliance with less stringent laws in other states, countries, and international jurisdictions. This proactive approach also helps companies avoid having to react to each new law as it is passed, potentially giving them a competitive advantage over companies that take a more reactive approach.

While the content of regulations in these states varies, a common focus is evident: ensuring transparency, protecting individuals' interests, and imposing obligations on companies that process large-scale personal data. As a result, regional data regulation in the United States is becoming increasingly complex, creating additional barriers to cross-border initiatives. When analyzing enforcement, it is important to determine whether a business entity falls under the scope of a specific regulation. Laws are based

on revenue indicators, the number of consumers in the relevant territory, and other factors. Despite commonalities, individual states have established differences in terminology and enforcement approaches. In some cases, regulations place increased emphasis on the conditions for providing informed consent, while in others, the focus is on notification procedures in the event of a personal data breach. Some regulations stipulate the appointment of an authorized employee responsible for monitoring compliance with rules regarding the processing of confidential information. Other regulations are limited to the requirement to ensure the necessary technical and organisational measures.

Chapter 3. Formation and development of the right to personal data protection in Russia[1]

3.1 Early legal and philosophical foundations of personal data protection in Russia before 1993

3.1.1 Historical foundations of the privacy and confidential information protection framework

Russian academic scholars state that the institution of personal data protection in Russia developed as a distinct entity, separate from broader concepts such as privacy and the protection of confidential information (Vilisova & Grishin, 2022; Berzin & Mitianov, 2025). The evolution of Russian personal data protection initially arose from the need to address privacy intrusions and subsequently evolved into a separate legal institution. This development can be traced through specific historical milestones, illustrating how personal data protection gradually diverged from general privacy concerns and adapted to new forms of governmental and private data use (Vilisova & Grishin, 2022).

In Russia, prior to 1993, personal data protection was embedded within broader notions such as "privacy" and "secrecy of correspondence." Zharova and Elin (2017) emphasize that the inviolability of private life, closely associated with the concept of "privacy," encompasses both sociological and legal dimensions. From the individual's perspective, privacy establishes a personal domain with boundaries that should not be crossed. Additionally, Sexte and Markevich (2020) argue that a comprehensive understanding of Russian personal data protection necessitates an analysis of its historical regulatory stages.

Stebivko (2023) identifies elements of the right to privacy as early as the 9th century AD in Ancient Rus' (Ruthenia). While this period cannot be considered the origin of a formal institution for protecting individual personal data, it is notable that the concept of privacy began to take shape. With the development of writing and the introduction of courier services in Rus', the term "gramotie" ("charters") (Likhachev, 1978) became prevalent, referring to both official and private business documents and letters. As a result, norms regulating the circulation of such charters emerged. These norms were

[1] *Unless otherwise indicated, all translations from Russian sources are the author's own.*

situational, addressing specific violations without generalization, but were nonetheless applied broadly in practice. As Stebivko (2023) observes, they were used by analogy and applied to the widest possible range of situations.

Moreover, Peter the Great's reforms in the 17th and 18th centuries are considered foundational for personal data protection in Russia, supporting the argument that such protection developed in response to evolving state and societal needs. His decrees revised postal regulations, explicitly prohibiting couriers from opening or reading others' charters (Rybakov, 1985). Specialized procedures were implemented for handling charters: documents were sealed, rolled, and transported in secure cases or bags by couriers (Vigilev, 1990). According to Stebivko (2023), these rules prioritized secrecy (primarily to protect state secrets) but also included general provisions for safeguarding personal correspondence. Stebivko further notes that Peter the Great's policies and reforms significantly transformed Russian law and personal data protection, and that Russia's emergence as a European power introduced new legislative approaches to private life.

After the completion of Peter the Great's reforms, Russia saw the earliest forms of collecting, processing, and recording personal data, commonly linked to the state's fiscal and military needs. Legal regulation in the modern sense was absent. The collection and use of personal data was the prerogative of the state and was uncontrolled. For example, the Revision Tales (18th-19th centuries) and per capita censuses introduced by Peter the Great in 1718 for tax purposes were introduced. They took into account name, age, gender, and social status (Avdeev & Troitskaya, 2025). According to Filonova (2022), Peter the Great's decree introducing the poll tax in 1724 is one of the first written legal sources in the history of Russian statehood to ensure information protection, since the introduction of the poll tax implied a census of the population for tax collection (except for the nobility and clergy). Since the 18th century, Church registers have also been introduced, recording births, marriages, and deaths. At that time, they served as civil registry offices (Migranova, 2024).

Moving into the 19th century, a new phase emerged as the collection, processing, and recording of personal data continued, primarily for police purposes. The first card indexes of individuals under surveillance were compiled after the Decembrist uprising

in 1825. In 1845, Russian Emperor Nicholas I introduced penalties for disclosure of commercial secrets ("Code of General Penalties"). Subsequently, under Emperor Alexander II, measures were taken to strengthen and improve the institution of protecting privacy and confidential information. For example, the Postal Regulations of 1857 enshrined the secrecy of correspondence and banned opening mail in the recipient's absence. According to the Art. 9 of the Telegraph Regulations, also enacted in 1857, responsibility for accurate delivery and the safety of message secrecy was assigned to telegraph line inspectors (Korevo, 1915).

Following these 19th-century changes, the political climate shifted again after Alexander II was assassinated in 1881. Alexander III issued the May 11 Proclamation, reaffirming autocratic power and reversing his father's liberal reforms, marking a return to autocracy through tighter censorship, expanded police surveillance, and the undoing of previous judicial and administrative changes. The Proclamation allowed the Minister of Internal Affairs to open correspondence for state protection outside judicial procedures (Szeftel, 2019; Avdeev, 2025). At the time, forty to fifty people worked in censorship, barred from viewing letters of the Emperor and Minister. Even though the Russian Empire did not establish a centralized system for state secrets or personal data protection, nor a unified legal framework for information protection, until the 20th century (Filonova, 2022).

3.1.2 Proto-forms of personal data protection in the Soviet legal system

The next and key stage in the development of legal frameworks for the protection of personal data is associated with the development of Soviet statehood. To illustrate this, Popova (2022) argues that Soviet-era legislation effectively lacked privacy guarantees, with liability for privacy infringement mentioned only in special orders to people's courts and judges. Furthermore, this issue was never formally addressed in sectoral legislation. However, Stebivko (2023) links the early 20th century with the starting point for the formation of the institution of personal data protection as a separate, fragmented institution, owing to the proclamation of the right to personal privacy on October 17, 1905, in the Manifesto "On the Improvement of State Order" and the enshrinement of this right in the "Fundamental State Laws" of the collection of laws of April 23, 1906. Kukushkin and Chistyakov (1980) believe that, based on these acts, the

legislative consolidation of a broad system of personal rights for citizens in the new society was laid out in the 1918 Constitution of the RSFSR. For example, in April 1918, Lenin (1969) noted that "socialism without postal services, telegraphs, and machinery is an empty phrase." Building on this, Stetsovsky (2000) notes that after 1918, due to the authorities' expanded political surveillance, which was concentrated in the hands of the Central Committee of the RCP(b), three channels of classified information emerged: party-Soviet, military, and through Chekist organisations. By the late 1920s, this system evolved into a powerful conspiratorial network for the comprehensive collection of political information (Ivansky, 1998).

Transitioning from the early Soviet era to the post-revolutionary period, Filonova (2022) believes that the first separate legal document in the field of information protection was essentially the list of information constituting a secret and not subject to dissemination, approved by the Decree of the Council of People's Commissars of the RSFSR of October 13, 1921. In the same year, Department 8 was created within the All-Russian Extraordinary Commission for Combating Counter-Revolution and Sabotage under the Council of People's Commissars of the RSFSR, whose main task was to ensure the security of state secrets. Additionally, building on state efforts to monitor and control, Volkov (1990) believes that with the advent of Soviet power, the collection, processing, and recording of personal data became a tool of control and management. For example, general population censuses were increasingly conducted in 1926, 1937, and 1939, and they began to include not only demographic but also ideological data, such as the question on religion in 1937, which was proposed personally by Stalin. The instruction manual for the enumerator stated, "In particular, explain that when asking about religion, the respondent must indicate his or her current personal beliefs (non-believer, Orthodox believer, Muslim believer, etc.), and not the religion to which the respondent or his or her parents were officially assigned in the past" (Resolution of the Central Committee of the BCP(b), 1936).

Following the increased state monitoring described above, a passport system was also introduced in 1932, which included internal passports with registration. The passport became the only form of identification, containing information such as first name, patronymic, last name, date and place of birth, nationality, social status, and place of

employment (Popov, 2015). The passport undoubtedly became an instrument for regulating migration and repressive policies. Building on these identification systems, the USSR State Security Committee subsequently began compiling entire files on dissidents, "unreliable" citizens, and foreign contacts, storing information about these individuals. Legal regulation was virtually nonexistent throughout these developments.

In light of these developments, the state used the data without restrictions, and its protection was not guaranteed. Additionally, the practice of using informants was introduced: "Many were offered to buy their lives or the lives of loved ones by assuming the functions of secret agents. Great importance was attached to information compromising senior officials. Listening devices were installed in their offices, apartments, and dachas." The secret collection of information for dossiers was common practice and was supported by members of the Politburo (Markomenko, 1997; Matuzov, 1966 & 1972). Thus, already at a very early stage, one can observe the emergence of a systematic practice of collecting, using, and disseminating personal information without an individual's consent, primarily in relation to officials, which subsequently became one of the main problems that modern data protection legislation seeks to address. Informants illegally collected and used information about people's private lives, compromising material on them without their consent, and also for further coercion. The offer to "buy one's life" by assuming the functions of a secret agent is a form of blackmail, using compromising information, that is, personal data, for illegal purposes. Nevertheless, a shift in oversight emerged only in 1952, in the resolution of the Central Committee of the Communist Party of the USSR (1952), "On the situation in the Ministry of State Security of the USSR," where it was proposed "to decisively end the lack of control in the activities of the bodies of the Ministry of State Security and place their work under the systematic and constant control of the party" (Izvestia of the Central Committee of the CPSU, 1991).

Turning to the issue of official surveillance mechanisms, the procedure for wiretapping and recording conversations was described in detail in the monograph by Stetsovsky (2000) "The Right to Freedom and Personal Inviolability. Norms and Reality," where the author wrote that it was officially believed that "in the USSR, no dossiers (files) containing information about the identity and activities of citizens could be formed,

since this contradicts the essence of democratic rights and freedoms. One cannot even accept the possibility that state bodies in the USSR could have formed such dossiers" (Novoselov, 1976). However, the problem was not so much the existence of such dossiers, which simply put the private lives of citizens on display, but the fact that people did not reliably know whether a dossier had been opened on them, and even if they did, they could not familiarize themselves with the information contained therein. Furthermore, the regulatory legal acts related to this area were not accessible (Markomenko, 1997; Matuzov, 1966 & 1972). Notably, individuals were deliberately excluded from any legal procedures that would allow them to identify, access or verify information collected about them. Later attempts were made to exclude from registration documents items that lacked legal significance, such as information on nationality or social origin. Nonetheless, the Resolution of the Central Committee of the CPSU stated: "State and public organisations shall be prohibited from making changes or additions to the personnel record sheets and questionnaires approved by this Resolution" (Resolution of the Central Committee of the CPSU, 1955).

Alongside the realities of state surveillance, a new phase in legal responses emerged with the Criminal Code of the RSFSR (1926), which for the first time introduced independent offenses, establishing criminal liability for violating the privacy of correspondence, telephone conversations, and telegraph messages (Art. 135), and for violating the inviolability of the home (Art. 136). Building on this, the Constitution of the USSR (1936) would specifically stipulate that "the privacy of correspondence shall be protected by law" (Art. 128). It should be noted that even before the Constitution (1936), secrecy of correspondence was provided (though not a constitutional guarantee), and its protection was ensured by criminal and criminal procedural legislation, for example, the Criminal Code of the RSFSR of 1926. Moving forward, the Constitution of the USSR (1977) reaffirmed the provisions according to which the secrecy of correspondence, telephone conversations, and telegraph messages is protected by law (Art. 56), thus emphasizing that there is data and information that is different from state data, and the law separately guarantees the protection of people's personal data. Zharova and Elin (2017) believe that the inclusion of this category of legal relations in the Criminal Code (1961) confirms the significance of such legal relations for the legislator: Art. 135 was providing for liability for violating the privacy of correspondence,

telephone conversations, and telegraph messages of citizens. In this regard, these provisions of Russian law can be compared with American concepts of confidentiality or privacy, as discussed earlier in the work of Warren and Brandeis (1890).

3.1.3 The reorientation process of Soviet legislation to international standards

In 1948, Soviet legislation started to align with international standards after the UN's adoption of the Universal Declaration of Human Rights. However, almost 30 years later, in December 1976, the International Covenant on Civil and Political Rights was adopted and entered into force in the USSR. Pranitskaya (2010) considers this a major step forward for the Soviet approach. The Covenant, following the 1948 Act, sets out the principle that arbitrary or unlawful interference with anyone's private or family life, as well as with their correspondence, is inadmissible. It also guarantees protection of this right from interference or infringement (Art. 17 of the International Covenant on Civil and Political Rights, 1976).

As a result, the UN Declaration's principles from 1948 were finally set in Soviet law. This took the form of the principle of a "harmonious combination of public and private" (Dozhdev, 2008). Soviet society came to recognize the existence of a sphere of human life in which a person is guaranteed some independence from society and the state, organisations, or neighbors, except in necessary cases (Turgarinov, 1965). Pranitskaya (2010) argues this allowed Soviet scholars to justify the need for a separate legal institution to ensure the privacy of a citizen's personal life. It would also prohibit dissemination of information about a person (including in the media) without their consent.

From 1993 to 2011, Russia actively negotiated joining the WTO. In November 2001, Russia needed to meet the organisation's requirement to sign the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, commonly known as Convention 108 (1981). This international treaty set a legal framework for protecting people's personal data during automated processing. It became the basis for Russian law on personal data, leading to the adoption of the Federal Law "On Personal Data" on July 27, 2006.

3.2 The contemporary institutional framework of personal data protection in Russia after 1993

3.2.1 Constitutional foundations of privacy and personal data protection in post-Soviet Russia

Scholars note that in the history of Russian jurisprudence, the right to privacy and personal data protection was recognized by scholars much earlier than it was enshrined in law (Bogoraz, 1998; Nersesyants & Slavin, 1993; Nikolaychik, 1973). However, it was only after the collapse of the USSR that the development of a modern system for personal data protection began, specifically with the first steps towards legal regulation of this new institution.

First and foremost, the Constitution of Russia (1993) is the first to enshrine the right to privacy: "Everyone has the right to privacy, personal and family secrets, and the protection of their honor and good name" (P. 1, Art. 23). Building on this foundation, the Constitution (1993), in a significantly broader, more comprehensive, and more detailed manner than its predecessors, enshrines and guarantees various aspects of the right to privacy, including the secrecy of correspondence, telephone conversations, postal, telegraphic, and other communications (Art. 23). Restrictions on this right are permitted only by court order. The collection, storage, use, and dissemination of information about an individual's private life without their consent are prohibited (Art. 24). Avdeev (2017) writes that such provisions of the Constitution allow us to conclude that, in the end, the principle of privacy has taken precedence over the principle guaranteeing the right to receive information, despite the fact that privacy protection was definitely a new area for Russian law in 1993.

Voinikanis et al. (2014) write, "Despite the fact that the concept of personal data is not precisely used in the Constitution of Russia, the authors of some authoritative commentaries note that P. 1 of Art. 24 of the 1993 Constitution establishes the fundamental principles for processing personal data." The authors further cite the opinion of Gadzhiev, a renowned scholar and judge of the Constitutional Court of Russia: "From the perspective of P. 1 of Art. 24 of the Constitution, the most vulnerable information is that which can be used to identify an individual and which is outside the

constant control of that individual." Russian legislation classifies this type of information as a separate category of "personal data." This classification, although overlapping with the definition of "private information," is not entirely identical to it. Zharova and Elin (2017) believe that the constitutional principle defines the right of every person to the privacy of any information relating directly or indirectly to an identified or identifiable individual (the subject of personal data). Accordingly, this constitutional principle is directly related to personal data.

3.2.2 From fragmented bylaws to the 1995 Federal Law: the initial legal framework for personal data in Russia

Ryzhov (2015) argues that bylaws regulated rapidly developing information relations, or, more precisely, their individual aspects, in the first half of the 1990s. These bylaws did not form any overall functional system. Ryzhov writes: "Therefore, it quickly became clear that a basic legislative act was needed that could serve as a starting point for the formation of such a system." The adoption of Federal Law No. 24-FZ "On Information, Informatization, and Information Protection" (hereinafter, the 1995 Federal Law) in 1995 was the first attempt to regulate the collection, processing, storage, and accounting of data. However, it lacked specific provisions on personal data. This was primarily due to the growth of digital technologies. Banks, telecom operators, and state registries, such as the Russian Pension Fund and Sberbank, began actively collecting personal data, but there were no clear rules governing this.

There is a legal need to enshrine the right of citizens to protect their personal data, as well as to prohibit organisations from collecting, storing, and using individuals' personal data without their consent. This is particularly true because the improper use of such information violates the right to privacy. It also violates the constitutional prohibition on collecting, storing, using, and disseminating information about a person's private life without their consent and knowledge. As noted by Bachilo and Volokitin (1996), with the adoption of this Federal Law, "for the first time in Russian legislation, a crucial step has been taken to regulate relations related to the creation of conditions for the realization of the right to information and affecting the interests of both the state and each citizen." In this case, the legislator considers the object of legal regulation not the content or meaning of information or the tangible medium of information, but

documented information (documents) as a whole. The law covers the information space, the backbone of which is documented information (documents) and the information resources formed on its basis. Furthermore, historical analysis shows that ensuring confidentiality initially rested on moral and ethical norms. As legal regulation developed, this evolved into criminal liability (Popova, 2022).

The law was aimed at regulating relatively new legal relations in Russia: the protection of information and the rights of subjects participating in information processes and informatization. Thus, the term "personal data" first appeared and was legally enshrined in this law: personal data, or in other words, information about citizens, is information about facts, events, and circumstances in a citizen's life that allows for their identification (Art. 2 of the Federal Law No. 24-FZ, 1995), and personal data was classified as confidential information (P. 1, Art. 11 of the Federal Law No. 24-FZ, 1995). The term "personal data" was subsequently redefined and further detailed in 1997 in Decree No. 188 of the President of Russia "On Approval of the List of Confidential Information." Personal data was defined as a category of confidential, restricted information, consisting of "information about facts, events, and circumstances of a citizen's private life that allow for their identification, with the exception of information subject to dissemination in the media in cases established by federal laws" (Clause 1 of the Decree No. 188, 1997). Zharova and Elin (2017) believe that, based on the provisions of this Decree, "information about facts, events, and circumstances of an individual's private life, based on which an individual can be identified, constitutes the individual's private life."

The law prohibited the collection, storage, use, and dissemination of information about a person's private life, as well as information that violates personal privacy, family secrets, the privacy of correspondence, telephone conversations, postal, telegraphic, and other communications of an individual, without their consent, except on the basis of a court decision (P. 1, Art. 11 of the Federal Law No. 24-FZ, 1995). The law stipulated that personal data could not be used to cause property or moral harm to citizens, or to impede the exercise of their rights and freedoms (P. 2, Art. 11 of the Federal Law No. 24-FZ, 1995). The same section and article also prohibited the restriction of the rights of Russian citizens based on information about their social origin, race, nationality,

language, religion, or party affiliation. It also stipulated that the activities of non-governmental organisations and individuals related to the processing and provision of personal data to users were subject to licensing.

This Federal Law has been repeatedly criticized. For example, Avdeev (2017) said that the law was framework-based and contained numerous references to other regulations that had not yet been developed at the time of its adoption. These regulations were supposed to detail the procedures and guarantees for the protection of personal data, including requirements for its collection, storage, and processing. As a result, the law was impossible to fully implement in practice. Specifically, there were no mechanisms to enforce its provisions, particularly regarding the protection and defence of citizens' rights in the information sphere. This situation demonstrated that more specific, detailed legislation was required to effectively regulate information relations and protect personal data. Furthermore, another problem, according to Sekste and Markevich (2020), was the uncertainty and vagueness of the scope of social and information relations in the area of protecting individuals' privacy, which hindered the law's proper implementation. For instance, the 1995 Federal Law at the federal level codified the basic requirements and conditions for processing personal data only for Russian citizens, thereby excluding stateless and dual citizens from legal regulation.

3.2.3 From international commitments to the Federal Law No. 152-FZ (2006): the formation of the modern personal data protection framework in Russia

Regarding the immediate formation of the modern institution of personal data protection, its emergence is generally associated with the agreements reached at the Fourteenth Russia-EU Summit in 2004 (The Hague, 2004) and with Russia's signing in November 2001 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The Convention requires signatory countries to impose their own technical requirements for the protection of personal databases by their controllers—companies that process personal data. To implement this, countries must adopt a personal data law that enshrines these requirements. Prior to the issuance of this law, it was possible to declare the processing of personal data illegal under the Convention, but no such precedents are

known. Korzhov (2011) believes that the Convention was formally adopted but not effectively implemented due to the lack of Russian regulations.

In a joint press statement following the summit, Russian and EU leaders emphasized that "a good basis has been created for closer cooperation on issues such as facilitating the movement of people, advancing the agreed long-term goal of visa-free travel, readmission, border management, migration, and the fight against terrorism, organized crime, corruption, and human trafficking. Judicial cooperation will also be strengthened within this common space" (Russia-EU Summit, 2004). The visa-free regime, as well as the ability to exchange data with Europol and Interpol, became incentives for the accelerated implementation of the new legislative institution. The signing of the Convention and the joint agreements reached at the Summit resulted in the accelerated introduction of a package of four bills, as stipulated by the Russian Government Instruction No. АЖ-П4-3825, as early as August 2005:

- Bill No. 217346-4 "On Ratification of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;"
- Bill No. 217352-4 "On Personal Data;"
- Bill No. 217354-4 "On Information, Information Technology, and Information Protection;"
- Bill No. 217355-4 "On Amendments to Certain Legislative Acts of Russia in Connection with the Adoption of the Federal Law "On Ratification of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" and the Federal Law "On Personal Data."

These documents were the result of an interdepartmental working group's efforts to develop a set of measures necessary for ratification of the Convention: in September 2005, a bill ratifying the Convention was adopted, and in 2006, two other bills, one on information and one on personal data, were successfully passed.

Federal Law No. 152-FZ "On Personal Data" of July 27, 2006, is considered revolutionary in the regulation of personal data, as it codified the concept of "personal data" and the principles of its processing: legality, consent, intended purpose, legal validity and good faith, minimization, limited storage periods, confidentiality, security guarantees, and information transparency (Art. 5). Furthermore, the law obligated operators to protect data (including the requirement to localize databases within Russia as of 2015). This law also created a separate regulatory body, the Federal Service for Supervision of Communications, Information Technology, and Mass Media (better known as Roskomnadzor), which began regulating communications, information technology, and the media and ensuring the protection of personal data.

It is stated that personal data is any information that directly or indirectly identifies an individual acting as the subject of the personal data (Art. 3). The list of personal data is not exhaustive; it may include any other information that allows an individual to be identified. This definition corresponds to the broad understanding of personal data set out in Convention 108 (Art. 2). A subject of personal data is any individual (Art. 3) who owns the following data: name, date of birth, telephone number, email address, tax identification number (INN), passport information, and even biometric data. In other words, any information that allows for the identification of an individual. Each subject has the right to know what data is being processed, for what purposes, and to request the correction or deletion of inaccurate information or if it has become inaccurate.

Any company collecting information about clients, employees, or other individuals is obligated to comply with Federal Law No. 152-FZ on the Protection of Personal Data. Violations are punishable by fines and reputational damage, as the requirements have become significantly more stringent since 2025. Fines for data leaks have increased to 5 million rubles (€52,898); for compromising biometric data, up to 15 million rubles (€158,694); and for spam mailings without consent, up to 700,000 rubles (€7,405), with the risk of resource blocking (Ayrapetyan, 2025). By law, a personal data operator is a legal entity or individual that, independently or jointly with other organisations, processes personal data, determines the purposes of data processing, as well as the methods and scope of such processing (Art. 3). Companies that process full names,

email addresses, or employment information automatically qualify as personal data operators and are obligated to comply with all established requirements.

The operator has the right to carry out the full processing cycle: from collection to destruction of information, including collection, recording, accumulation, storage, use, transfer, analysis, and blocking. According to the law, the processing of personal data includes any actions with data: collection, recording, systematization, accumulation, and storage (Art. 3). Responsibility for compliance with the law on personal data protection lies squarely with the operator. This means they must ensure the lawfulness of processing, protect data from leakage, provide the subject with access to their information upon request, and obtain the subject's consent to processing (Art. 6). Consent must be informed: it is important for the person to understand what data is being collected, for what purpose, for how long, and to whom it may be transferred (Art. 9). For example, adding a client to a mailing list without explicit consent violates the law. From September 1, 2025, consent must be formalized separately and cannot be included in contracts or other documents. As follows from the explanatory note to the bill, the new requirement should "eliminate the legal uncertainty that allows unscrupulous personal data operators to "disorient" citizens in matters of consent to the processing of their personal data, determining the conditions and purposes of processing such data" (Gosudarstvennaya Duma, 2024).

In the Federal Law No. 152-FZ (2006), it is also stated that the operator is obligated to take technical and organisational measures, including encryption, backups, restricting employee access, and staff training (Art. 19). Any unauthorized access or data leakage is the operator's responsibility. Furthermore, the operator is obligated to notify Roskomnadzor of the commencement of personal data processing prior to the actual data collection, and if the purposes or methods of processing change, another notification must be submitted (Art. 22). The purpose of this innovation is to allow the state to monitor compliance with regulations and prevent violations. If data is transferred outside of Russia, the operator must ensure that the foreign state ensures adequate information protection (Art. 12). For example, storing customer databases on foreign servers requires approval from Roskomnadzor. All data of Russian citizens must

be stored and processed on servers located exclusively within the country. Exceptions are permitted only with Roskomnadzor's approval (Art. 18).

Also, starting in 2025, operators' liability for violating personal data protection laws has been increased and enshrined in the Code of Administrative Offenses of Russia (2001). Thus, if a personal data leak occurs from a company's databases, a fine of up to 20 million rubles (approximately € 210,771) is imposed (Art. 13.11). For a repeat violation, the fine is up to €500 million (€5,269,290) or a turnover-based fine of 1-3% of annual revenue. Failure to notify Roskomnadzor of the commencement of personal data processing will result in a fine of up to €300,000 rubles (€3,161). For processing personal data without the subject's consent when required, the fine is up to €700,000 rubles (€7,377). For violating data localization requirements in Russia, the fine is up to €6 million (€63,231) (Art. 13.11).

However, the law has been repeatedly criticized, primarily because it remained a "framework" for a long time. Real protection mechanisms (such as liability for leaks) were introduced only in the 2010s, and the penalties for leaks were not as severe as they are now. During the first two years of its implementation, the law was practically ignored. This was due to the supervisory authority's limited activity: according to a 2008 report, only 76 inspections were conducted and 146 citizen complaints were reviewed, as well as the lack of amendments to other laws and regulations that would detail the regulations and facilitate their precise application. Furthermore, requirements for personal data information systems only came into force in 2010 (RTM Group, 2023).

Korzhov (2011) believes that the law initially granted greater rights to the subject of personal data, while the majority of citizens are also data operators. At the same time, he specifically points out that there were significant difficulties in implementing this law, for example, with mandatory certification of security tools for personal databases, certification of objects, and protection of so-called special types of personal data. The requirements were excessively high, but they could only be imposed on new systems, since the law is not retroactive. It was necessary to update a huge number of systems already in effect at that time and the standards for working with them. Until 2010, companies had to bring such systems into compliance with the new standards, and only

after January 1, 2010, all companies without exception must comply with the regulators' instructions. Only then could inspections be conducted for compliance with technical requirements. In a letter dated September 9, 2009, No. SS-05-3/6055 addressed to the Minister of Communications and Mass Media of Russia, Acting In Shchegoleva, Roskomnadzor head Sitnikov writes about the lack of financial resources among operators "to comply with the requirements established by Federal Law and the aforementioned agencies (Roskomnadzor, 2009). In this letter, Roskomnadzor also notes that "the current legislative framework ensures the protection of information itself, not the rights of citizens when their personal data is processed in information systems" (Roskomnadzor, 2009).

In its letter to the Ministry of Communications of Russia dated September 14, 2009, No. 23-5-2-5/1914, the Bank of Russia points to "the strictness of certain provisions of the Federal Law "On Personal Data" and regulatory bylaws, which effectively prevent their implementation" (Central Bank of Russia, 2009). According to Roskomnadzor data as of August 2009, only five federal executive bodies (the Ministry of Culture of Russia, the Ministry of Emergency Situations of Russia, the Ministry of Natural Resources of Russia, the Federal Tariff Service of Russia, and the Federal Security Service of Russia) declared their full readiness to comply with the Law's requirements for personal data information systems. The remaining federal executive bodies were not prepared to implement the standards and norms established in the Law (Roskomnadzor, 2009).

Recognizing the impossibility of complying with the requirements of the Law on Personal Data and its bylaws led to a postponement of the entry into force of the requirements for personal data information systems, as well as to the adoption in 2011 of significant amendments to the Law (effectively a new version), eliminating some of the restrictions on personal data processing and reducing the financial costs of its implementation. Unfortunately, even in its current, "amended and supplemented" version, the Personal Data Law retains two fundamental shortcomings: its formal nature and the lack of protection for the interests of personal data subjects. Korzhov (2011) notes that the new version of the law removes some of the most difficult-to-implement requirements of the old law, such as those related to obtaining consent and justifying the

processing of personal data. However, the law itself now requires a "conformity assessment" of protection against security threats.

By 2025, the legal framework regulating personal data is estimated to be quite extensive (RTM Group, 2023). The primary law remains Federal Law No. 152-FZ of July 27, 2006, "On Personal Data," but a number of other laws, regulations, and other acts are also in effect:

1. Federal Law No. 149-FZ of July 27, 2006, "On Information, Information Technologies, and the Protection of Information;"
2. RF Government Resolution No. 1119 of November 1, 2012, "On Approval of Requirements for the Protection of Personal Data When Processed in Personal Data Information Systems;"
3. The Regulation on the Specifics of Personal Data Processing Carried Out Without the Use of Automation Tools was approved by RF Government Resolution No. 687 of September 15, 2008 (687-P);
4. FSTEC Order No. 21 of February 18, 2013, "On Approval of the Composition and Content of Organisational and Technical Measures to Ensure the Security of Personal Data When Processed in Personal Data Information Systems;"
5. Methodology for Identifying Current Threats to the Security of Personal Data When Processed in Personal Data Information Systems (FSTEC of Russia, 2008);
6. Basic Model of Threats to the Security of Personal Data When Processed in Personal Data Information Systems (February 15, 2008);
7. Database of Information Security Threats (FSTEC);
8. GOST R 50922–2006 "Information Security. Basic Terms and Definitions". Moscow: Standartinform, 2008;
9. GOST RISO/IEC 27002–2012 "Information Technology. Security Methods and Tools. Information Security Management Standards and Rules."

3.3 Current issues and trends in Russian personal data protection

3.3.1 Gaps, ambiguities, and contradictions in personal data legislation implementation: analysis of Russian case law and judicial practice

In recent years, judicial practice protecting the rights of personal data subjects has expanded significantly. Gude et al. (2015) believe that currently accepted practice in the field of personal data protection lies in a reasonable balance of the interests of the individual, the state, society, and business: "this balance is a necessary compromise to ensure the validity and feasibility of adopted requirements."

Judicial practice protecting the rights of personal data subjects in Russia covers a wide range of categories, the most common of which are: unlawful collection, processing, or transfer of personal data; violation of the rights of personal data subjects to access their information; data leakage and security breaches; and the use of personal data without consent. However, judicial practice is quite varied. Roskomnadzor plays a special role in data protection disputes, as it has key powers to monitor compliance with the relevant legislation.

The first difficulty concerns proper jurisdiction determination, as the Russian judicial system is extensive and complex. For example, magistrates and district courts (lower courts of general jurisdiction), which serve as first-instance courts in cases involving personal data, are not always able to determine how to handle such cases on the first try (Kondratieva, 2020). For example, in a case against Whois Privacy Corp., a man filed a complaint with Roskomnadzor. He claimed that the Bahamas-based company, Whois Privacy Corp., had distributed his personal data online without his permission. Roskomnadzor filed a complaint on his behalf, demanding that his rights as a personal data subject be protected and that access to information about him be restricted. The Khabarovsk Central District Court, where the claim was filed, refused to accept it, ruling that the applicant's claims were administrative in nature and should not be considered as civil proceedings. The appeals court agreed with this position and held that Roskomnadzor's claims concern the administrative regulation of an online resource's legal activities as a media outlet; accordingly, the first instance's conclusions on the administrative review of the dispute were correct. The Civil Cases Panel of the

Supreme Court, chaired by Judge Astashov, found the lower court's error. The application should have been considered through civil proceedings, in accordance with the ruling in the case (*Opredelenie Sudebnoy kollegii po grazhdanskim delam No. 58-KG20-2*, 2020).

Kondratieva (2020) refers to the opinion of Sozina, a lawyer with the law firm AB Vertikal, points out that claims related to the violation of rights to personal data processing are considered through civil proceedings based on the provisions of the Civil Procedure Code (for example, *Apellyatsionnoye opredeleniye Moskovskogo gorodskogo suda No. 33-35187/2019*, 2019). However, administrative cases are the exception rather than the rule under certain circumstances. "Despite the rather specific nature of the claims and the often complex nature of the structure, expert examinations in personal data protection lawsuits are ordered by the court in exceptional cases. This means that the courts independently assess whether certain information constitutes personal data and whether it is subject to protection under the specified procedure, meaning that the approach to personal data protection is shaped by judicial discretion" (Kondratieva, 2020).

As of May 30, 2025, a significant shift occurred: all cases under Art. 13.11 of the Code of Administrative Offenses of Russia (2001) concerning violations of personal data were transferred from the jurisdiction of justices of the peace or district courts to arbitration courts. Arbitration courts traditionally specialize in economic disputes and matters related to business activities, which is essential for law enforcement in the area of personal data. This is due to the need for a more qualified approach to cases requiring economic and legal expertise, as judicial practice shows that magistrates and district courts are courts of general jurisdiction that hear a wide range of cases, often lacking specialized training in economic or technical matters related to personal data protection. This has indeed led to unpredictable and fragmented judicial practice, with decisions often dependent on the qualifications and subjective views of individual judges.

Here, another important issue for judicial practice was raised: the ambiguous interpretation of the term "personal data." The definition of personal data remains one of the most confusing issues, primarily because the definition enshrined in legislation is broad, and the list of what may constitute personal data is not exhaustive. This approach

reflects the deliberately open-ended definition of personal data introduced by Convention 108 and subsequently adopted in EU and other Western data protection regimes. This means that the court itself must decide in each specific case whether certain information constitutes personal data. Court cases clearly demonstrate how diverse information can be interpreted. "Classic" personal data includes an individual's full name, as it allows them to be identified among others (Bychkov, 2021). This opinion is also supported by judicial practice, which holds that "Banks cannot distribute payment cards with open customer data, and management companies cannot send out payment documents in clear text, since in such cases, people's personal data is not protected from accidental access by third parties" (*Apellyatsionnoye opredeleniye Samarskogo oblastnogo suda No. 33-12118/2019*, 2019).

However, in addition to a full name, an individual's personal data also includes their specific residential address, including the city, street, house number, and apartment number, but not a full address (for example, without specifying a specific apartment), no longer allows for the identification of a specific subject of personal data (Bychkov, 2021). For example, the court considers it a typical violation on the part of the management company managing a residential building to post information on the presence of arrears in electricity and utility bills for specific individuals, with their apartment numbers, on the front door leading to the entrance, on billboards, and in other publicly accessible places. This information pertains to the private life of specific individuals, so its disclosure will be considered a violation, which gives the injured party the right to demand monetary compensation for moral damages on the basis of Art. 151 of the Civil Code of Russia (*Resheniye Moskovskogo raionnogo suda g. Kaliningrada No. 2-688/2017*, 2017). At the same time, posting information about arrears on electricity and utility bills, with a list of the corresponding apartments, but without specifying personal data such as full names, will not be considered a violation (*Apellyatsionnoye resheniye Sverdlovskogo oblastnogo suda No. 33-15137/2019*, 2019).

Bychkov (2021) also points out that a citizen's personal data includes the year, date, month, and place of birth, marital and property status, educational level, income, and other information that can identify a specific individual. A citizen's passport series and number, which constitute a unique combination of digits on the primary identity

document, can also be considered personal data. The Roskomnadzor Methodological Recommendations of May 30, 2017, state that personal data unambiguously includes: last name, first name, patronymic, date and place of birth, permanent residence address, information on marital status, social status and property, information on education, professional activity and income (Roskomnadzor, 2017).

Furthermore, in 2022, in a case against Facebook Inc., the court, in its *Postanovleniye Vtorogo kassatsionnogo suda obshchey yurisdiktsii No. 16-707/2022* (2022), identified a broad range of personal data that Facebook processes and designated this list as the personal data of Russian data subjects. This list included the following personal data:

1. Information about health, race, religious beliefs, and political views;
2. Contact information from a mobile device (including address book, call log);
3. Transaction information and location data;
4. Passport information (in some cases, for identity verification);
5. Information about applications, browsers, and devices that the user uses to access Facebook products;
6. Unique identifiers (such as the user's mobile phone identification number), as well as information about the browser and device type and settings.

The Perm Regional Court also considers profession and education to be personal data, as they can identify a specific individual. However, some experts, such as Bychkov (2021), argue that profession and education alone should not be considered personal data, as they are common to many people and not sufficiently unique to identify an individual. The key factor here should be how this data is used. If information about a profession or education is combined with other data (for example, full name or place of residence), it becomes uniquely identifying and, therefore, personal data.

For example, in the Arsenal Insurance Company case, the court found that publishing the company's management data on its website complied with information disclosure laws. Moreover, the purpose of such publication, fulfilling regulatory obligations, was the determining factor in its legality (*Postanovleniye arbitrazhnogo suda Moskovskogo*

okruga No. Ф05-4354/2023 in re No. A40-139096/2022, 2023). A different view is presented in the Farpost DV case. The court stated that posting data online, unless it identifies a specific individual, cannot be considered personal data processing. Therefore, processing issues apply only to information that clearly relates to a specific individual (*Postanovleniye Arbitrazhnogo suda Zapadno-Sibirskogo okruga No. F04-1436/2023 in re No. A27-13261/2022*, 2023).

Furthermore, the Supreme Court of Russia rejected Roskomnadzor's claim and did not recognize an email address as personal data in a case involving an insurance company regarding the processing of personal data on its website. The primary complaint was the insurance policy form, which requested the visitor's email address and phone number. According to the courts, it is impossible to identify a specific individual based solely on an email address. Therefore, an email address is not personal data. Furthermore, the courts noted that the form on the website is used as a feedback tool and is not intended to identify a consumer of financial services. The court also found that this form does not allow for the precise identification of an individual based on the provided phone number or email address, as it does not require full personal data or identifiers, such as passport information or INN. The court noted that email addresses are not permanent either, and if an account is deleted, the same address may be re-registered by another user. This is similar to the process of re-registering a telephone number to a new subscriber after terminating the contract with the previous one (*Opredeleniye Verkhovnogo Suda RF No. 305-ES23-12160 in re No. A40-139096/2022 "On the refusal to transfer a complaint to the Judicial Collegium of the Supreme Court of Russia", 2023*).

At the same time, lawyers Arkhipov et al. (2023) expressed the opinion that such a position of the Supreme Court of Russia is highly vulnerable to criticism from the standpoint of a literal interpretation of the provisions of the law, as well as the position of regulatory executive authorities in this area and doctrine, such a position runs counter to global practice in determining personal data. Here, the following is outlined: the law does not define the ability to uniquely identify a person as a characteristic of personal data. Russian judicial practice has established positions that information should be considered personal data not by the criterion of "full identification," but by virtue of its "relevance" to a specific or identifiable individual, including through the use of other

information. For example, information collected through cookies and IP addresses has been classified as personal data.

Therefore, lawyers point out that the law does not mandate the unambiguous identification of the subject of personal data. A crucial factor is the ability to determine that a given data set belongs to a specific or potentially identifiable individual, even when that individual is not clearly identified: "Otherwise, we would have a situation in which, for example, information collected using cookies, IP addresses, and any other identifiers such as residential address, telephone number, or place of work would not be considered personal data. This would mean that such data would not be protected by the Federal Law "On Personal Data," thereby significantly infringing on citizens' rights. For example, this would mean that the collection of such data would not require the consent of the subject" (Arkhipov et al., 2023). Furthermore, the position that an identifier must be immutable to be considered personal data appears controversial, since, in general, virtually any personal data is mutable, except that associated with certain immutable personal characteristics (e.g., biometric personal data). For example, a person's first name, last name, passport number, or phone number can be changed. Finally, the assertion that data collected for purposes other than identification is not personal data lacks legal grounds.

3.3.2 Between digital efficiency and data sovereignty: Russia's security-oriented regulatory model of personal data regulation in the era of digital platforms

Zharova and Elin (2017) believe that in contemporary Russian public consciousness, privacy is primarily understood as the right to be left alone, secrecy, or the option to conceal information from others. Citizens recognize the state's right to control them in cases of ensuring the security of the state, society, and citizens (secrecy as an option for concealing information from others). A distinctive feature of public consciousness is the recognition of the state's right to control the principle of states' privacy (vs. states of privacy) in cases of ensuring the security of the state, society, and citizens, i.e., "a state in private life" (and not "a state for private life"). As Ivansky and Melnichuk (2017) rightly observes, "the state tries to find a balance between citizens' need for the free exchange of information and restrictions associated with ensuring national security. As a

result, Russians are less likely than Westerners to oppose surveillance in the name of security.

By 2025, Russia had developed a comprehensive Federal State Information System, the "Unified Portal of State and Municipal Services (Functions)" (better known as Gosuslugi). This service provides remote access to key state and municipal services, necessitating the consolidation of citizens' personal data. Over 117 million Russian citizens are currently registered on the Gosuslugi portal, approximately 95% of Russians over the age of 14. More than 10 million people use Gosuslugi services daily (Pylaev, 2025). The portal not only allows you to pay state fees and submit service requests, but also, for example, block loans issued in your name or obtain information about all SIM cards registered to you, so this is literally another layer of personal data that needs to be protected. Furthermore, in 2025, the Unified State Register of Civil Status Acts (EGR ZAGS) became fully operational, digitizing over 560 million birth, death, and marriage records (Skan, 2025). This also enabled the launch of the "Birth of a Child" platform, which allows mothers to obtain a birth certificate immediately after giving birth through Gosuslugi and quickly obtain an extract from the EGR ZAGS. In parallel, the Unified Biometric System was introduced in 2018, allowing banks and government agencies to remotely identify citizens using fingerprints and facial images. This allows people to pay in stores or on the subway simply with a smile (Global Fact-Checking Network, 2025). Roskomnadzor is also implementing AI systems to automatically monitor websites to verify the validity of consent forms (Ayrapetyan, 2025).

This growth in digital services and databases that aggregate vast amounts of citizen information improves service efficiency (e.g., the convenience of "super services," targeted payments, etc.), but increases the risks of leaks and surveillance. This stimulates the development of data protection institutions and stricter controls, and also raises the question of modern legal regulation. For example, a plaintiff learned through the Gosuslugi website about a lawsuit against him regarding an allegedly concluded loan agreement. The plaintiff did not enter into any agreement and did not consent to the provision of personal data. Ultimately, the court upheld the plaintiff's claims, terminated the contract, and awarded the plaintiff damages (*Resheniye Zyuzinskogo rayonnogo*

suda (Gorod Moskva) No. 02-1758/2023 [M-8517/2022], 2023). In another case, the plaintiff filed a lawsuit alleging that unknown individuals, using his personal account on the State Services portal, had verified his identity and remotely entered into a loan agreement on his behalf, the proceeds of which were then transferred to the fraudsters. The court concluded that the borrower had failed to properly verify the validity and authenticity of the plaintiff's consent to the processing of his personal data and had failed to verify that the expression of intent to enter into agreements and provide personal data for processing and transfer came from the proper person, that is, from the subject of the personal data, which resulted in the plaintiff's negative credit history. The agreement was declared invalid and the funds were ordered to be returned (*Resheniye Presnenskogo rayonnogo suda (Gorod Moskva) No. 02-0522/2023 [02-9418/2022; M-8559/2022],* 2023).

Furthermore, citizens' demands for personal data protection are growing. According to a survey by the Garda Center for Data Protection, in 2025, only 3% of Russians will not react to data leaks. Conversely, 55% consider data compromise a serious problem, and 51% would stop using a company's services if a data leak is the company's fault (Bystrova, 2025). The growing concern among ordinary people reinforces the trend toward stricter legislation and requirements for companies: trust is quickly lost and difficult to restore (every major leak undermines the entire digital sector's reputation). This intensifies the debate about the trade-off between the convenience of such digital systems and the risks of total surveillance or data leaks. On the one hand, the unification of services improves quality of life and access to care, but on the other, people are increasingly concerned about their data being concentrated in the hands of the state or companies, sold, or leaked to other companies. According to Raymond and Sherman (2024), Russia is moving toward cybersecurity authoritarianism: the key emphasis is on preventing external threats and internal protectionism, which sometimes runs counter to the principles of a "free internet."

The government responded to data consolidation by strengthening the regulatory framework and increasing penalties for companies that violate personal data protection regulations. In 2014, Federal Law No. 242-FZ was adopted. It concerns "Amendments to Certain Legislative Acts of Russia Regarding Clarification of the Procedure for

Processing Personal Data in Information and Telecommunication Networks" and requires storage of Russian citizens' data on servers within the country (Art. 2). Now, personal data operators, meaning any company or organisation, must indicate the location of the database that processes Russian citizens' personal data.

The most important source in the area of ensuring and protecting personal data was Decree No. 646 of the President of Russia dated December 5, 2016, which approved the Information Security Doctrine of Russia. This legal act specified and detailed the most important constitutional provisions regarding the protection of individual privacy, outlined the main directions of information policy in relation to the country's national interests, and established high standards for information security. In essence, this doctrine formally proclaims privacy as a national interest, but in practice it prioritizes security: the state seeks a balance between freedom of information and control in the name of "sovereignty and security" (President of Russia, 2016).

In 2019, Federal Law No. 90-FZ "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technology, and the Protection of Information" (better known as the "Sovereign Runet Law") entered into force. It provides for the creation of a national internet traffic routing system and centralized management tools, essentially requiring the installation of FSB technical means (a DPI filter) on provider networks and the creation of a national domain name system. This infrastructure would enable routing control and traffic filtering at the agency's discretion. The need for the bill was explained by the "aggressive nature of the US National Cybersecurity Strategy adopted in September 2018," which provides for the ability to shut down the internet in hostile states. One of the bill's sponsors, Senator Klishas A., emphasized that the amendments to the laws "do not provide for new powers to block prohibited information. It is only proposed to change the technology for blocking it..." (Klishas, 2021). Supporters of the law justify its adoption by citing the need to ensure Russia's security in the event of its disconnection from the internet. Although the law is described as protection against external cyberthreats, experts immediately warned of the risk of censorship and excessive surveillance, and also expressed the opinion that it is technically possible to disconnect the RuNet from the global network upon external command (Prokopenko, 2019; Chernyshova, 2022).

Currently, the debate over personal data protection in Russia is being conducted between businesses and the government, without including ordinary people. Despite the fact that neither businesses nor the government are subjects of personal data, they are discussing about others, not about themselves. Combined with purely bureaucratic regulatory methods, this essentially morphs into a discussion about a convenient procedure for protecting personal data that addresses security risks (for the state) or property losses (for businesses). Sekste and Markevich (2020) attributes this to the continuity of the Soviet system, when the political system of the Soviet state was shaped by the principle of "priority of state interests over personal ones." Nothing "private" was recognized in the Soviet Union, including the right to private property, so under this format, the possibility of protecting an individual's privacy and personal data was not even mentioned. The history of personal data collection in Russia reflects the evolution from uncontrolled recording for the state's benefit to attempts to establish legal guarantees, while the state repeatedly takes steps backward in protecting personal data.

It's enough to recall the 2016 "Yarovaya Law" (the "Yarovaya Package"), aimed at strengthening the fight against terrorist threats, which expanded the powers of law enforcement agencies to interfere with the privacy of certain citizens suspected of organizing terrorist attacks or aiding terrorists. The "Yarovaya Law" expanded the state's ability to collect, process, record, and store personal data without sufficient judicial guarantees against arbitrary interference. Essentially, this shifted the balance in favor of state interests, weakening constitutional protections for citizens' personal data. The Federal Law N 126-FZ "On Communications" (2003) stipulates that Telecom operators are required to store the contents of calls, messages, correspondence, as well as metadata—in simple terms, who communicated, when, with whom, and from where, for up to six months (Art. 64). Such wholesale collection of information is comprehensive, as data is collected on everyone, not just those suspected of terrorism and/or extremism. Moreover, the law did not provide for judicial or independent oversight mechanisms, nor did it give citizens additional tools to control how their data was used.

The "Yarovaya Law" dramatically undermined not only public trust in the institution of personal data protection but also the legal guarantees at the federal level for the lawful

and fair protection of people's data. Against the backdrop of prevailing trends in European and international data protection law, notwithstanding security-driven expansions of surveillance in certain jurisdictions, such as the United States after 9/11, Russia took the opposite step, expanding the state's scope for intrusion into the private sphere. Instead of moving toward standards of "privacy by design" and "data protection as a human right," a rollback to the "state above privacy" model was adopted. In European legal tradition, such practices have already been recognized as violating human rights (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* 2014).

The priority of security over individual rights is becoming unconditional, and the balance enshrined in constitutions is being disrupted, as has happened in Russia. Thus, the "Yarovaya Law" made personal data (including even intimate details of communication) accessible to the state by default, rather than by exception. This has negated the very idea of personal data as a legal object requiring special protection. Sekste and Markevich (2020) raise the question of which government agency is capable of balancing the interests of the individual and the state in ensuring information security, since although Roskomnadzor is empowered to represent citizens in court, it primarily defends public interests. The authors also raise the need to create a public body independent of the state that could serve as a counterweight to the state security system in the area of personal data protection, referring to comparative experiences in jurisdictions such as Belgium, the United Kingdom, and Australia (Sekste & Markevich, 2020). However, none of these models can be considered ideal. For example, before the institutional reforms initiated by the GDPR, serious concerns were raised regarding the independence of the Belgian Data Protection Authority, and national restrictions on supervisory autonomy and compliance with Art. 52 of the GDPR have been repeatedly challenged by the European Commission and commentators (European Commission, 2021; Dimitrova, 2024). This illustrates that foreign regulatory models should not be adopted uncritically, but rather assessed with careful attention to their structural limitations, enforcement practices, and suitability to the local legal and institutional context. Sekste and Markevich (2020) as well emphasize that despite the positive experience of some European countries in forming intermediary public structures to protect individual interests, this point of view is supported by

Ivansky and Melnichuk (2017), who write that "a guarantee can be expressed not only in the ability to be alone, but also in the possibility of legally protecting the information space from the influence of various ideologies, including state ones."

3.3.3 The 2022–2025 regulatory shift: strengthening sanctions and restructuring personal data governance in Russia

In December 2024, a law came into force in Russia that toughens penalties for personal data leaks. First, it significantly increased fines for companies and introduced turnover-based fines of 1% to 3% of annual turnover, with a minimum of 25 million rubles (€265,339) and a maximum of 500 million rubles (€5,306,790). Secondly, criminal liability was introduced for the illegal collection, storage, and distribution of personal data: Art. 272.1 of the Criminal Code of Russia (1996) stipulates that the creation or administration of a website or program designed to store and transmit illegally obtained personal data is punishable by a fine of up to 700,000 rubles (€7,459) or imprisonment for up to five years (Denisenko, 2025).

The latest trend in the field of personal data in Russia is a significant tightening of regulations for the processing of various categories of personal data, increased penalties for personal data leakage or the collection, processing, and storage of personal data in violation of international law, as well as restrictions on cross-border data exchange, which could not but be influenced by the current global situation. Between January 1, 2022, and July 1, 2022, 4,855 court decisions related to the processing of personal data were issued. During the same period in 2023, 5,875 court decisions were issued, representing a 21% increase in personal data-related cases (RTM Group, 2023).

In a recent analysis, Domshenko and Sabirov (2025) reviewed court decisions in more than 100 cases in general jurisdiction courts related to major data breaches over the past two and a half years and concluded that 96% of cases resulted in administrative liability, while 60% of operators admitted guilt in the data breach, mostly due to a reluctance to bear the financial costs of legal representation. Furthermore, a correlation was found between the admission of guilt and the size of the fine imposed on the operators: "those who admitted guilt were fined below the minimum limit in 15% of cases, that is, five times more often than those who did not admit guilt." In turn, operators who did not

admit guilt were 5% less likely to receive the minimum fine, and in 17% of cases they were subject to a fine above the minimum, whereas in cases of guilty pleas, fines exceeding 60,000 rubles (634 euros) were not imposed at all. Regardless of whether the operator admits guilt, the likelihood of receiving a warning remains the same. It can be assumed that the determining factor for issuing a warning to the operator is the conclusion that a specific leak is insignificant. In addition, the study showed that, regardless of the circumstance of the operators' admission of guilt, their liability was distributed as follows: in 75% of cases, the courts imposed the minimum penalty (60,000 rubles / 634 euros), in 10% of cases - even below the minimum (30,000 rubles / 317 euros), and in 7% of cases only a warning was issued to the offender. Punishment in an amount above the minimum, that is, 70,000-100,000 rubles (740 - 1057 euros). Courts currently impose fines extremely rarely,in only 7% of cases (Domshenko & Sabirov, 2025).

This study also showed that operators' admissions of guilt, relatively low fines, and the frequent imposition of minimal fines have led to the formation of a paradigm: "if the authorized body initiates such a case, then the operator is the offender." In only 2% of cases, although the courts found the elements of an offense, they nonetheless released the operators from liability due to its insignificance, without establishing a significant violation of protected public relations (Domshenko & Sabirov, 2025). For example, in the *Postanovleniye mirovogo sud'i sudebnogo uchastka № 456 Danilovskogo rayona Moskvy No. 05-1415/456/2023* (2023) the insignificance was justified by the following factors: the small size of the leak (only one entry), and the personal data were published and then deleted within three minutes and no evidence was presented that anyone had copied them.

Cases related to personal data leaks at AlfaStrakhovanie (*Postanovlenie Mirovogo sud'i sudebnogo uchastka № 244 Donskogo rayona g. Moskvy No. 05-1048/244/2023*, 2023) and Sportmaster (*Postanovleniye Mirovogo sud'i sudebnogo uchastka № 54 Kon'kovskogo rayona g. Moskvy No. 05-0309/52/2023*, 2023) are illustrative in this regard. These cases were dismissed for lack of evidence of an administrative offense. This was not because the leaks were not confirmed, but because the operators were able to convince the court that they had taken all possible and reasonable actions before and

after the leaks. The court rulings do not specify the actions taken by the operators before the leaks, but they state that the operators complied with the requirements stipulated by the Federal Law "On Personal Data" and the regulatory legal acts adopted in accordance with it, in a timely and full manner. The court rulings also indicate what the operators did after the leaks: they terminated access to the compromised database; changed the password for the technological account used to upload information unauthorizedly; reset user passwords; engaged information security consultants; initiated a criminal case under P. 3 of Art. 272 "Unauthorized access to computer security" of the Criminal Code (1996). It is important to note that a new special offense, Art. 272.1 of the Criminal Code (1996), was introduced in December 2024. Based on the totality of the circumstances in both cases, the courts concluded that there was no administrative offense (*Postanovleniye Mirovogo sud'i sudebnogo uchastka № 244 Donskogo rayona g. Moskvy No. 05-1048/244/2023*, 2023; *Postanovlenie Mirovogo sud'i sudebnogo uchastka № 54 Kon'kovskogo rayona g. Moskvy No. 05-0309/52/2023*, 2023).

According to the Federal Law N 152-ФЗ "On Personal Data" (2006), operators are required to notify the authorized body of a data breach (Part 3.1, Art. 21). However, on May 30, 2025, an amendment came into force introducing a new administrative offense—the failure to notify the authorized body of a data breach or the late notification of a data breach. Domshenko and Sabirov (2025) indicate that "judging by the global trend, operators often fail to notify authorized bodies of data breaches; current Russian judicial practice shows that 82% of operators did send notifications." The authors also predicted that, after May 30, 2025, approximately 18% of operators who fail to notify of a data breach could be subject to administrative liability under the new offense, which carries a fine of between 1 and 3 million rubles (10,574 and 31,722 euros).

Furthermore, until mid-2025, companies often circumvented localization requirements by duplicating data or hosting a formally "some" database in Russia. However, amendments to Art. 18 of the Federal Law "On Personal Data" came into force on July 1, 2025, making it much easier to violate localization requirements, even if a company's intentions are bona fide. P. 5 of Art. 18 of the Law now directly prohibits the primary collection of personal data of Russian citizens using foreign storage facilities. The law

now mandates that primary processing (including collection, recording, systematization, and storage) must occur only on servers physically located in Russia. In fact, this provision was in the law before 2025, but it is now formulated more strictly and unambiguously, eliminating the possibility of interpretation in favor of collection abroad and subsequent copying to Russia. For example, a website form could send data directly to a cloud-based customer relationship management system (e.g., HubSpot or Salesforce), whose server was located in the EU or the US. This was considered legal because there were no requirements for primary data storage in Russia. A copy or modified version of the database could be created in Russia, if desired, but this was not mandatory. Now, this approach violates the updated P. 5 of Art. 18 of Federal Law No. 152-FZ, since the primary entry must occur in a database physically located in Russia. In the Federal Law No. 152-FZ (2006), it is stipulated that only then is cross-border data transfer possible, provided there is an appropriate legal basis (Art. 12).

One of the most high-profile court cases in this category is the Roskomnadzor case against the American company Snap Inc., the owner of the Snapchat messenger. Roskomnadzor claimed that Snap Inc. processed the personal data of Russian citizens without their consent and without localizing this data in Russia. Roskomnadzor also noted that the United States, where Snap Inc.'s servers are located, is included on the list of "unfriendly" countries, which increases the risk to data security. Snap Inc. claimed that it "is not a personal data operator" under Russian law, since it "does not directly collect or process personal data of Russian citizens." The company also stated that its "activities do not pose a threat to the security of Russian citizens' data" (*Postanovlenie Sudebnogo uchastka № 422 Taganskogo sudebnogo rayona g. Moskvy No. 05-1344/422/2022*, 2022). Ultimately, the court fined Snap Inc. under P. 8 of Art. 13.11 of the Code of Administrative Offenses of Russia (2001) for failure to comply with the requirement to "land" databases in the amount of 1 million rubles (10,538 euros). The court rejected Snap Inc.'s arguments and ruled that the company is a "personal data operator" under Russian law, and Snap Inc.'s activities are not a personal data operator. poses a threat to the security of Russian citizens' data, since its servers are located in an "unfriendly" country.

Similar legal proceedings have also occurred against Apple and WhatsApp LLC. In 2022, a court found Apple guilty of violating Russian data protection laws and fined the company 2 million rubles (€21,077). The court ruled that the company violated the law by processing the personal data of Russian citizens without their consent and without localizing this data in Russia (TASS, 2022). Another high-profile court case in Russia involving non-compliance with database localization rules for processing personal data resulted in an administrative offense against WhatsApp LLC. The court found WhatsApp guilty and fined the company 3 million rubles (€31,615), and then an additional 18 million rubles (€189,694) for repeated failure to organize the storage of Russian citizens' data on servers located in Russia (TASS, 2022). In 2022-2023, other well-known foreign companies were also cited for violating database localization in Russia: Airbnb, Hotels.com, Speedtest, myheritage.com, Likee, and Freelancer.com (RTM Group, 2023). In Russia, one of the most significant violations is the leakage of personal data. The average fine imposed in 2022-2023 on large companies such as Yandex. Food, Yandex Educational Technologies, Skyeng, Ingosstrakh, the Higher School of Economics, Tinkoff Bank, and Sovcombank that experienced personal data leaks in 2022-2023 reached 60,000 rubles (634 euros) (*Postanovleniye Sudebnogo uchastka № 101 Zamoskvoretskogo sudebnogo rayona g. Moskvy № 05-0413/101/2022*, 2022; *Postanovlenie Sudebnogo uchastka № 425 Khamovnicheskogo sudebnogo rayona g. Moskvy № 05-1728/425/2022*, 2022; *Postanovlenie Sudebnogo uchastka № 374 Taganskogo sudebnogo rayona g. Moskvy № 05-0195/374/2023*, 2023; *Postanovlenie Sudebnogo uchastka № 398 Zamoskvoretskogo sudebnogo rayona g. Moskvy № 05-0436/398/2023*, 2023; *Postanovlenie Sudebnogo uchastka № 387 Basmannogo sudebnogo rayona g. Moskvy № 05-0463/387/2023*, 2023; *Postanovlenie Sudebnogo uchastka № 348 Savyolovskogo sudebnogo rayona g. Moskvy № 05-0612/348/2023*, 2023). In reality, there were no consequences for the bank after this incident (*Postanovleniye Vtorogo kassatsionnogo suda obshchey yurisdiktsii № 16-4474/2022*, 2022).

Another significant category of personal data lawsuits concerns the leakage of users' personal data onto the internet. In 2022, a court fined Yandex.Eda 60,000 rubles (634 euros) for a personal data leak (*Postanovleniye Sudebnogo uchastka № 101 Zamoskvoretskogo sudebnogo rayona g. Moskvy № 05-0413/101/2022*, 2022). Yandex.

Eda acknowledged the data leak but stated that it immediately warned users and took all necessary measures to protect user data. The company also stated that the leak did not result in any negative consequences for users, despite affecting the data of more than 58 million users (TASS, 2022).

Furthermore, in 2025, the first criminal case was opened under Art. 272.1 of the Criminal Code of Russia (1996) for the illegal use of personal data against a Telegram bot (a bot in the Telegram messenger) for searching for personal data called "God's Eye" (Kamitdinov, 2021). This bot could search for information on any person by phone number, first and last name, car registration number, VKontakte page, Telegram nickname, or email address. To do this, the bot connects to the APIs of social networks and messengers. However, since March 2021, amendments to the Law "On Personal Data" have come into force, according to which even publicly available personal information cannot be distributed by default. Therefore, owners of platforms that host such data must obtain users' consent each time they transfer data to third parties or publish it publicly.

Roskomnadzor demanded that Telegram remove data mining bots, as information search bots such as AVInfo, Smart Search Bot, "Archangel," Mail Search Bot, and How To Find Bot were developing in parallel with "God's Eye" (Kamitdinov, 2021). Big Data specialist Khachuyan doesn't rule out the possibility that the bot creators may have purchased the license plate database on the darknet, noting that proving this was done illegally is difficult. Legally, everything is perfectly legal, and to prove a violation of the Law on Personal Data, it is necessary not only to present the fact of a data leak in court but also to prove malicious intent and profit from the use of this data (Kamitdinov, 2021). Another specialist, Darbinyan, is convinced that the bot also uses leaked databases: "Information about, for example, mobile phone numbers or a person's place of residence is never contained in government information systems. Therefore, these are enriched databases." Thus, data mining bots have identified "massive holes" and vulnerabilities in government information systems, from which the largest volumes of data are leaked (Kamitdinov, 2021). According to Lukatsky, an IT security specialist at Positive Technologies, the main source of information for any data-mining bot is leaks from large companies that have access to the personal data of Russians. Furthermore,

personal data can end up in such IT services due to the actions of employees of government or commercial organisations that sell this information (Denisenko, 2025). Kuznetsov, Deputy Chairman of the Management Board of Sberbank (SBER), Russia's largest universal bank and financial conglomerate, admitted in an interview that clients' data is regularly put up for sale on darknet forums (Poltavskaya, 2020). A good database with 90% up-to-date data, including client account information, can cost $3 per line, while a database with 60% data costs $2 (Mikhailova, 2020).

As of November 2, 2025, another criminal case has been opened under Art. 272.1 of the Criminal Code of Russia (1996) for the illegal use of personal data against another Telegram bot, Userbox, for the purpose of searching for personal data (Plugina, 2025). According to the Ministry of Internal Affairs, the service was one of the largest in the Russian-speaking internet, providing access to residential addresses, income information, bank accounts, vehicles, and other confidential data obtained from leaks (Plugina, 2025). Userbox, also known as User_Search, is considered an alternative to the Telegram bot "God's Eye," which ceased operation in February 2025 (TASS, 2025). Ultimately, the elimination of "God's Eye" did not solve the problem—it merely fragmented it. Its place was taken by dozens of small, anonymous, and decentralized "search" bots, operating under the same schemes but even more covertly. Most of them switched to cryptocurrency payments, abandoned public registration, and began using mirror sites (Kostunov, 2025).

Thus, changes in the regulation and protection of personal data in 2025 reflect a shift in the state's focus—not on individual hackers, but on the IT infrastructure for data trading as a whole. The Telegram bot "God's Eye" has become a symbol of digital espionage and surveillance in Russia (Kostunov, 2025). According to CNews, approximately 40% of Russian-language IT platforms specializing in searching for open data online have suspended operations or closed by November 2025. The market for such IT services, worth up to 15 billion rubles, could finally migrate to the darknet and fall under the control of foreign operators (Denisenko, 2025).

In this sense, judicial practice in Russia's personal data processing field is constantly evolving to ensure a balance between businesses' interests and individuals' privacy rights. Trends observed in judicial practice since 2022 indicate courts' efforts to

maintain a balance between the legitimate interests of personal data subjects and the need to use such data for various purposes, as well as to increase liability for organisations that fail to comply with legal norms or violate statutory rules, standards, or procedures. Until May 30, 2025, operators were more likely to admit guilt, and courts, in turn, imposed the minimum administrative liability. However, after the entry into force of new amendments and tightening of the rules, lawyers express the opinion that, taking into account significant fines, from 3 to 15 million rubles (31,722 - 158,617 euros) for the first leak and a turnover fine of 20–500 million rubles (211,490 - 5,287,255 euros), these penalties will increase significantly. For repeat offenders, operators are unlikely to readily admit guilt and are more likely to settle for quick proceedings and minimal fines. Such fines will be costly even for the largest market players (Domshenko & Sabirov, 2025).

It has also been suggested that operators will significantly change their litigation strategies: "they will dispute the fact, volume, and date of the leak, the type of data, and other important circumstances of the dispute, actively using various means of evidence (expert opinions, computer forensics), and engaging consultants to handle such disputes." Thus, the number of cases in favor of operators should increase (Domshenko & Sabirov, 2025). The new regulations create additional barriers and significantly increase the burden on small and medium-sized businesses, while the actual effectiveness of these innovations raises serious doubts among lawyers. They cite such problems as a consequence of insufficient drafting of the legislation, a lack of broad discussion with the business community, and a lack of understanding of how the new rules will work in practice (Ayrapetyan, 2025). At the same time, the influence of the global political situation on the regulation of personal data processing in Russia cannot be overlooked, particularly regarding cross-border transfers of personal data (RTM Group, 2023).

Ayrapetyan (2025) believes that the new regulations have certain positive aspects: increased protection of citizens' data, which is especially relevant in light of the increasing frequency of data leaks from large corporations; unification of requirements, which should, in theory, simplify compliance monitoring and make requirements more predictable; an incentive for IT infrastructure modernization, which could encourage

large companies to improve information security systems and implement modern security technologies; and increased transparency, which requires mandatory operator registration and publication of data processing policies to make processes more open to regulatory authorities and citizens themselves.

At the same time, the author believes that the main problem with the new regulations is that they apply equally to everyone, including transnational corporations, individual entrepreneurs, and even citizens. Almost any business now falls under the definition of "personal data operator," and Roskomnadzor's registry is becoming a "gigantic data array" where it is impossible to distinguish between those who truly pose a risk to user privacy and those who work with minimal information (Ayrapetyan, 2025). Furthermore, the new rules create a significant burden on businesses without addressing key issues: the need to appoint a person responsible for personal data; to develop a proprietary processing policy; to submit separate notifications for each processing purpose; and to specify technical details, including server addresses. Ayrapetyan (2025) also points out the importance of differentiated personal data regulation.

Chapter 4. Formation and development of the right to personal data protection in Europe

4.1 Early legal and philosophical foundations of personal data protection before 1980

4.1.1 Historical evolution of the right to privacy in Europe until the mid-20th century

Dmitrik (2020) argues that, until the 1940s, the process of legally defining citizens' rights to information about themselves in Europe was in sync with that in the US, although the results lagged significantly behind those in the US. As well, he points out that the doctrine of the right to privacy in the UK was "completely dissolved" in the US. On the one hand, the word "privacy" was first mentioned already in the 19th century in the case *Prince Albert v Strange* (1849). The court recognised that, even without violating property rights, publication could be prohibited for breaches of trust and confidentiality. The case also raised the question of what privacy is based on—property rights, contract, trust, or confidence. This case was later cited in Warren and Brandeis's article (1890). However, the common law doctrine in the UK never developed either a definition of privacy or the associated tort. A 1967 study on privacy in Europe noted that privacy in England remains a theoretical concept adopted by researchers under American influence (Strömholm, 1967).

Before World War II, this slow legal development of privacy rights was mirrored in both France and Germany, where neither had a legally enshrined right to privacy (Dmitrik, 2020). However, since the early 19th century, France has had a so-called "rubber" rule, which provides the right to seek compensation from anyone who causes harm, which is stated in the Art. 1240 (formerly Art. 1382) of the French Civil Code (1804). The courts applied this rule in such a way that it covered most cases of violation of privacy, for example, the publication of private correspondence or the use of someone else's name (Strömholm, 1967; in the work mentioned the author cites decisions of French courts: *Trib. civ. de la Seine*, 1849; *Cour de Paris D. 1851.2.1*, 1850; *Cour de Paris, S. 1827.2.155 and D. 1827.2.55*, 1826; *Trib. civ. de la Seine D. 1858.3.62,* 1858). Thus, it is believed that the French doctrine of privacy did not develop due to a lack of need, since most of the interests violated were already protected under current civil legislation (Dmitrik, 2002). Furthermore, the author points out that later, at the beginning of the 20th century, the legal doctrine of privacy in France began to develop from the moral

rights of authors (droit moral), when purely proprietary exclusive rights suddenly proved insufficient to protect the author's interests. This approach (by recognising non-property rights as proprietary rights) introduced a new dimension to the idea of privacy: personal rights (droit de la personnalité).

This evolution of privacy thought continued with subsequent legal scholarship. In particular, Perreau's (1909) major work, "Les Droits de la personnalité," played an important role, systematising and quite fully expounding the concept of personal rights. At the same time, Dmitrik (2020) also points out that Germany, Austria, and Switzerland occupy a "place comparable to the United States" in the history of privacy: the categories of personal (Persönlichkeitsrechte) or individual rights (Individualrechte) have been present in German-language doctrine in one way or another since the late 17th century and included a different set of rights. However, in the first half of the 19th century, the shift in the dominant legal ideology from natural law to positivism led to the rejection of ill-defined doctrines, including the concept of personal rights. A return to the doctrine of personal rights occurred only after Gareis (1877), who mentioned the right to a name and the right to organise one's life as one sees fit in relation to copyright.

By the early 20th century, European scholars continued to refine how personal rights were understood and legislated. Building on this earlier intellectual foundation, Kohler (1907) offered a more cautious understanding of "general personal rights," viewing them as "a kind of continuation of copyright, protecting what was not protected by copyright in contemporary law: the privacy of correspondence, the name and image of an individual, and information about one's personal life." It is particularly noteworthy that Kohler combined all of these rights into a general "right to secrecy," where the actual impossibility of obtaining information served as a means of ensuring the legal impossibility of obtaining it. Ultimately, however, the drafters of the German Civil Code did not include personal rights in their work. Strömholm (1967) points out that the works of Kohler, Gareis, and Perreau allow us to speak about the origins of privacy legislation in continental law: first, it was a synthesis of interests—a vision of complete protection given by essentially homogeneous legal norms to non-property interests that had not previously been analysed in their unity—and, second, the recognition of these interests by private law. In a broader context, Whitman (2004) observed that Europe has "two Western cultures of privacy: dignity versus liberty," with Europe's approach

safeguarding personal identity in society, while the U.S. focuses more on keeping the state out of the private. These philosophical differences later shaped divergent legal frameworks: Europe moved toward explicit personal data protection as a fundamental right, rather than treating personal information as a tradable commodity (Lissens, 2024).

4.1.2 The historical origins of the GDPR: the evolution of data protection principles following World War II

The literature indicates that the principles underlying the revolutionary General Data Protection Regulation (GDPR) (2018) are far from new. In fact, the principles embodied in the GDPR date back to World War II. At that time, European leaders realised that the best way to ensure lasting peace and prosperity was to promote greater international cooperation and reconstruction (Kramer & Hoar, 2023). To facilitate these efforts, the Organisation for Economic Co-operation and Development (OECD) was established in 1945. The OECD later issued a series of international data protection and privacy guidelines in 1980, known as the "Guiding Principles for the Protection of Privacy and Transborder Flows of Personal Data."

Whitman (2004) and Buitelaar (2019) trace the origins of the concept of privacy to the experience of World War II, when personal data was systematically used by the Nazi regime to identify, classify, and persecute Jewish citizens. Black (2001) notes that the persecution was not only ideological but also bureaucratic and technologically enabled. He also states that the mechanical data processing systems developed by IBM were used to process census data, allowing for the rapid sorting and extraction of records previously labeled as "Jewish." This historical experience demonstrated how administrative data collection, combined with state power and technological efficiency, can transform personal information into a tool of exclusion and repression.

Whitman (2004) believes that it was the combination of, first, the differences between the upper and lower classes, second, the spread of "upper-class rights" to the whole of society, and third, the Nazi cruelties that established the notion that everyone’s dignity had to be respected. Thus, to ensure such atrocities never recurred after the war, the connection between privacy and human dignity was enshrined in national and international legal documents. In 1948, the right to privacy was enshrined—along with other fundamental rights and freedoms—in Art. 12 of the Universal Declaration of

Human Rights (1948). It was then included in the German Constitution (1949), and in 1950, in Art. 8 of the European Convention on Human Rights (1950). The heightened attention to human rights at that time was primarily due to the devastating consequences of World War II. The main priorities then were the most significant social issues of the post-war period: the privacy of private and family life and the confidentiality of correspondence. It is important to understand, however, that the issue of personal data protection, while seemingly a logical consequence of the right to privacy, has not received widespread attention. For example, the ECHR classified the right to the protection of personal data as part of the right to privacy, which is enshrined in Art. 8 (ECHR, 1950). The formulations of the 1948 Declaration and the 1950 ECHR, for all their universality, affirmed privacy as a mechanism for protecting roughly the same interests that gave rise to it in the late 19th century.

Later, in 1968, the Parliamentary Assembly of the Council of Europe issued Recommendation No. 509 (1968). This document expressed concern about the threats to the right to privacy posed by new data processing technologies. It became an early step in the development of legislation on the protection of personal data. The Assembly subsequently requested the Committee of Ministers and the Human Rights Committee to consider whether the ECHR and the domestic laws of member states provide sufficient protection for the right to privacy in light of developments in modern science and technology. The literature (Pazyuk & Sokolova, 2015) notes that this recommendation is a starting point for the development of personal data protection laws, despite the fact that full-fledged legislation emerged much later. Research carried out at the request of the Committee of Ministers in response to this Recommendation showed that national legislation currently does not provide sufficient protection for individuals' privacy and other rights and interests in relation to automated data banks. Based on these findings, the Committee of Ministers of the Council of Europe adopted two resolutions on data protection in 1973 and 1974. The first, Resolution 22 (1973), established principles of data protection in the private sector. The second, Resolution 29 (1974), established principles for the public sector. However, it soon became apparent that, given the varying interpretations of the concept of "privacy" across countries, extraterritorial protection of personal data is impossible without common data protection principles. Such standards would enable the harmonisation of the Member

States' national laws (Pazyuk & Sokolova, 2015). Thus, Bennett (1992) believes that the foundations of a proper attitude towards information privacy were formulated in Europe in the late 1960s and early 1970s. Data protection legislation as a separate legal institution was formed in Europe, not in the United States, where the development of computing technology was faster (Dmitrik, 2020).

In 1968, the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, 1968) was adopted in Germany, dramatically expanding the rights of intelligence agencies to use the most modern automated technologies for eavesdropping on communications. One of the main provisions of the Act was that a citizen in relation to whom wiretapping occurred could not have learned of it, even later, when the wiretapping ceased, and no legal action was taken against the citizen. In 1969, the UK Parliament passed the Data Surveillance Bill (1969), establishing controls over the use of collected information about citizens.

Since the 1970s, many states have adopted data protection laws, developing fundamental principles that later became part of European data protection law (Craig & Búrca, 2021). In response to the Council of Europe Resolutions of 1973 and 1974, Germany was the first to act: the state of Hesse adopted the world's first personal data law in 1970. This legislation is seen as one of the most successful first-generation laws and continues to serve as a model in this area (Pazyuk and Sokolova, 2015). The authors of the law based their work on the premise that information flows from the "nerve centre of public life" and that holding information about citizens represents "social power." They believed that automated data processing without protective measures poses a threat to personal freedom and, consequently, creates a new threat to civil society (Craig & Búrca, 2021). It is important to note that this was a local law that applied exclusively within the state's territory, not at the federal level (Craig & Búrca, 2021). Other member states followed suit, creating their own, various domestic data protection laws during the 1970s, including Sweden (1973), Germany (1977), Austria (1978), Denmark (1978), France (1978), and Luxembourg (1979).

Particular attention should be paid to the first national personal data laws in Sweden and France. The Swedish Law (Datalagen, 1973), unlike the Hessian State Law (1970),

applied to the private sector and introduced a permissive principle for automatic data processing (initially via licenses, which were later replaced by notification registration due to the large number of licensees). Furthermore, the law introduced a list of new crimes for violations of individual rights committed with computer equipment and established corresponding sanctions.

Slightly later, in 1978, France adopted the Law on Information Technologies, Data Files, and Individual Liberties (Loi Informatique et Libertés, 1978) in response to local events. In the early 1970s, the French government developed the SAFARI project. This project aimed to create a single data registry using the social security number to identify any citizen. All this information was planned to be processed using the advanced computing technologies of the time. In 1974, the newspaper Le Monde published an article titled "SAFARI ou la chasse aux Français" (1974) (SAFARI or the hunt for the French), which provoked a major scandal about mass surveillance. Under public pressure, the government retreated. This led to the adoption of the Law on Information Technologies, Data Files and Individual Liberties (1978) and the creation of the Commission on Informatics and Civil Liberties. French legislation drew on experience regulating the processing of personal information from the United States, Germany, Sweden, and other countries. However, it applied only to automated processing; traditional paper-based card indexes were not covered. If the procedure for automated information processing were regulated in detail, the regulation of the collection, storage, and dissemination of information would be of a rather general nature (Pazyuk & Sokolova, 2015). Thus, Swedish, German, and French laws serve as the cornerstone for personal data and provide significant impetus for the development of this field.

Another important event for the personal data institute was the *"Census Decision"* (*Das Volkszählungsurteil*) of the Federal Constitutional Court of Germany in 1983. In this decision, the court formulated the fundamental principle of the "right to informational self-determination" by prohibiting the state from collecting excessive data on citizens without clear boundaries, transparency, and a justified necessity (*Das Volkszählungsurteil*, 1983). This way, the German court issued the first decision in the world to formulate an individual's right to control their personal data (Bennett, 2008). Many experts (e.g., Pazyuk and Sokolova, 2015) believe that the European approach to data protection arose from the German court's decision. It served as the basis for the

future Directive 95/46/EC and the GDPR. This decision transformed data protection from a technical issue into a fundamental right, which was then enshrined in the Charter of Fundamental Rights of the European Union (CFR) as a separate right (Art. 8).

4.2 Evolving policy landscape: data protection in Europe after 1980

4.2.1 Normative and technological foundations of the European data protection regime: OECD, Convention 108, and PETs

De Hert (2004) believes that the ECHR had significant limits by the 1970s due to modern technology. These drawbacks included the application's ambiguous scope (because privacy was not defined), its protection of individuals only against state meddling, and its limited protection for "personal data in the modern sense." These limitations led to the need for a new, more digitally adapted right: the right to data protection, aimed at protecting individuals in the information society. To this end, the OECD Recommendations Governing the Privacy and Transborder Flows of Personal Data (OECD) were adopted in 1980. This document first codified the basic principles of personal data processing at the international level and remains the primary document setting forth policy norms regarding personal data (Hert, 2013).

The OECD (1980) established principles that still underpin policymaking and the development of legal instruments for the protection of personal data: personal data must be collected lawfully, fairly, and, where possible, with the consent of the subject (Collection limitation principle) and be accurate, up-to-date, and used strictly for the purposes specified (Data quality principle and Purpose specification principle). Access, disclosure, and processing of the data are permitted only when consistent with these purposes or based on consent or law (Use limitation principle), subject to adequate security measures (Security safeguards principle) and transparency (Openness principle). Data subjects have the right to know what data is held about them, access it, challenge its accuracy, and obtain correction or erasure (Individual participation principle), and the data controller is responsible for ensuring compliance with all of these requirements (Accountability principle).

As European countries sought to implement these principles, several separate, sometimes conflicting privacy laws were adopted by OECD member states, ultimately

leading to considerable confusion about how to comply with the disparate regional set of privacy requirements (Craig & Búrca, 2021). The OECD Guidelines apply to personal data processed in a manner that poses a risk to privacy rights and individual liberties, given the nature or context of the data. However, the OECD does not include provisions on "sensitive data" because there were significant differences among OECD member countries in how such data were treated. The OECD's primary objective was to eliminate differences in member countries' legislation, as such deviations could be used by states to regulate and limit data flows. States with stronger privacy protections could prohibit the export of data to countries with weaker protections. This is why the OECD Guidelines sought to establish a "uniform level of protection." Gutwirth (2002) also points out that this "uniform level of protection" could not be too high, as it would, in itself, upset the regulatory balance and create obstacles to the free flow of data. Despite its non-binding nature, the OECD has had a significant influence on the development of national systems for the legal protection of personal data subjects, and not only in OECD countries (Pazuk & Sokolova, 2015).

To fill gaps and streamline the legislation of European countries, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (better known as Convention 108) in 1981. Fogarty (2009) points out that its adoption was preceded by significant case law from the European Court of Human Rights (ECtHR), which has repeatedly considered issues related to data processing under Art. 8 ECHR. Furthermore, the European Commission publishes recommendations for EU member states on adopting agreements implementing the Convention, and Convention 108 becomes the first international treaty in the field of data privacy. The scope of the Convention extends to personal data files and the automated processing of personal data in the public and private sectors. Convention 108 protects the right to privacy of individuals, given the growing cross-border flow of personal data subject to automated processing (Art. 1): it established fundamental rights of access to personal data and their correction (Art. 8), formulated important data protection concepts, including "fairness, lawfulness, proportionality and purpose limitation, based on national precedents" (Art. 5), and began to protect individuals from intrusion into their privacy by public authorities and the administration of private organisations (Arts. 1 & 5). In addition, the Convention, for the first time, formally

required the adequacy of safeguards for the exchange of personal data between countries (Art. 12). Thanks to this principle, national data protection laws have, in most cases, taken into account the provisions of the Convention, which remains the only international legally binding instrument.

However, even Convention 108 does not apply to all data processing: "…its regulation does not apply to all data processing, since it does not apply to processing that does not infringe on the privacy of the individual" (Gellert & Gutwirth, 2013). However, privacy is also broader and specific, as it "may apply to the processing of non-personal data while still impacting privacy" (De Hert, 2004). Another key difference is that "in contrast to the right to privacy, which is more abstract, the right to data protection is subject to a complex set of laws that include definitions, guiding principles, and other provisions" (Gellert & Gutwirth, 2013). Therefore, data protection is a more formalised, procedural, and technically intensive area of law than the traditional right to privacy.

Both documents, the 1980 OECD and the 1981 Convention, addressed the problem of information flow, which had become a given in the 1970s: flow could no longer be prohibited; it could only be channelled through available legal instruments (Dmitrik, 2020). Gutwirth (2002) points out that both documents, especially Convention 108, are discriminatory against states that have not implemented the minimum level of personal data protection established by these international instruments in their legislation. Such countries ultimately found themselves isolated because they were not part of the unified legal framework of Convention 108, and the transition from privacy protection to personal data protection is not always an indicator of an increase in the level of protection of the rights and legitimate interests of data subjects. In parallel, in the 1980s, amid the rapid growth of surveillance technologies and mass data collection, engineers began developing, for the first time, technical solutions aimed not at surveillance but at protecting users, leading to the emergence of Privacy Enhancing Technologies (PETs). These technologies enabled minimising the amount of data collected, ensuring anonymity, and preventing unnecessary processing without compromising system functionality (Dewitte, 2023). The works of Chaum and the concept of multilateral security laid the foundation for the European approach, according to which systems should protect users not only from intruders but also from the data controllers themselves (Chaum, 1983 & 1985). Thus, it was PETs that paved the way for the

principle of "Data Protection by Design and by Default," which was later enshrined in the GDPR and became a key element of the European data protection model. The active process of shaping the modern institution of personal data began.

4.2.2 Directive 95/46/EC: its objectives, mechanisms, and limitations

After the adoption of Convention 108, it became clear that its ratification in many countries would pose significant challenges, primarily due to inconsistencies in local legislation and a lack of technical preparedness (Gorokhova, 2013). The ever-accelerating development of information technology and the emergence and growth of the Internet created new challenges in the areas of data privacy and privacy of private life. In addition, in 1993, a high-profile case, *Regina v. Brown* (1993), occurred in which a police officer was charged with using personal data (obtained in the course of official activities) for purposes not specified in the Data Protection Register (Bainbridge, 2010). Under the Data Protection Act 1984 in the UK, using data outside the registered purposes was considered an offence. However, the court subsequently overturned the decision and ruled that the Data Protection Act 1984 was too narrow: it required an exact match between the "registered purpose" and the actual purpose of processing. However, in reality, the purposes of processing were not always clearly or specifically formulated, and the court decided that Brown had not acted contrary to the stated principles—it was simply that the "purpose" had been interpreted too narrowly (Bainbridge, 2010). Thus, the case of *Regina v. Brown* (1993) exposed the shortcomings of earlier laws and influenced the modernisation of European legislation—namely, the development of the idea of creating a European data protection standard.

In response to these threats and to address problems arising from the patchwork of European privacy laws, the European Commission introduced a data protection directive in 1990. This was largely due to the demand for pan-European measures by Member States' data protection commissioners (International Conference of Data Protection and Privacy Commissioners, 1989). The Directive relied heavily on the principles of Convention No. 108 and national laws. It often expanded their scope of application. For example, it explicitly required each country to establish an independent supervisory authority (the Data Protection Authority) and provide individuals with enforceable rights to access, rectify, and object to processing (European Union Agency

for Fundamental Rights, Council of Europe & European Data Protection Supervisor, 2018).

Building on the introduction of the Directive, the European Commission invoked the competence of the internal market (then Art. 100a TEC, now Art. 114 TFEU), arguing that disparate national data protection regimes threatened the free movement of personal data within the internal market. The EU deliberately chose the directive as a legislative form to ensure harmonisation, since all Member States had adopted data protection laws (Craig & Búrca G., 2021). Subsequently, the lengthy legislative process showed that Member States primarily wanted to preserve their established data protection concepts rather than invent new ones. The Directive, adopted as a supranational document, aimed to harmonise national data protection legislation. Simitis (1995) stated that "Experience has shown that the primary interest of the Member States is not to achieve new, union-wide principles, but rather to preserve their own, familiar rules. A harmonisation of the regulatory regimes is, therefore, perfectly tolerable to a Member State as long as it amounts to a reproduction of the State's specific national approach." By 1998, all EU countries had transposed the Directive into national laws (European Union Agency for Fundamental Rights, Council of Europe & European Data Protection Supervisor, 2018).

To further understand the Directive's impact, it is important to note that it recognised the internal market's competence and stated that the free flow of personal data within it was threatened by the fragmentation of national data protection regimes in Arts. 1 and 25 (Directive 95/46/EC, 1995). Since each Member State adopted data protection legislation, harmonisation was achieved through the adoption of the Directive (Art. 1). The lengthy legislative process clearly demonstrated that Member States were more interested in preserving their existing data protection ideas than in developing new ones. However, practice fell short of allowing all Member States to maintain their preferred approach (Craig & Búrca, 2021). The Directive was developed as "an internal market tool to facilitate cross-border commerce by harmonising data protection laws, since this variability posed a barrier to the growth of the internal market" (Bennett & Raab, 2006). Its primary goal was not to establish a legal framework that could handle upcoming challenges in data processing and privacy, but rather to "harmonise existing regulations to protect the right to informational privacy of the data subject and to establish a common European market for the free movement of personal data" (Bennett & Raab,

2006). By regulating the "collection, use, and sharing of individuals' personal data" (Art. 6), the Directive 95/46/EC (1995) seeks to safeguard the privacy and basic rights, and is applicable to "all EU member states and specifies obligations for data controllers, who are in charge of ensuring that personal data is handled in compliance with the directive's rules" (Arts. 3 and 6).

Despite the Directive's explicitly regulatory focus, it implicitly supports privacy protection through technology, particularly in Art. 17: "The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access…" The addition of Rec. 46 strengthened this approach, specifying that such measures must be integrated into both the data processing system and the processing itself. In other words, security cannot be imposed on top of existing systems; it must be built into the architecture from the outset. This idea subsequently became known as privacy-by-design (Dewitte, 2023). One of the key features of the Directive is its focus on the concept of personal data rather than the much broader, vaguer category of privacy. This meant that the Directive also covered processing operations that were not considered particularly privacy-sensitive. Thus, the Directive served several functions simultaneously: in addition to protecting privacy, it promoted freedom of expression, combated discrimination, and increased administrative efficiency (Bennett & Raab, 2006).

Craig and Búrca (2021) point out that the Data Protection Directive's adoption of a unified concept of "data controller" eliminated the fundamental distinction between data processing in the public and private sectors, on which, for example, German data protection law was based. However, Directive 95/46/EC has often been criticised for its structural and conceptual shortcomings, which were revealed during its implementation. In national legal orders, this proved that the level of harmonisation was insufficient. Cifaldi (2023) gives the example that the requirements of the Directive were effectively implemented in some EU Member States but led to failures and uncertainty in others, indicating that it allows excessive freedom of interpretation. Such variability in national strategies directly affects the effectiveness of harmonisation: the impact of the Data Protection Directive turned out to be limited, since it applies only to issues of the

internal market of the first pillar and does not cover many aspects of inter-agency exchange of information or specific national practices (Fogarty, 2009).

A study by Rand Research Europe (Robinson et al., 2009) described the following problems and shortcomings of Directive 95/46/EC: firstly, the lack of clarity about the relationship between the concept of personal data and real risks, since enforcement was excessively dependent on the binary criterion of "personal/non-personal data" has led to counterintuitive results and inconsistent practices. Moreover, the link between privacy protection and data protection has been criticised as being ambiguous, which has led some to question whether the Directive's emphasis is "weak because not all actions of processing personal data covered by the Directive have a clear or discernible impact on privacy" (Lieshout et al., 2007). Secondly, inconsistencies in transparency and notification measures were identified, with these measures implemented differently across national jurisdictions, making the mechanism cumbersome and ineffective (Robinson et al., 2009). In addition, in this study the authors questioned the outdated rules for data transfer to third countries, since the concept of "adequacy" and the very concept of a "third country" were poorly suited to the conditions of the globalized digital economy, and the tools for international transfers were characterised as complex, due to the fact that obtaining standard contractual clauses or BCRs took too much time, and approval procedures differed from country to country (Robinson et al., 2009). Those national data protection regimes that were in force at that time often limited the transfer of data from the EEA to third countries, but did so with significant differences in terms of justification, substantive standards, and institutional assessment (Schwartz, 1995).

The desire of Member States to preserve their domaines réservés led to broad ("in any case") exceptions in matters of public and national security, defence, and criminal law in Art. 3(2) (Directive 95/46/EC, 1995). The Directive obliged each EU Member State to adopt privacy laws that were "equivalent" to each other and established that data could only be exported to third countries that could ensure an "adequate level of protection" for European citizens' data through their domestic legislation or adopted international obligations. Finally, a study by Rand Research Europe (Robinson et al., 2009) noted the inconsistency and fragmentation of supervisory authorities' (DPAs) work, as national regulators applied sanctions and controls according to different criteria, undermining

uniformity of enforcement. Finally, the rapid growth of the data reuse ecosystem made the traditional delineation of roles too rigid and inappropriate for modern processing models, leading to static definitions of controller and processor.

Finally, Directive 95/46/EC became "the final result, combining elements of several national data protection laws" (Craig & Búrca, 2021). Its main objective was to create a single internal market (Gorokhova, 2013). In addition, the Directive aimed to unify and adapt the EU Member States' personal data legislation to new threats. To this end, the mechanisms provided for in Convention 108 were improved, and new obligations for personal data controllers and new rights for EU citizens were introduced. The purpose of the Directive was not so much to create a universal, long-term regulatory model for future technological challenges, but to harmonise existing rules to protect the privacy of data subjects and to form a single European market for the free movement of personal data (Bennett & Raab, 2006).

According to Dmitrik (2020), the development of personal data regulation in Europe has followed the path of expanding data processing procedures and further aligning regulations in countries that form a common legal space for data circulation. Ultimately, the 1995 Directive gained global recognition as a paradigmatic model and emerged from a complex political struggle in which Member States pursued their own interests (Craig & Búrca, 2021). The Directive had a significant impact on data processing practices in Europe and played a key role, as its principles became the standard for legal definitions of personal data, state responses to their use, and many subsequent data protection legislative initiatives. It ensured the formation of clear rights for data subjects, established special requirements for the processing of sensitive data, and laid the foundations for both national and international supervisory mechanisms (Craig & Búrca, 2021; Cifaldi, 2023). Under the Directive’s sector-agnostic (omnibus) approach, Europe firmly embraced comprehensive data protection rather than a patchwork of sector-specific rules (unlike the U.S. model).

4.2.3 The formation of the contemporary European data protection regime: ePrivacy Directive, EDPS, and the EU Charter

In the late 20th and early 21st centuries, two high-profile cases emerged that played a huge role in shaping the European data protection framework: *Leander v. Sweden*

(1987) and *Rotaru v. Romania* (2000). In *Leander v. Sweden* (1987), Herman Leander, a maritime museum employee, was denied a job because the police had disclosed "negative information" from classified files to his employer. Leander wanted to know what data was stored on him and why it was used against him, but the state refused to answer. This became the first major case in which the ECtHR recognised that the storage and processing of data by intelligence agencies amounted to an invasion of privacy and, in effect, laid the foundation for the principle: "if the state collects data, the citizen must have minimum protection mechanisms."

Like the precedent established in Leander, the *Rotaru v. Romania* (2000) case addressed the state's handling of personal data. Gheorghe Rotaru learned that the Romanian Securitate (former secret police) maintained a secret file on him, including false allegations that he was an extremist and a threat to national security. However, after the file was disclosed, Romanian courts refused to correct or delete the false information. The ECHR found a violation of Art. 8, stating that the state stored and used personal data without sufficient legal regulation, and that individuals must be able to access, correct, or challenge their data. This marked a turning point, as for the first time the ECHR explicitly linked the right to access data, the right to correct inaccurate information, and the right to privacy. This decision served as the legal precursor to future rights under the GDPR: the right to access (Art. 15), the right to rectification (Art. 16), and the right to erasure (Art. 17).

While the legal landscape was changing, a parallel transformation was underway in the late 1990s with the emergence of the Big Five, or GAFAM (Google, Amazon, Facebook (now Meta), Apple, Microsoft). Their rise enabled a new system of monetising commercial activity on the Internet, based on the systematic collection and analysis of user data. It was Google and Facebook that, in 2007, began to use DoubleClick's behavioural targeting technologies, that is, they displayed advertising based on an analysis of their users' behaviour (Collins & Buchanan, 2018). However, by 2007, DoubleClick was known for tracking the behaviour of more than 100 million users daily—an unprecedented scale of data processing at the time (Story and Helft, 2007). Contextual advertising quickly became extremely popular, and Amazon, Microsoft, and Apple joined this system (Alcantara et al., 2021). To ensure advertising remained as relevant as possible, the aforementioned companies began collecting vast amounts of

data on users worldwide. In parallel, technologies that enabled the analysis of all this information and the identification of online user behaviour patterns were rapidly developing. Events came to a head in 2007, when Facebook launched its own advertising platform, Facebook Ads, and the Facebook Beacon system, which became one of the first major scandals in the field of commercial tracking of user activity. Beacon recorded data on visited websites, purchases, search queries, and other actions performed outside of Facebook and automatically transmitted it to the social network, where the information could be displayed to the user's friends—without their informed consent (Perez, 2007; Esguerra, 2007). According to The New York Times (2007), more than 65 third-party websites were secretly connected to the system, sparking a massive public outcry and international debate about the limits of acceptable commercial data use.

The rapid growth of digital platforms and their capacity to process data at a massive scale revealed that these new actors could collect and use personal data in ways previously reserved for states and intelligence agencies (Solove, 2004; Zuboff, 2019). This convergence of private and state capabilities set the stage for significant legal reform (Cohen, 2012). As a result of these industry practices, momentum for legal reform in the EU increased significantly (European Commission, 2012). Regulatory investigations and public pressure over DoubleClick and Beacon demonstrated the shortcomings of the traditional "privacy as notice and consent" model in the context of mass surveillance and opaque algorithms (*FTC v. DoubleClick Inc*, 2001; Solove, 2008). Thus, by the end of the 20th century, it was clear that data protection law in the EU was developing from two directions—the state and the private sector (Bygrave, 2014; Lynskey, 2015). Together, state abuses of classified files (exposed by the courts) and the commercial monetisation of user data (created by GAFAM) underscored for Europe the need for comprehensive data protection that addresses both government and private actors (*Leander v. Sweden*, 1987; Zuboff, 2019; European Commission, 2012).

In direct response to these new challenges, especially those posed by contextual advertising, the EU took action to protect individuals. In 2002, Directive 2002/58/EC on Privacy and Electronic Communications (the ePrivacy Directive) began regulating the use of cookies, including for advertising. Its main goal was to ensure individuals' right to self-determination in automated processing of personal data, minimise the

dissemination of personal data in user networks, and protect anonymity wherever possible (Art. 1(1); Gorokhova, 2013). This Directive addressed key issues, including privacy (Art. 5(1)), traffic data processing (Art. 6), spam (Art. 13), and cookies (Art. 5(3)). Importantly, it defined the "right to privacy in the electronic communication sector" and established the free movement of data, equipment, and services (Arts. 1(1) & 3). Unlike the Data Protection Directive, which addresses only individuals, Article 1(2) clarifies that the ePrivacy Directive also applies to legal entities (Art. 1(2)).

To further bolster the protection of personal data in the evolving digital environment, Wiewiórowski (2024) argues that, upon adopting its own data protection legislation, the EU also established an independent supervisory authority—the European Data Protection Supervisor (EDPS)—in 2004. This step marked a shift from earlier legal frameworks, further solidifying protection and oversight. Even now, after years of operation, the key aim of the EDPS is to ensure that EU institutions and bodies respect people's right to privacy when processing their personal data. The first three heads of the EDPS— Hustinx (2004–2014), Buttarelli (2014–2019), and Wiewiórowski (2019–present)—used this independence not only to oversee data processing within EU institutions but also to actively influence the development of European legislation. Their opinions on draft legislation, interpretations of existing regulations, and controversial Commission decisions (especially on adequacy issues) carried significant weight and often shaped political debate (Wiewiórowski, 2024).

The EDPS monitors how European institutions process personal data, which is stated in the Art. 52 (Regulation 2018/1725, 2018) and Art. 16 (TFEU, 2012). For example, it can conduct inspections and audits in the European Parliament, the European Commission, and EU agencies, states in the Art. 58(1)(b) (Regulation 2018/1725, 2018). It can also investigate violations, thereby fulfilling a supervisory and control function over the EU institutions (Art. 58(1)(a) & (f)). In addition, the EDPS oversees major EU information systems, including Eurodac, VIS, ETIAS, and SIS II (Art. 57(1)). It can audit the security of biometric data repositories and investigate unlawful data sharing between agencies (Art. 58(1)(g)). The EDPS also formulates security and privacy standards for EU institutions (Art. 57(1)(b)). It advises EU legislators and is responsible for assessing every new European law affecting data (Art. 42(1)). The EDPS issues official opinions on draft regulations, directives, agreements, and various

initiatives (Art. 42(2)). In fact, it was the EDPS that criticised the EU-US data transfer agreements (Safe Harbour, Privacy Shield, or DPF).

Moreover, the EDPS manages the network of data protection officers (DPOs) within institutions, thereby coordinating the work of all EU bodies (Art. 45(2)). It establishes guidelines, security recommendations, standards for internal EU systems, and risk assessment rules (DPIA templates) (Arts. 39 & 89). Finally, the EDPS processes complaints from individuals whose data have been breached by an EU institution (Art. 63). The EDPS does not work directly with companies or Member States. That is the responsibility of national supervisory authorities and the EDPB, states in the Arts. 51–56 (GDPR, 2016). The EDPS specifically concerns data processed by European institutions, states in the (Art. 2(1)) (Regulation 2018/1725, 2018). The EDPS's expertise spans four mandates, each with its own priorities that shape the data protection landscape we know today. These range from the implementation of privacy mechanisms in EU institutions, the enshrinement of data protection rights after the Lisbon Treaty, states in the Art. 16 (TFEU, 2012) and Art. 8 (CFR, 2012), and the legislative revolution with the adoption of the GDPR and Regulation 2018/1725, to the development of a positive and secure digital future in the current mandate (Wiewiórowski, 2024).

As a result of these rapid changes in electronic communications and internet technologies in the early 2000s, email addresses and mobile numbers became primary marketing and sales tools, and technology enabled companies to collect and aggregate contact information for millions of people. The commercialisation of communications brought new challenges and forced the EU to reconsider its regulatory approach. First, the ePrivacy Directive was adopted, followed by the establishment of the EDPS, the supervisory authority responsible for monitoring data processing in EU institutions. To highlight the growing importance of data protection, the right to data protection was included in the EU Charter as a full-fledged fundamental right in 2009 (EuroCloud, 2018).

The CFR (2012) recognises the right to the protection of personal data as a fundamental human right: "Everyone has the right to the protection of personal data concerning him or her" (Art. 8). Craig and Búrca (2021) believe that the Charter's enshrinement of the

right to personal data protection as an independent right and its subsequent elevation to a primary source of law with the entry into force of the Lisbon Treaty in 2009 were significant moments in the development of the institution of personal data protection in Europe. Since then, the CFR has become a central reference point for the CJEU, which has increasingly relied on it in key cases, demonstrating that the codification of fundamental rights has a real, rather than symbolic, normative effect.

Furthermore, Craig and Búrca (2021) note that the CFR has created a form of jurisdictional competition, which has encouraged the CJEU to actively utilise fundamental rights. The CJEU has taken a stronger rights-based approach to data protection than in a number of other areas of EU law, for example, the CJEU's position in the case *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* (2010) is indicative, where it was the first to invalidate an act of secondary EU law for violating the rights to privacy and data protection and the first to apply the EU Charter to EU institutions – directly referring to the fundamental rights in the EU Charter. This case set a precedent for subsequent decisions, such as *Digital Rights Ireland* (2014), *Schrems I* (2015), and *Schrems II* (2020). This way, the CJEU decision transformed the EU Charter into a truly operational instrument, rather than a mere declaration.

Furthermore, Craig and Búrca (2021) argue that the enshrinement of the fundamental right to the protection of personal data in the EU Charter became the key structuring element and starting point for the development of data protection legislation, as for a long time the EU lacked its own direct economic freedom in this area, similar to the free movement of goods, services, capital, or people. Consequently, the judicial and regulatory system could not rely on market logic. Thus, the strong influence of fundamental rights on European data law is explained by a combination of normative innovations (the EU Charter), institutional competition, and the lack of pure economic freedom capable of structuring this area in a manner similar to other sectors of the internal market. Taken together, these factors explain why the Court of Justice of the EU has, over the past decades, developed a comprehensive, increasingly self-contained, and refined data protection doctrine, in which fundamental rights serve a dual function. On the one hand, they serve as a powerful tool for invalidating disproportionate measures, such as national data retention schemes, acts of EU institutions, or international agreements. On the other hand, fundamental rights shape the new content of EU law.

However, it is worth understanding that this evolution has inevitably encountered institutional difficulties: the task of balancing competing rights and interests often shifts to private actors—primarily large platforms—who are forced to perform the delicate balancing act of fundamental rights themselves.

4.3 The contemporary European framework for personal data protection since the 2010s

4.3.1 GDPR in practice: strengths, limitations, and criticism

The combination of problems with Directive 95/46/EC, from conceptual limitations to inconsistent enforcement, was one of the key factors that led to the need for reform and the replacement of the Directive with the GDPR. The GDPR adopts a risk-based approach, clear obligations, and more harmonised supervisory mechanisms (Cifaldi, 2023). In 2011, the European Data Protection Supervisor (EDPS) supported the Commission's 2010 "Comprehensive Approach on Personal Data Protection in the EU." The EDPS viewed it as a crucial step toward updating Directive 95/46/EC. It emphasised stricter principles such as consent and data minimisation as well as the rights of access, rectification, and portability. The EDPS also advocated for uniform standards across all EU activities and robust guarantees of fundamental rights. These guarantees were especially relevant in light of new technologies such as the Internet of Things (IoT) and tracking (Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions, 2010). Later, in 2012, the European Commission proposed a comprehensive reform of the 1995 Data Protection rules to strengthen online privacy rights and boost Europe's digital economy. The Commission's proposals updated and modernised the principles enshrined in the 1995 Data Protection Directive to bring them into the digital age. The reforms included a proposal for a Regulation establishing a general EU data protection framework. They also included a proposal for a Directive on protecting personal data processed for the purposes of prevention, detection, investigation, or prosecution of criminal offences and related judicial activities (European Commission, 2012).

The transition from regulatory reform to public perception is evident in the European Commission (2013), which reported that 74% of Europeans considered disclosing

personal data to be a major part of modern life. At the same time, 72% of Internet users were worried they were sharing too much personal data. This indicated that fading trust in online services and tools began to hold back the growth of the digital economy and Europe's digital single market. In response to this challenge, the EU's Justice Commissioner and Vice-President Reding emphasised the need for regulatory reform. She stated that "a uniform and modern data protection law for the European Union is exactly what we need to secure trust and generate growth in the digital single market" (European Commission, 2013). Building on these concerns and regulatory developments, this policy shift soon became evident in 2013. Specifically, that year, the European Commission adopted Regulation No. 611/2013 and introduced mandatory notification requirements for personal data breaches under Directive 2002/58/EC. The Commission aimed to enhance transparency and accountability (European Data Protection Supervisor, 2026). This shift also influenced the judiciary. For example, the CJEU, in the case *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014), recognised that individuals could request the removal of search engine results associated with their names. This principle became widely known as the "right to be forgotten." The ruling further strengthened individual control over personal data in the digital environment.

One prominent example of this tension is the Data Retention Directive (Directive 2006/24/EC, 2006). It required the retention of data generated or processed in connection with publicly available electronic communications services and public communications networks (Art. 3(1)). The directive aimed to facilitate crime prevention and national security objectives by mandating large-scale data storage by private service providers (Arts. 1(1) & 3(1)). However, the directive's implementation revealed significant structural problems. Its application varied widely across Member States. This variation reflected divergent national approaches to data governance (Art. 4). In some jurisdictions, authorities emphasised extensive data-sharing among administrative bodies to reduce duplication and improve efficiency (Art. 1(1)). In others, a more cautious, sector-specific approach was adopted, with the minimisation of privacy and confidentiality risks taking priority (Arts. 7 & 9). These concerns were further exacerbated by the blurring of boundaries between public and private actors in data governance (Arts. 3 & 4). As noted by Lieshout et al. (2007), "the boundaries between

stewardship and accountability for personal data can become unclear when the private sector is deemed an agent of the state." This problem became particularly visible in the context of mandatory data retention obligations.

Consequently, these governance challenges had significant repercussions. These issues not only created the risk of an uneven playing field for data controllers in the private sector, but they could also distort the level of data protection across Europe (Gao, 2025). As a result of these inconsistencies—coupled with persistent enforcement deficits and growing concerns about fundamental rights—the CJEU ultimately declared the directive invalid in the case *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (2014). Specifically, the Court held that the indiscriminate retention of personal data constituted a disproportionate interference with fundamental rights, particularly the rights to privacy and data protection. In light of these developments, the European Commission increasingly favoured regulations over directives in data protection. This legislative shift reflects a broader strategy to ensure greater uniformity in the application and enforcement of EU law, particularly in areas involving fundamental rights and cross-border digital activities.

With this regulatory context established, the EU next undertook a major data protection reform. Building on this momentum of reform, the next major development occurred in April 2016, when the EU adopted the GDPR after more than four years of intensive negotiations. As Jones and Kaminski (2020) point out, the GDPR's systemic corporate compliance system not only establishes extensive rules and guidelines from above to ensure a high standard of data protection, but is also closely monitored by robust enforcement and supervisory mechanisms (i.e., national data protection authorities with significant sanctioning powers) and an active human rights tribunal (namely, the CJEU, which serves as the highest authority for the protection of fundamental rights). Thus, the GDPR is based on the EU's human rights framework, making the co-governance system fundamentally different from a laissez-faire, self-regulatory regime. This progression illustrates how previous regulatory shifts and legal decisions laid a foundation for the GDPR's comprehensive approach.

One of the most significant changes brought about by the GDPR is the establishment of binding, directly applicable rules across all EU/EEA countries. The GDPR also brought in stricter sanctions to ensure compliance (Gao, 2025). The GDPR (2016) is directly applicable in all EU Member States (including EEA countries) to achieve greater harmonisation of national data protection laws and enforcement policies (Art. 3). As a result, it promotes the harmonisation of existing EU data protection legislation. It also expands data protection rights and commercial opportunities in the Digital Single Market (Watchter & Mittelstadt, 2018). The regulation achieves its goals in two ways. First, it enhances well-known data protection principles previously outlined in the data protection directive, such as consent and purpose limitation. Second, it incorporates new concepts, such as the right to be forgotten, the right to data portability, the requirement for data protection impact assessments, and privacy by design, among others" (Watchter & Mittelstadt, 2018).

First and foremost, the GDPR is considered from the perspective of regulatory design, not simply a set of legal norms. The GDPR goes beyond establishing material prohibitions. It constructs an institutional architecture in which compliance with the law is ensured through organisational roles, procedures, and the distribution of responsibility. This shifts the focus from ex post sanctions to ex ante risk management. It decentralises the interpretation of the law and embeds enforcement. Art. 5(2) GDPR (2016) states that compliance with the GDPR is not enough; it must also be demonstrated that compliance is built into processes. Furthermore, Art. 25 states that "The controller shall implement appropriate technical and organisational measures...," thereby transforming the law into an architectural requirement and establishing the normative basis for the DPO's role as a permanent interpreter. Art. 24 emphasises that "taking into account the nature, scope, context, and purposes of processing... the controller shall implement appropriate technical and organisational measures...." This basically forms a risk-based approach without creating universal rules, but instead shaping the rules for internal assessment.

Moreover, the GDPR (2016) stipulates that the controller and the processor shall designate a data protection officer (DPO). DPOs shall not receive any instructions regarding the implementation of these tasks (Arts. 37 & 38(3)). Thus, the EU deliberately limits the management hierarchy to protect regulatory rationality within

businesses. It was understood that national DPOs are physically unable to inspect thousands of companies and penetrate every processing system. To address this problem, some interpretation and primary control were transferred within organisations. This technique is called decentralised enforcement.

The GDPR (2016) defines personal data as "any information relating to an identified or identifiable natural person ("data subject")" (Art. 4), which basically means that personal data is all pieces of information that may be used alone or in conjunction with other pieces of information to identify, contact, or locate a person. Cifaldi (2023) believes that the term "information" should be used liberally and encompass both factual information (such as a person's identity or the presence of a certain drug in their blood) and subjective analyses (such as information, views, and assessments). Although the ECJ has since clarified, relevant legal analysis (the evaluation) does not constitute personal data, unlike information contained in a residence permit application and data from legal analysis (*YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S.*, 2014). Additionally, personal information can be in any format, including text, numbers, images, videos, and more (Craig & Búrca, 2021). Additionally, the phrase "any information" represents "the goal of the EU legislative to attribute a wide scope to that notion, which is potentially inclusive of all forms of information, not just objective but also subjective" (Finck & Pallas, 2020). The ECJ determined that metadata (such as location information or IP addresses combined with log files on retrieved web pages) that only permits the indirect identification of the data subject can still be considered personal data because it enables "to know the identity of the person with whom a subscriber or registered user has communicated and by what means, to identify the time of the communication and the location from which that communication took place" (*YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S.*, 2014).

GDPR further strengthens the substantive and procedural rights of individuals, empowering data subjects to play a more active role in protecting their data (Gao, 2025). Building on Art. 12 of the Directive 95/46/EC, the GDPR (2016) expands the right to access by introducing new elements: subjects' right to obtain information from the controllers regarding (i) the envisaged or applied storage period for their personal data, (ii) the existence of the right to rectification, erasure, restriction of data processing,

and objection to such processing, and (iii) the right to lodge a complaint with a competent DPA (Art. 15(1)(d)–(f)). Such a right makes it easier for data subjects to access their personal data, thereby strengthening their ability to verify the accuracy of that data and the lawfulness of its processing. Moreover, under the GDPR, the right to be forgotten is formally codified as a standalone right in Art. 17, featuring clarified and expanded normative elements and a stronger bite. The GDPR (2016) also introduces new rights for data subjects, for example, the "right to data portability." This right enables a data subject to obtain from the data controller a copy of his personal data "in a structured, commonly used and machine-readable format," where the data processing is automatic and based on consent (or necessary for the performance of a contract) (Art. 20(1)). A data subject is also entitled to transfer their personal data from one controller to another if it is technically feasible (Art. 20(1)–(2)). In addition, the Regulation creates new individual rights specific to algorithmic decision-making. These include the right to be notified of the existence of solely automated decision-making (including profiling) (Arts. 13–14), the right to be informed of the significance and envisaged consequences of such processing (Arts. 13–15), the right to obtain an explanation of the decision made by algorithms, as well as the right to contest that decision, express the data subject's point of view, and obtain human intervention on the part of the controller for such processing (Art. 22(3). Moreover, the Regulation improves the means for individuals to exercise their rights and seek legal redress. Most notably, it creates a class-action-like legal remedy for data subjects (Art. 80) and subjects processors to data subjects' claims for damages and regulators' administrative fines, just as it does for controllers (Art. 82(5)).

The GDPR (2016) establishes a more complex and robust system of compliance obligations for companies that apply regardless of whether individuals exercise their rights. The Regulation establishes a "privacy by design and by default" obligation to integrate data protection into information and communications technology, organisational processes, and infrastructure (Art. 25). In accordance with this obligation, technologies used to process personal data must be designed and created in such a way as to minimise data processing (including data volume, retention period, accessibility, and scope of processing), pseudonymize personal data as much as possible, and ensure transparency during processing (Art. 25). Thus, data controllers shall implement

appropriate technical measures (e.g., encryption, pseudonymization, and access controls) to ensure that personal data is protected, monitored, and secured by default. The Regulation adds the accountability principle as one of the core principles governing data processing, obliging data controllers to "be responsible for, and be able to demonstrate compliance with" its requirement (Art. 5(2)). Gao (2025) argues that, on the contrary, the Regulation establishes requirements for organisations' accountability to ensure data protection at the systemic level, complementing and protecting the exercise of individual rights. Jones and Kaminski (2020) emphasise that, taken together, the GDPR's accountability and privacy requirements by design and by default demonstrate its approach to corporate governance, which bears the hallmark of "collaborative governance" as a regulatory model.

The GDPR adopts a governance-oriented regulatory design, embedding compliance within organisational structures through accountability, risk-based obligations, and the mandatory appointment of independent Data Protection Officers. Gao (2025) and Jones and Kaminski (2020) believe that, taken together, the GDPR's accountability and privacy requirements, by design and by default, demonstrate its approach to corporate governance, which bears the hallmark of "collaborative governance" as a regulatory model. This approach clearly differs from the American model of business "self-regulation," as government plays a significant role (Kaminski & Malgieri, 2019). Under the GDPR, a systemic corporate compliance system not only establishes extensive rules and guidelines from above to ensure a high standard of data protection, but is also closely monitored by robust enforcement and supervisory mechanisms (i.e., national data protection authorities with significant sanctioning powers) and an active human rights tribunal (namely, the CJEU, serving as the highest authority for the protection of fundamental rights) (Jones & Kaminski, 2020).

In particular, since data protection is a fundamental right applicable to public actors and private firms (like the right to privacy), the GDPR is based on the EU human rights system, making the co-governance system fundamentally different from the Neuchâtel, self-regulatory regime (Gao, 2025; Jones & Kaminski, 2020). However, the GDPR is often criticised (e.g., Bincoletto, 2021) for failing to provide details on the measures controllers must implement to comply with the principle of data protection by design. Bincoletto (2021) points out the vagueness and complexity of Art. 25(1) GDPR hinders

its effective implementation. Waldman (2020) argues that "Art. 25 is a broad, vague, almost-meaningless, catch-all provision that does not reflect the privacy by design literature. Art. 25 is a repetition of other sections of the GDPR and lacks its own identity… The plain language of Art. 25 transforms privacy by design into nothing."

While the GDPR remains the normative core of the European digital constitution, it is structurally strained in 2026 and has not kept pace with practice in some respects. By 2026, concerns have intensified, as the existing system is being challenged not only by technological developments but also by evolving legislative practices within the EU itself. In particular, the European Commission's growing reliance on the so-called "bundled" regulatory approach, combining numerous significant amendments into large-scale simplification packages, has raised questions about the transparency, legal certainty, and integrity of the Union's regulatory architecture. As Alemanno (2025) argues in his preliminary analysis of the Omnibus I Simplification Directive concerning the CSRD and CSDD, this legislative strategy could weaken parliamentary oversight and undermine the systemic coherence of EU law. If this practice were to extend to data management or related areas of regulation, it risks undermining the carefully crafted balance between rights protection and regulatory predictability at the heart of the GDPR. Thus, tensions within the European model arise not only from technological acceleration and the fragmentation of enforcement, but also from internal institutional dynamics that could impact its constitutional character.

Three other main lines of academic criticism of the GDPR stand out in this regard. First, the GDPR follows a comprehensive, complex, and user-control-oriented model, yet it cannot achieve its aims, as it assumes a rational, informed data subject when, in reality, users do not read notices or understand the consequences of processing. Therefore, such a "user control" model can be called formalistic, where compliance is shifted towards checkboxes and consent interfaces. For example, Kwon et al. (2023) review 201 interdisciplinary studies, which show that the data subject rights model often fails to achieve its stated goals and that there is a serious gap between the idea of giving users control and the actual effectiveness of these rights. Other studies from 2018 to 2024 also show a gap between the proclaimed rights of data subjects and their actual implementation in research/application practice (Cejas et al., 2024; Shastri et al., 2019).

Second, criticism argues that the GDPR fails to address changes in the digital economy, particularly the transformations brought about by big data, as the idea of repurposing and maximising the economic and social value of personal data conflicts with established data protection concepts such as purpose limitation and data minimisation. The European Parliamentary Research Service (2020) states that "there is indeed a tension between the traditional data protection principles—purpose limitation, data minimisation, the special treatment of "sensitive data," the limitation on automated decisions—and the full deployment of the power of AI and big data." In his dissertation, Ajibade (2019) questions the compatibility of the GDPR with modern data analytics methods, particularly with regard to the principles of purpose limitation and minimisation. Moreover, the European Parliamentary Research Service (2020) observes that "there is indeed a tension between the traditional data protection principles—purpose limitation, data minimisation, the special treatment of sensitive data, and limitations on automated decision-making—and the full deployment of the power of AI and big data." Thus, the GDPR's logic conflicts with that of big data regulation. The GDPR is based on the principle of collecting minimal data and using it only for a specific purpose, whereas the logic of the digital economy is to collect large amounts of data, reuse it, and find new uses and purposes for processing it (Kalyanpur & Newman, 2019; Hijmans, 2016).

Thirdly, critics focus on the GDPR's economic impact and argue that the law has failed to achieve an optimal balance between market integration and the protection of individual rights. Research shows that GDPR compliance is expensive and significantly more difficult for small companies than for large ones, while large platforms adapt more easily. Johnson (2022) demonstrates in his study that the GDPR has reduced investment in tech companies, reduced data for marketing, reduced innovation in mobile apps, and impacted competition. Dixon (2025) also points out that the GDPR causes significant administrative costs, complications with the Digital Single Market, and fragmentation of enforcement.

4.3.2 From GDPR to a multi-layered data protection framework: supplementary EU regulations

In 2019, the case of *GC and Others v Commission nationale de l'informatique et des libertés* (2019) revealed the structural problem of the GDPR, namely the dependence of EU digital services on US infrastructure, the risks of cross-border data flows, and the incompatibility of standard IT solutions with the requirements of the GDPR after Schrems II. This identification of gaps and systemic risks showed that the GDPR did not stop EU legislative activity in the field of personal data protection (Graux et. al., 2025), but they became stimulators for the adoption of new regulatory decisions and add-ons to the GDPR: such documents as the EU Digital Services Act (Regulation 2022/2065), the EU Digital Markets Act (Regulation 2022/1925), the EU Data Governance Act (Regulation 2022/868), the EU Artificial Intelligence Act (Regulation (2024/1689) were adopted. Although the GDPR has successfully established a high standard of fundamental rights protection and has become a global benchmark (the Brussels effect), it is not the standard for regulating the modern digital economy (Shastri et al., 2019; Dixon, 2025; Saglam et al., 2022).

In particular, the GDPR regulates personal data at the constitutional level and enshrines principles such as lawfulness, purpose limitation, data minimisation, the rights of data subjects, and an institutional architecture (DPAs and the EDPB). Amending the GDPR would mean reconsidering the balance of fundamental rights. This risks fragmentation of enforcement and could weaken legal certainty. Thus, the GDPR has become the core around which the EU continues to develop and refine its personal data protection system. Criticism of the GDPR has become a catalyst for add-ons. New documents supplement it in areas where it is not intended to work at all. For example, in 2018, the EU adopted Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (EUDPR). This regulation primarily aligns data protection rules governing EU institutions with GDPR principles. The Deloitte research (2018) states that "the objective of the new rules is to offer EU citizens the same rights as they enjoy under the GDPR when interacting with EUIs." It reinforces the principle of accountability with requirements such as publicly accessible records of processing, which is stated in the Art. 31 (EUDPR, 2018), a risk-based approach to security of

processing (Art. 33), and an explicit obligation to notify personal data breaches to the EDPS (Art. 34). These elements are not structured in the same institutional and supervisory manner in the GDPR for private and national public sector controllers.

In 2022, the EU adopted Regulation 2022/868, known as the Data Governance Act (DGA). The DGA (2022) aims "to create a legal framework for data sharing for the benefit of the European single market, ensuring neutral access to data and interoperability and helping to avoid lock-in effects" (Rec. 2). To achieve this, it establishes a cross-sectoral EU framework that enhances trust and enables wider sharing and reuse of data, including data protected by the public sector and data voluntarily provided in the public interest. Strong safeguards for personal data are maintained through the application of the GDPR (Arts. 1–2). The DGA also sets rules for neutral data intermediaries and data altruistic organisations, which facilitate secure and trustworthy data sharing and support the development of common European data spaces across sectors and Member States (Arts. 4–8 & 10–12).

Heinzke et al. (2025) point out that the DGA, together with the Data Act, have become the real "pillar" of the "European Data Strategy." The EU adopted Regulation 2023/2854, more commonly known as the Data Act, to provide rules for access and control. It clarifies who can use data, under what conditions, and ensures fair, interoperable access to data from connected devices and systems. The Data Act (2023) gives individuals and businesses greater control over the data generated by connected devices (e.g., Internet of Things devices). Users gain the right to access and use data generated through their use of connected products. This data must be available by default in a structured, machine-readable format (Art. 3). The Act also allows this data to be transferred to third parties of the user's choice under clear conditions. This promotes portability and a competitive choice of services (Arts. 4-6). The law harmonises data exchange rules across sectors, including obligations for transparent, fair, reasonable and non-discriminatory (FRAND) terms, and combats unfair contractual conditions. This protects against vulnerabilities that may hinder the fair exchange of data (Art. 13). It supports the seamless flow of data and interoperability between participants. At the same time, it protects privacy, trade secrets, and intellectual property (Arts. 12-14). Thus, this dual architecture of the Data Act, together with the DGA, supports broader EU goals. It helps create a single data market, unleash innovation,

enhance competition, and ensure cross-industry data flows in line with European values (European Commission, 2024).

Later in the same year, two key documents were adopted: the EU Regulation 2022/2065, known as the Digital Services Act (DSA), and the EU Regulation 2022/1925, commonly known as the Digital Markets Act (DMA). The DSA became a framework for online intermediaries and platforms with obligations on transparency, risk management, and user data. Now, the GDPR applies to personal data aspects within the DSA. Harmeling (2025) states that it aims "to stop illegal content, harmful activities, and the spread of false information online." The DSA (2022) applies to all digital intermediary services that connect EU users to goods, services, or content (Art. 2). It follows a tiered regulatory approach (Harmeling, 2025). Under this system, the largest platforms and online search engines with more than 45 million average monthly EU users are designated as Very Large Online Platforms or Search Engines. These platforms are subject to enhanced obligations due to their systemic impact (Art. 33). In general, the DSA strengthens data protection safeguards by requiring greater transparency in advertising. It requires platforms to clearly explain why a particular advertisement is shown to a particular user, including the main targeting parameters and the data sources used (Art. 26(1)). Platforms must also provide a simple way to opt out of profiling-based advertising, including a one-click alternative where applicable (Art. 26(2)). Furthermore, the DSA provides enhanced protection for minors and sensitive data. It explicitly prohibits profiling-based advertising using children's personal data (Art. 28(2)) and prohibits the use of special categories of personal data under the GDPR for targeted advertising. This includes health, religion, or ethnicity (Art. 26(3)).

In contrast, the DMA focuses on competition and fair digital markets, with certain obligations related to the processing of personal data and compliance with the GDPR. Harmeling (2025) notes that this regulation aims to foster competition, strengthen consumer protection, and safeguard privacy in the digital sector by placing specific obligations on these dominant market players. The DMA (2022) imposes additional obligations on gatekeepers due to their significant market power (Arts. 1(2) & 5). The European Commission has formally appointed seven companies as gatekeepers under the DMA: Alphabet (Google), Amazon, Apple, Booking.com, ByteDance, Meta, and Microsoft (Art. 3). These gatekeepers must obtain explicit consent from users before

processing personal data for advertising purposes. The same applies to combining personal data across different core platform services, in accordance with the GDPR (Art. 5(2)). The DMA requires consent to be voluntary, specific, informed, and unambiguous (Art. 5(2)). Gatekeepers also face strict restrictions on data sharing between platforms (Art. 5(2)), preventing practices such as using WhatsApp data to target Facebook ads without explicit consent (Harmeling, 2025). Furthermore, the DMA requires data portability and effective user choice mechanisms. These allow users to transfer their data between competing services and strengthen control over their digital footprint (Art. 6(9)). Finally, the regulation prohibits gatekeepers from processing personal data obtained through third-party services using their platforms for advertising purposes unless valid consent is obtained. This significantly limits the scope of permissible data collection (Art. 5(2)).

Two other significant documents are the EU Directive 2022/2555, known as the NIS2 Directive, and the EU Regulation 2022/2554, better known as the Digital Operational Resilience Act (DORA). The NIS2 Directive (2022), which became effective and enforceable across the EU in October 2024, covers a wide range of "important" and "key" sectors: energy, medicine, transport, logistics, telecoms, digital infrastructure, and the production of key goods. It establishes a strengthened cybersecurity risk management and corporate governance framework for important and significant organisations (Art. 3). In contrast, DORA (2022) became applicable and enforceable in January 2025 and targets solely the financial sector by creating a comprehensive information and communication technology (ICT) risk management framework (Arts. 2 & 5–16). It introduces mandatory ICT-related incident reporting, requiring financial entities to notify competent authorities of major incidents within strict and short timeframes (Arts. 17–19), mandates regular digital operational resilience testing, including advanced testing methods for significant institutions (Arts. 24–27), and imposes stringent requirements for the management and oversight of ICT third-party service providers, covering contractual arrangements, risk monitoring, and supervisory oversight of critical providers (Arts. 28–44). Competent authorities are empowered to impose effective, proportionate and dissuasive penalties, including administrative fines, for breaches of the Regulation (Arts. 46–54). Similarly, the NIS2 Directive (2022) establishes a harmonised enforcement framework requiring Member States to impose

administrative fines proportionate to the severity and duration of cybersecurity breaches, thereby reinforcing compliance incentives across critical sectors (Art. 34).

It is worth mentioning that the EU Regulation 2024/1689, known as the Artificial Intelligence Act (AI Act), which will be fully effective in August 2026, builds on the provisions of the GDPR by adding specific rules for the development and use of AI systems, focusing on security, transparency, and accountability, going beyond the general data protection principles of the GDPR. It is clear that most high-risk AI systems process personal data (often sensitive), thus organisations must comply with both regulations, meaning that GDPR compliance is typically required alongside new AI-specific obligations (Gonzalez-Riedel & Idema, 2024). In certain cases, the AI Act (2024) adds new obligations or exceptions to the GDPR, such as permitting the processing of sensitive data solely for the purpose of identifying and correcting bias, subject to safeguards, such as pseudonymization (Art. 10(5)). It also introduces risk-based requirements, such as establishing a risk management system that continuously identifies and mitigates risks throughout the lifecycle of an AI system (Art. 9) and imposing obligations for structured documentation and oversight of high-risk systems. These measures strengthen data protection by requiring AI developers and deployers to assess and mitigate risks to individuals' rights and freedoms (Art. 9). Overall, the AI Act strengthens and contextualises GDPR principles within the lifecycle of trusted AI systems, making GDPR compliance necessary for obtaining a certificate of compliance for high-risk AI and helping organisations interpret how data protection applies to AI (Schuler, 2025).

Another document that supplements the GDPR is the EU Regulation 2024/1183, now known as eIDAS2.0 (2024), which aims to establish a harmonized framework for digital identification and trust services that ensures the confidentiality, integrity, and authenticity of personal data processed during electronic identification and transactions, while explicitly complying with key provisions of the GDPR, such as the data subject's rights of access, rectification, and erasure (Art. 2(4)). It emphasizes user consent and transparency by requiring European digital wallet providers not to collect or combine personal data beyond what is necessary for the operation of the wallet without the explicit request of the user (Art. 5a(14)), thus reinforcing the principles of the GDPR in the specific context of digital identification and authentication services (Prinz & Hille,

2025). It also promotes data minimisation, for example, through selective disclosure mechanisms that allow users to share only necessary information with interested parties. Thus, eIDAS2.0 (2024) helps reduce unnecessary disclosure of personal data beyond what is required by the GDPR (Rec. 54 & 55). Furthermore, eIDAS2.0 strengthens cross-border data protection by harmonising the provision and acceptance of European digital identity wallets across Member States, thereby helping to ensure compliance with GDPR data protection standards when using personal data across different national systems (Art. 5f).

Last but not least, at the end of 2025, the EU introduced the Digital Omnibus Proposal (2025), which aims to simplify the European digital regulatory system, including data, AI, cybersecurity, and platform regulation, without reducing the level of safeguards. Compared to the GDPR, the Digital Omnibus should adjust key procedural rules, such as extending the data breach notification period from 72 to 96 hours and aligning the requirement to notify only if there is a "high risk" to affected individuals, which will simplify the reporting process for data controllers (Art. 33). In addition, the Digital Omnibus proposes adding new provisions on cookie consent and device access, which would transpose the core ePrivacy rules regarding cookies into the GDPR and require one-click opt-in/opt-out and respect for automated "privacy preference signals" once technical standards are adopted (Art. 88a-88c). Herbers et al. (2025) argue that such changes modernise consent management and integrate ePrivacy concepts, such as the low-risk exception and machine-readable preferences, directly into the GDPR framework while preserving core data protection principles, providing clearer and more consistent rules for digital practices. Also, Herbers et al. (2025) point out that the Digital Omnibus "lands at an inflexion point in EU tech regulation," as it "re-keys several obligations, consolidates overlapping regimes, and introduces new "digital by design" compliance rails, notably a single cyber incident reporting entry point." Thus, this proposal promises to reduce the existing compliance burden and clarify the interaction of rules. As Herbers et al. (2025) note, the key message of the new document is "clear, simple, more cost-effective, and above all innovation-friendly implementation of the rules."

However, it is important to mention that this simplification approach is not without controversy. Alemanno (2025) warns that increasing reliance on complex legislative

methods could undermine the structural integrity of EU law by consolidating disparate regulatory changes into single legislative instruments. As a result, such consolidation risks weakening parliamentary oversight, compressing deliberative processes, and obscuring the normative trade-offs inherent in complex regulatory regimes. In the context of data governance, the pursuit of simplification and cost-effectiveness could shift the balance from human rights-based guarantees to administrative convenience and economic competitiveness. Thus, while the "Digital Omnibus" wants regulatory clarity and rationalization, it simultaneously raises constitutional questions regarding transparency, institutional balance, and the long-term integrity of the Union's digital regulatory framework. Running alongside the Digital Omnibus, in June 2025, the Council of the EU and the European Parliament reached an agreement on reforms to cross-border enforcement procedures under the GDPR. Grossman (2025) believes that "these reforms focus specifically on fixing weaknesses in the GDPR's cooperation and consistency mechanisms, which have historically led to slow investigations and inconsistent outcomes in cross-border cases." Overall, these reforms aim to speed up the handling of cross-border complaints; improve cooperation and information-sharing between national data protection authorities; and reduce procedural bottlenecks where multiple regulators are involved (European Parliament & Council, 2025).

In summary, the combination of all of the above documents, along with the GDPR, demonstrates that the EU is moving toward creating a single, multi-layered data governance system, with experts predicting a new trend in 2026, namely, the relaxation of existing digital rules (Burton et al., 2026). In this regard, back in November 2025, the European Commission published proposals to simplify the EU legal framework for data processing and AI, launching a legislative process that will last until 2026 and possibly beyond (Burton et al., 2026). Among other key trends in 2026, specialists (Haie, 2025) highlight that the enforcement of certain high-risk AI requirements will be postponed until all compliance tools, guidance, and national authorities are fully ready, with deadlines extended to 2027–2028. In addition, a trend toward practical, risk-based regulation is emerging: the notion of personal data will be clarified as relative to the recipient’s means of identification, and greater flexibility is proposed for AI development, automated decision-making, transparency obligations, and breach notification thresholds (including extending the reporting deadline to 96 hours) (Haie,

2025). The final trend is the consolidation and simplification of data regulations, as the Data Act will merge rules from the Free Flow of Data Regulation, the Data Governance Act, and the Open Data Directive, with lighter obligations for SMEs and mid-caps, exemptions for custom-made services, and clarified reuse of public sector data, demonstrating a move toward a single, coherent EU data framework (Haie, 2025). Against this backdrop, the EDPS will continue to play a key role in the development and practical implementation of key EU data protection legislation (Wiewiórowski, 2024).

4.3.3 Judicial interpretation of the right to data protection in Europe: ECtHR, CJEU, and national courts

However, the development and transformation of the European approach to personal data protection occurs not only through new regulations (such as the AI Act, DSA, DMA, and others). It also develops through the European Court of Human Rights' (ECtHR) judicial interpretation of the fundamental right to data protection (Eskens, 2020). The right to personal data protection continues to evolve through judicial practice, thanks to the ECtHR's interpretation of Art. 8 ECHR. The ECtHR has built a rich Art. 8 practice that reinforces data protection principles (Koops & Sluijs, 2012). The ECtHR significantly expands and clarifies the content of Art. 8 (European Court of Human Rights, 2024). This indirectly affects how the GDPR should be understood and applied. This is a continuation of regulatory development. First, it has condemned excessive secret surveillance (*Roman Zakharov v. Russia*, 2015; and *Big Brother Watch and others v. The United Kingdom*, 2021). It also affirmed individuals should have a right to know about and challenge personal data held by authorities (*Segerstedt-Wiberg and others v. Sweden*, 2006; *M.M. v. The United Kingdom*, 2012). In the 2017 judgments (*Aycaguer v. France*, 2017; *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, 2017), the ECtHR explicitly acknowledged Art. 8 ECHR as encompassing a form of "informational self-determination." It aligned its language with the data protection concept and emphasised that the protection of personal data plays a "paramount role" in ensuring the right to respect for private life. These 2017 cases laid the foundation for the modern understanding of the GDPR and the recognition of the "digital dignity" of individuals. They confirmed that a person does not lose rights to

their data just because it ends up in a state database or becomes public (Rossi Dal Pozzo & Zoboli, 2021).

Meanwhile, the Court of Justice of the EU (CJEU) is central in shaping data protection within the EU. Its interpretations of the GDPR and related laws are binding across all member states, effectively harmonising understanding and enforcement. The CJEU has issued key decisions striking down laws and even creating new rights. For example, it created the right to be forgotten, a right not previously formalised (*Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014). This ruling significantly changed data processing practices across Europe and was later codified in Art. 17 GDPR. The CJEU also annulled the Data Retention Directive 2006/24/EC, establishing strict constitutional limits for data retention and laying the foundation for future practice on surveillance and metadata (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, 2014). In subsequent cases, such as *Maximillian Schrems v Data Protection Commissioner* (2015) and *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* (2020), the CJEU formulated the adequacy standard and established a new compliance-by-design system for international data transfers, serving as a leading reviewer of transfer mechanisms. More recently, in *Meta Platforms Inc and Others v Bundeskartellamt* (2023), the CJEU continued to clarify granular GDPR questions, holding that even inferences about a person's health, drawn from purchasing habits, are considered sensitive personal data if they indirectly reveal health information. As a result, the decision became the starting point for profiling, behavioural advertising, and inference-based analytics to fall under the strictest protection regime, with the court significantly expanding the concepts of personal and sensitive data (*Meta Platforms Inc and Others v Bundeskartellamt*, 2023).

The CJEU clarified the legal basis for processing in *Orange Romania SA v. National Authority for the Protection of Personal Data* (2020). Silence, pre-checked boxes, or general agreements with embedded consent do not qualify as valid consent. The client must take a clear, conscious action to agree to data processing. This strengthens consent standards under the GDPR and makes Arts. 4(11) and 7 real compliance tests. In *Fashion ID GmbH & Co. KG contro Verbraucherzentrale NRW eV* (2019), the CJEU

developed the concept of joint controllership. It was decided that a website embedding a third-party social plug-in shares responsibility for any data collected by that plug-in. This extends accountability across the data ecosystem and adapts the GDPR to platform-based businesses. Another case, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme"* (2017) clarified the "legitimate interests" ground. The court stated that a controller's interest must be genuine, and the data subject's interests can override it if processing is unexpected. This introduced an objective "reasonable expectation test" to limit misuse.

As well, the CJEU fills GDPR gaps. Although the GDPR does not define standards for non-material damage or psychological harm, recent and coming cases in 2026 (*UI v Österreichische Post AG* (2023); *UI v Österreichische Post* (2023); *VB v Natsionalna agentsia za prihodite* (2023); *JU and SO v Scalable Capital GmbH* (2024) clarify compensation for such harm under Art. 82. In 2025, the CJEU confirmed that data is only personal for recipients who can lawfully and reasonably re-identify individuals. It held that comments expressing personal views are closely linked to identity. This set a strict transparency standard in the EU (*European Data Protection Supervisor v Single Resolution Board Case* (2025). Also in 2025, the CJEU ruled that, in setting administrative fines, authorities must consider the offender's real economic strength, including the full group, not only the legal entity (*Criminal proceedings against ILVA A/S* (2025). This makes fines under Art. 83 of the GDPR is more effective and helps harmonise practices across the EU. Finally, that year, the CJEU broadly interpreted Art. 15(1)(h) GDPR. It confirmed that data subjects have a right to meaningful information about automated decisions, including the system's logic and the specific data that influenced the outcome. Companies must explain their system so people understand which data affected decisions and how results could differ (*CK v Magistrat der Stadt Wien*, 2025). This decision strengthened transparency in algorithmic governance and increased protection from "black box" decision-making.

Moreover, it is crucial to note that national constitutional courts continue to shape the landscape of data protection standards. For example, Germany's Constitutional Court issued judgments that affected the interpretation of the GDPR and the CJEU's position. The court invalidated expansive data retention laws (*Rechtsprechung BVerfG Az. 1 BvR 256/08 u.a.,* 2010) and ordered strict proportionality for police surveillance powers (*Die*

Entwicklungen und das Jahr 2020, 2020). In 2025, the German Federal Court of Justice also ruled on claims for damages under the GDPR. It clearly stated that Art. 82 GDPR has a purely compensatory, rather than punitive or preventive, function (*Rechtsprechung BGH VI ZR 183/22*, 2025). Furthermore, the decision set a benchmark for German courts. In typical cases, courts will award "moderate" rather than symbolic amounts for the illegal transfer of data to credit bureaus. For example, in this case, the court awarded 500 euros in compensation for the transfer of data on the plaintiff's "debt" to Germany's largest credit bureau, SCHUFA (*Rechtsprechung BGH VI ZR 183/22*, 2025). In another case, the court recognised that although loss of control over data is a form of harm, in the context of a single email, this harm is insignificant. To award compensation in such cases, the violation must have a certain "weight" (*Rechtsprechung BGH VI ZR 109/23*, 2025). In France, the Constitutional Council influences the legitimacy of national implementations of the GDPR. It has reviewed surveillance laws against privacy guarantees, at times striking down provisions (*Décision N. 2018-765 du Conseil constitutionnel*, 2018). Another representative case is *Lloyd v Google* (2021). There, the court set boundaries on collective privacy damage claims, influencing how data protection rights are enforced in the UK. It limited claims for minor or technical violations where the harm is considered "frivolous" (de minimis). Thus, such decisions are part of the process by which national courts develop GDPR standards through case law. This, in turn, influences pan-European judicial dialogue and future applications to the EU Court of Justice (Gibson, Dunn & Crutcher LLP, 2021).

In summary, contemporary case law serves as the living instrument of data protection rights. It ensures that broad principles are applied to concrete situations. This ongoing judicial dialogue among the ECtHR, the CJEU, and national courts keeps the European data protection framework adaptable. It also underscores that the right to personal data protection in Europe is deeply jurisprudence-driven. Judges have entrenched it as a fundamental right and balanced it against other interests (such as freedom of expression or public security). This ensures it remains meaningful as society and technology evolve. This jurisprudence-driven development complements legislative layering at the EU level. It demonstrates that data protection in the EU remains a dynamic regulatory field, shaped by continuous interaction between legislation and case law (Lynskey, 2020; Kuner, 2020; Schwartz & Solove, 2014).

Chapter 5. Discussion of the results and findings

This chapter summarizes the results of the historical and comparative legal analysis conducted in the previous chapters and interprets them in the context of the dissertation's research questions. The study proceeded from the assumption that contemporary personal data protection regimes in the United States, Russia, and Europe are not entirely new legal constructs, but rather adaptive extensions of historically ingrained legal traditions and subsequent threat perception practices. The comparative analysis confirms this assumption, demonstrating that historical continuity plays a decisive role not only in shaping the structure of modern data protection systems but also in defining their regulatory blind spots and structural limitations.

Initially, it was assumed that the effectiveness and efficiency of regulation depended not only on the text of laws. Rather, the entire legal system, including the institutional structure, enforcement mechanisms, judicial interpretation, and historical development, was important. The study's findings also show that effectiveness is determined by the interaction of legal norms and broader regulatory governance structures, including administrative capacity, political priorities, and technological infrastructure. It was also assumed that discrepancies between the three regulatory models would persist despite technological convergence and international coordination. Underlying threat perceptions were expected to systematically influence legislative programs and enforcement. The study's findings largely confirm these assumptions. Each system reflects a consistent internal logic rooted in history: a "skeleton" that persists but acquires "muscle" and "skin" through subsequent laws and enforcement.

None of the three models provides comprehensive protection against all contemporary data protection risks. Each exhibits its own strengths and weaknesses, determined by its legal culture and institutional priorities. The limitations observed in various jurisdictions are not simply implementation failures but reflect the structural contradictions inherent in modern data protection legislation. The results of this dissertation confirm that even the most coherent legal framework can suffer from deficiencies in effectiveness when institutional capacity varies and compliance becomes procedural rather than substantive. Thus, the effectiveness of regulation depends not only on legislative ambition but also

on the interplay between the law, institutions, enforcement culture, and political economy.

A comparative analysis reveals a persistent divergence between the US, EU, and Russian models. This divergence cannot be reduced to temporary political circumstances. Instead, it reflects deeper constitutional philosophies, threat perceptions, and governance logics. The US model prioritizes innovation, competition, and litigation-based redress. The European model enshrines personal data protection as a fundamental right. The Russian model embeds data governance within the rationale of sovereignty and security. Thus, the dissertation's findings challenge simplistic classification approaches. Labels such as "centralized," "hybrid," or "sectoral" obscure deeper institutional processes. Regulatory effectiveness cannot be inferred solely from structural typology. Legal reforms and legislative harmonization do not automatically lead to functional convergence when institutional capacities and enforcement cultures differ.

An analysis of the approach to personal data protection in the United States reveals a regulatory model characterised by flexibility, fragmentation, sectoral legislation, and a heavy reliance on ex post facto enforcement mechanisms. This structure is not arbitrary, but reflects deeply rooted constitutional traditions that emphasize limited government intervention, economic freedoms, and judicial remedies over comprehensive administrative regulation. The results show that the US system provides relatively strong protection in specific high-risk sectors (e.g., healthcare, finance, and children's data), but there are significant gaps in terms of overall personal data protection. The FTC plays a central role as the de facto data protection authority, but its mandate remains indirect and relies on concepts of unfairness and deception rather than the general right to protect personal data. These results confirm that the US model prioritizes adaptability and effective enforcement over coordinated regulation, standardization, and unification. While this approach allows for a rapid response to emerging risks through litigation tailored to the specific context of the case, it also creates legal uncertainty and uneven protection. In practice, individuals' rights depend largely on the sector in which their data is processed and their ability to utilize enforcement mechanisms after harm has occurred, and companies are unclear about the standards they should rely on to legally and securely serve customers across the country.

In contrast, the Russian data protection system reflects a fundamentally different regulatory structure and logic. Contemporary Russian data protection legislation, while formally compliant with international standards (e.g., Convention 108), is shaped by Soviet legal traditions, centralized governance, and security-oriented control of information. As a result, data protection is increasingly viewed not as an individual right, but as an administrative issue related to state sovereignty and national security. Although Russia has created a relatively coherent legislative framework with formal privacy guarantees, its effectiveness is limited by broad administrative powers and a cumbersome judicial system, whose courts issue inconsistent decisions. This creates confusion and complicates the application of data protection rules by companies, while individuals remain in the dark about what actually constitutes personal data. From 2022, legislative changes signal a shift from the prevention of data leaks and illegal collection to tighter state control over data flows, with stricter sanctions for violating localization requirements. Thus, the Russian model provides robust protection against foreign exploitation and cross-border data risks, but offers limited guarantees against state interference. This imbalance leaves key legislative gaps in personal data protection unaddressed. Analysis shows that effectiveness in this model is measured primarily by state control and resilience to security threats, rather than by the empowerment of individuals, raising normative questions about the very criterion used to assess "protection."

Compared to other systems, the European model proves to be the most structurally coherent and normatively consistent of the three regimes examined. Recognition of personal data protection as a fundamental right, underpinned by constitutional traditions and supranational judicial review, provides a solid regulatory foundation. The GDPR undoubtedly represents the culmination of a long historical process, but it is not its end point. The analysis shows that European data protection law offers the most comprehensive set of individual rights, including transparency, access, rectification, erasure, and accountability. The institutional architecture, consisting of independent supervisory authorities and coordinated enforcement through the European Data Protection Board, enhances regulatory consistency across jurisdictions. However, the results reveal significant limitations. Enforcement is uneven across member states. Compliance costs are high, particularly for smaller organisations that face a heavy

regulatory burden. The consent-based model also struggles to address the power imbalances on large data-driven platforms. Moreover, as research on regulatory governance shows, the increasing density and multilayered nature of digital technology regulation in the EU risks creating complexity that could undermine accessibility, clarity, and democratic legitimacy. While Europe provides the highest formal level of protection, practical effectiveness depends on institutional capacity and a culture of enforcement.

A comparative assessment of the three systems presented above shows that regulatory effectiveness depends on systemic coherence, not on the strictness or number of individual legal norms. However, coherence alone does not guarantee substantive protection if individuals remain structurally vulnerable within data-driven ecosystems.

The strength of the American model lies in its flexibility. Individual states, taking into account the local context and without additional bureaucracy, can formulate and adopt more relevant and effective legislation in a shorter timeframe than one adopted at the federal level, which may already be outdated due to the lengthy process of formulation and adoption. Its weakness lies in fragmentation, the lack of universal protection, and the practical difficulty of developing a unified policy for companies with customers in all states. Opportunities lie in potential convergence through state-level initiatives and sectoral expansion, while political resistance to comprehensive federal regulation remains a limitation.

The strength of the Russian model lies in its centralised control and the ability to quickly intervene in regulation. Its weakness lies in limited and fragmented judicial oversight and insufficient protection against state abuse of power. An opportunity lies in improving institutional transparency and developing a unified approach to judicial enforcement, while a limitation is the dominant security-oriented governance paradigm.

The strength of the European model lies in its human rights coherence and institutional independence. Its weakness lies in the decentralised enforcement structure and different institutional capacities in different Member States that often lead to inconsistent application of formally uniform EU rules. In addition, the European model's reliance on individual rights and consent assumes a level of rational agency on the data subjects that may not fully reflect structural power imbalances in digital markets. An opportunity lies

in improving enforcement mechanisms and more carefully considering the feasibility, appropriateness, and timeliness of applying certain norms across all EU member states, while a limitation remains the tension between harmonisation and national legal diversity.

The main contribution of this study is to demonstrate that personal data protection cannot be effectively assessed solely on the basis of individual legal provisions or current regulatory texts. Instead, regulatory effectiveness is determined by the interaction between historical legal traditions, institutional design, threat perception, enforcement culture, and increasingly, technological infrastructures that embed regulatory norms into code and algorithmic systems. The study challenges the assumption that convergence to the European model is inevitable or normatively superior in all contexts. Although the European system provides the highest level of formal protection, its effectiveness depends on institutional capacity and cultural acceptance. In contrast, the US and Russian systems, often portrayed as imperfect, demonstrate internal consistency when analysed within their historical and institutional contexts.

Copying the practices of one region to another seems impossible, as there is a high risk that this approach will simply not take root in the other region due to its distinct historical legal tradition, institutional design, and available resources. Furthermore, it is worth noting that no system is perfect at protecting personal data. More fundamentally, the analysis suggests that modern data protection law faces a structural paradox: while it aspires to safeguard autonomy and dignity, it operates within digital economies built on large-scale data extraction, inference, and predictive analytics. Thus, by integrating historical analysis with doctrinal and institutional assessment, this dissertation offers a more nuanced framework for assessing data protection regimes. It suggests that future reforms should focus not on copying foreign models, but on strengthening internal systemic coherence and addressing context-specific vulnerabilities.

In response to the central research question: "which regulatory model provides the most effective protection for personal data when assessed as a comprehensive legal system?", the results show that no single model fully satisfies all criteria of effectiveness, efficiency, sustainability, and legitimacy. The European model currently offers the most

comprehensive and rights-oriented personal data protection system. However, its effectiveness depends on consistent law enforcement, institutional capacity, resources, and an established culture in both society and lawmaking. The American model is characterised by the flexibility and adaptability of law enforcement, but lacks systemic consistency and standardisation. The Russian model ensures strict government control over data flows but offers limited protection in practice.

Ultimately, the study demonstrates that effective personal data protection requires a balanced combination of regulatory clarity, institutional independence, enforcement capacity, and historical continuity. It also requires confronting structural vulnerabilities inherent in data-driven governance and recognising that regulatory models are embedded in broader political and economic orders. The persistence of divergent regulatory models is not a failure of harmonisation or the result of inept policy, but a reflection of deeply entrenched legal traditions that continue to shape regulatory responses to digital transformation.

Taken together, the findings reveal a broader normative tension common to all the jurisdictions examined. Data protection law seeks to protect dignity, autonomy, and control, while the digital economy relies on scale, reuse, inference, and predictive analytics, and governance is increasingly exercised through algorithmic infrastructures rather than traditional litigation. This creates a structural paradox: the more technologically integrated society becomes, the less effective individual rights protection mechanisms appear as primary instruments of protection. Thus, this dissertation aims at contributing to scholarship not only by comparing regimes but also by demonstrating that personal data protection is evolving from a classic rights-based project to a hybrid governance ecosystem that combines law, institutional design, technological architecture, and economic power.

Conclusions

The purpose of this dissertation was to determine which regulatory model provides the most effective protection for personal data when assessed as a comprehensive system, rather than as a collection of individual legal instruments. Based on a historically informed and structurally integrated comparative analysis of the United States, Russia, and Europe, the study demonstrated that the effectiveness of personal data regulation cannot be assessed solely on the basis of legislative regulation or formal legal harmonization. Instead, it depends on the degree of systemic coherence, institutional architecture, enforcement mechanisms, and prevailing perceptions of digital threats.

The main conclusion of this study is that there is no universally optimal model of data protection regulation. Each jurisdiction studied reflects its own historical trajectory, legal culture, and understanding of the relationship between the individual, the state, and the digital environment. These structural foundations determine both the strengths and weaknesses of the respective regulatory systems. Consequently, regulatory effectiveness should be understood as context-specific rather than universally applicable.

When assessed using the systemic coherence criterion, the European Union currently exhibits the highest degree of structural integration among the systems examined. Its legal framework demonstrates a comparatively strong coherence between the fundamental rights doctrine, supranational institutional coordination, and harmonized legislative standards. However, this structural integration does not eliminate asymmetries in implementation or differences in enforcement among member states, which continue to determine the practical effectiveness of the regime. The United States model illustrates a different regulatory logic characterised by adaptability, sectoral differentiation, and institutional pluralism. Although this approach ensures regulatory flexibility and responsiveness to technological innovation, it lacks comprehensive structural coherence. The lack of a comprehensive federal structure leads to fragmentation, which impacts the coherence and predictability of protection. Russia reflects a model based on centralized institutional control and consolidated supervisory authority. This structure ensures regulatory clarity and administrative coherence but demonstrates a limited balance between state authority and guarantees of individual

rights. The balance between security-oriented governance and rights-based protection remains a defining structural feature of the system.

The results of this study support the thesis that historical developments fundamentally shape the modern approach to regulation. Legal traditions, constitutional principles, and previous experiences with government influence not only legislative decisions but also judicial practice, institutional trust, law enforcement culture, and threat perceptions. Therefore, data protection regimes cannot be meaningfully assessed outside their historical and political context. Beyond jurisdiction-specific differences, the comparative analysis reveals structural challenges common to all the regimes examined. For example, there remains a persistent imbalance between the capacity of government regulation and the rapidly growing technological power of private digital platforms.

This dissertation contributes to comparative data protection research by presenting a historically grounded systemic assessment framework that integrates legislative, institutional, judicial, and geopolitical considerations into a unified analytical model. By shifting the focus from formal legal comparison to structural coherence and contextual embeddedness, the study proposes a methodological approach that can account for the diversity of normative acts without reducing it to normative hierarchies.

The broader significance of this dissertation is that it challenges reductionist assessments of data protection regimes. The study demonstrates that labels such as "centralised," "hybrid," or "sectoral" are insufficient analytical tools. Regulatory models should not be assessed as inherently good or bad based on their structural classification, but rather through a contextual analysis of how they function in practice.

The dissertation also highlights the growing imbalance between state regulatory power and private technological power. Large digital platforms increasingly determine the practical rules of data processing, shaping norms through technical design, contractual structures, and market dominance. State attempts to counter such entities solely through restrictive regulation often prove ineffective. Instead, the analysis suggests that future regulatory strategies may benefit from considering structured forms of collaboration, dialogue, and co-regulation, enabling governments to act as equal participants rather than passive observers in the governance of digital ecosystems.

The study builds on and expands on the work of scholars, lawyers, political scientists, and analysts from around the world, demonstrating that data protection is not simply a contemporary regulatory response to digitalisation and automation, but a historically entrenched legal institution. Unlike purely synchronous comparative studies, this dissertation explains why regulatory divergence persists, why this is normal, and why legal borrowings often fail when divorced from their institutional context. Moreover, the study incorporates Russian data protection legislation and case law into the comparative analysis on an equal analytical footing, challenging its frequent portrayal as a simple deviation from European standards. By exploring its internal logic and historical continuity, the study offers a more balanced and explanatory account of the Russian model.

The dissertation also opens several avenues for further, more focused research. One important area is expanding the comparative paradigm beyond Western and post-Soviet models. Existing scholarly work, including studies examining the broadening impact of the GDPR in third countries (e.g., Gubenko, 2022), has examined whether and how regulatory practices developed in the European Union can be applied in jurisdictions with different legal traditions. While such analyses provide valuable insights into the diffusion of norms and the impact of regulation, they often view non-European systems through the lens of compliance with or divergence from the GDPR model.

This dissertation proceeds from a different premise. Legal norms do not operate in isolation; their effectiveness depends on the local institutional context, enforcement structures, administrative culture, judicial practice, and the actors responsible for implementation and compliance. When any element of this chain is structurally inappropriate, the effectiveness of the transferred norms is significantly weakened. Consequently, simply transferring regulatory models between jurisdictions does not guarantee functional equivalence or improved protection. Instead of examining the export or replication of GDPR standards, future research should focus on analyzing local regulatory practices, such as those in jurisdictions such as Japan, South Korea, China, and Singapore. These systems offer alternative governance configurations. A context-sensitive examination of their legislation, enforcement models, and judicial interpretation would allow us to identify regulatory approaches that function effectively in their respective socio-political contexts. Rather than viewing "Asia" as a

homogeneous normative space, the study would compare carefully selected models representing different regulatory logics: regimes reflecting GDPR-influenced reforms in Japan and South Korea (European Commission, 2019; Wahl, 2021), a hybrid compliance-focused system in Singapore (Chander & Sun, 2023), and a state-centered governance system in China (He & Fay, 2023).

Overall, the goal is not to hierarchically rank systems or promote regulatory transplantation, but to identify the structural conditions under which specific regulatory instruments prove effective. By analyzing strengths and weaknesses, implementation gaps, and institutional capacity across regions, such research can contribute to the development of more realistic, context-sensitive recommendations for policymakers. This approach recognizes that sustainable data protection reform requires internal systemic coherence rather than the uncritical adoption of external models.

In conclusion, this dissertation demonstrates that effective personal data protection cannot be achieved through uniform legal solutions or abstract regulatory models. Instead, sustainable and legitimate data protection frameworks must be historically grounded, institutionally embedded, and account for real power dynamics and available resources. By adopting a comparative and context-sensitive approach, this study contributes to a deeper understanding of personal data protection as a living legal institution and lays the foundation for future interdisciplinary and transnational research.

References

1. Scholarly Literature: Books, Peer-Reviewed Articles, and News Reports

1. Aftergood, S. (2003). Congress 2003 intelligence debates and legislative developments. *Federation of American Scientists*. https://irp.fas.org/congress/2003_cr/s051503.html

2. Aidun, E. (2025, March 5). Data privacy in the digital age: A comparative analysis of U.S. and EU regulations. *University of Cincinnati Law Review, 93*. https://uclawreview.org/2025/03/05/data-privacy-in-the-digital-age-a-comparative-analysis-of-u-s-and-eu-regulations/

3. Ajibade, O. (2018). *A critical appraisal of big data analytics within the General Data Protection Regulation (GDPR) landscape* (ANR: U787189) [Master's dissertation, Tilburg University]. Tilburg University. https://arno.uvt.nl/show.cgi?fid=145693

4. Alcantara, C., Schaul, K., De Vynck, G., & Albergotti, R. (2023, September 26). Amazon, Apple, Facebook and Google became big tech companies by acquiring hundreds of smaller companies. *The Washington Post*. https://www.washingtonpost.com/technology/interactive/2021/amazon-apple-facebook-google-acquisitions/

5. Alemanno, A. (2025, November 12). The omnibus road to constitutional drift: How the rise of omnibus legislation undermines procedural integrity in the EU. *Verfassungsblog – On Matters Constitutional*. https://verfassungsblog.de/omnibus-legislation-europe-constitutional/

6. Alemanno, A. (2025). The legality of omnibus legislation under EU law: A preliminary analysis of Omnibus I Simplification Directive of CSRD and CSDD and its legal consequences on the EU legal order. *SSRN*. https://doi.org/10.2139/ssrn.5727822

7. Alexander, J. (2024, March 21). House passes bill banning data brokers from selling personal data to foreign adversaries. *The Verge*. https://www.theverge.com/2024/3/20/24106991/house-data-broker-foreign-adversaries-bill-passes

8. American Federation of Information Processing Societies & Time, Inc. (1971). *A national survey of the public's attitudes toward computers. American Federation of*

Information Processing Societies. https://openlibrary.org/works/OL43599453W/A_National_survey_of_the_public%27s_attitudes_toward_computers

9. Anderson, H., & Pittman, P. (2025, January 21). 2025 state privacy laws: What businesses need to know for compliance. *White & Case LLP*. https://www.whitecase.com/insight-alert/2025-state-privacy-laws-what-businesses-need-know-compliance

10. Andruss, R. (2022, June 27). A brief history of data privacy, and what lies ahead. *Skyflow*. https://www.skyflow.com/post/a-brief-history-of-data-privacy-and-what-lies-ahead

11. Angwin, J. (2025, April 30). Elon Musk's legacy: DOGE's construction of a surveillance state. *The New York Times*. https://www.nytimes.com/2025/04/30/opinion/elon-musk-doge-surveillance-state.html

12. Arcila, F. (2012). GPS tracking out of Fourth Amendment dead ends: United States v. Jones and the Katz conundrum. *North Carolina Law Review, 91*, 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2091176

13. Arkhipov, V., Golovatsky, R., & Bulgakov, I. (2023, August 30). Verkhovnyy sud RF ne priznal adres elektronnoi pocty personal'nymi dannymi [Russian Supreme Court refuses to recognise email addresses as personal data]. *Denuo Legal*. https://denuo.legal/ru/insights/news/230830/

14. Arrington, M. (2006, August 6). AOL proudly releases massive amounts of private data. *TechCrunch*. https://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/

15. Article 19. (2015, August). Rossia – Zakon o prave na zabvenie [Russia —Law on the right to be forgotten]. https://www.article19.org/data/files/medialibrary/38099/R2BF-Bill-Russia-RU.pdf

16. Austin, L. (2019). Re-reading Westin. *Theoretical Inquiries in Law, 20*(1), 53–81. https://doi.org/10.1515/til-2019-0003

17. Avdeev, A., & Troitskaia, I. (2025). Dorevizskiy uchot naseleniia v Rossii (XIII–XVII veka): istoriografiia, diskussiia o dostovernosti informatsii [Pre-census population accounting in Russia (13th–17th centuries): historiography, discussion on the

reliability of information]. *Demograficheskoe obozrenie, 12*(1), 4–33. https://doi.org/10.17323/demreview.v12i1.26573

18. Avdeev, M. (2016). Soderzhanie i sushchnost' prava na neprikosnovennost' chastnoy zhizni v Rossiyskoy Federatsii [Contents and essence of the right to inviolability of private life in the Russian Federation]. *Evraziyskaya advokatura: yuridicheskiy zhurnal, 4*(23). https://alrf.msk.ru/soderzhanie_i_suschnost_prava_na_neprikosnovennost_chastnoy_zhi

19. Ayrpayetian, G. (2025, July 26). Kak rabotat' s personal'nymi dannymi bez riska shtrafov [How to work with personal data without risk of fines]. *Zakon.ru*. https://www.zakon.ru/blog/2025/7/26/kak_rabotat_s_personalnymi_dannymi_bez_riska_shtrafov

20. Bachilo, I. L., & Volokitin, A. V. (1996). *Kommentarii k Federal'nomu zakonu "Ob informatsii, informatizatsii i zashchite informatsii"*.

21. Bainbridge, D. (1996). Using personal data after R v. Brown. *Information & Communications Technology Law, 5*(3), 247–251. https://doi.org/10.1080/13600834.1996.9965748

22. Bakare, S., Adeniyi, A., Akpuokwe, C., & Eneh, N. (2024). Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations. *Computer Science & IT Research Journal, 5*(3), 528–543. https://doi.org/10.51594/csitrj.v5i3.859

23. Baker, M. (1973). Record privacy as a marginal problem: The limits of consciousness and concern. In Staff of the *Columbia Human Rights Law Review* (Ed.), *Surveillance, dataveillance and personal freedoms* (pp. 100–111). R. E. Burdick.

24. Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology, 8*(2), 121–144. https://doi.org/10.1111/ips.12048

25. BBC News Russian. (2024, June 25). Epopeia Assandzha: ot WikiLeaks do dolgoy zhizni v posol'stve Ekvadora i do tyur'my "Belmarsh" [The Assange saga: from WikiLeaks to long life in the Ecuador embassy and to Belmarsh prison]. *BBC News Russian*. https://www.bbc.com/russian/articles/cd11x9872e2o

26. Beck, U., Leiss, W., Ritter, M., Lash, S., & Wynne, B. (1995). Risk society, towards a new modernity. *Canadian Journal of Sociology, 19*. https://doi.org/10.2307/3341155

27. Bennett, C. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States.* Cornell University Press. http://www.jstor.org/stable/10.7591/j.ctv2n7hxs

28. Bennett, C. (2008). *The Privacy Advocates: Resisting the spread of surveillance.* The MIT Press. https://doi.org/10.7551/mitpress/7855.001.0001

29. Bennett, C., & Raab, C. (2003). *The Governance of Privacy: Policy Instruments in Global Perspective*. Ashgate. https://doi.org/10.4324/9781315199269

30. Berzin, O., & Mitianov, Z. (2025). Institutions of Personal Data in Russia and Personal Information in China: a Comparative Legal Analysis. *Legal Issues in the Digital Age, 6*(3), 77–98. https://doi.org/10.17323/2713-2749.2025.3.77.98

31. Bhoumik, A. (2005). Democratic responses to terrorism: A comparative study of the United States, Israel, and India. *Denver Journal of International Law & Policy, 33*(2), 285–318. https://digitalcommons.du.edu/djilp/vol33/iss2/5/

32. Bincoletto, G. (2021). Data Protection by Design in the E-Health Care Sector: Theoretical and Applied Perspectives [Monograph]. *Baden-Baden: Nomos, Luxembourg Legal Studies, 22*. https://doi.org/10.5771/9783748929895

33. Biryukov, M. (2015). Aktualnye aspekty pravovoy zashchity personalnykh dannykh v Evropeyskom soyuze, SSHA i Rossii [Topical aspects of legal protection of personal data in the European Union, the USA and Russia]. *Moskovskiy Zhurnal Mezhdunarodnogo Prava*, (3), 197–208.

34. Black, E. (2002). Book Reviews: IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation. *Journal of Business and Technical Communication, 16*, 215 - 220.

35. Bogoraz, L. (1998). *Neprekosnovennost' chastnoi zhizni: Prava i obyazannosti grazhdan. Sbornik materialov seminara Moskovskoi Khelsinkskoi gruppy "Prava cheloveka"* [Privacy: Rights and duties of citizens. Collection of materials from the seminar of the Moscow Helsinki Group "Human Rights"]. Moskva: Moskovskaya Khelsinkskaya gruppa, 1–74.

https://www.mhg.ru/sites/default/files/inline/files/prava-grazhdan-seminary-bogoraz-1997.pdf

36. Boyne, S. (2018). Data Protection in the United States. *American Journal of Comparative Law, 66*(1), 299–343. https://doi.org/10.1093/ajcl/avy016

37. Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

38. Brady, R. (2007). *From court to country: A legal, social and political analysis of privacy in the U.S., 1965–1974* (Political Science Honors Project, Paper 4). Macalester College. https://digitalcommons.macalester.edu/poli_honors/4

39. Brenton, M. (1964). *The privacy invaders*. Coward-McCann.

40. Brin, D. (1964). *The naked society*. D. McKay Co. https://archive.org/details/nakedsociety00pack/page/n5/mode/2up

41. Brown, M. (1980, May 1). FTC temporarily closed in budget dispute. *The Washington Post*. https://www.washingtonpost.com/archive/business/1980/05/01/ftc-temporarily-closed-in-budget-dispute/5c63ef5d-4e28-471d-8f9c-014d4d28d360/

42. Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies, 21*(5), 594–613. https://doi.org/10.1177/1367549417751151

43. Buitelaar, J. (2012). Privacy: Back to the Roots. *German Law Journal, 13*(3), 171–202. https://germanlawjournal.com/wp-content/uploads/GLJ_Vol_13_No_03_Buitelaar.pdf

44. Burgess, M. (2017, January 27). Trump's new order could wreck US-EU Privacy Shield. *WIRED*. https://www.wired.com/story/trump-privacy-shield-data/

45. Burton, C., Padova, Y., De Boel, L., Theodorakis, N., Evans, T., & Kosno, O. (2026, January 8). 2026 year in preview: European digital regulatory developments for companies to watch out for. *Wilson Sonsini Goodrich & Rosati*. https://www.wsgr.com/en/insights/2026-year-in-preview-european-digital-regulatory-developments-for-companies-to-watch-out-for.html

46. Bychkov, A. (2021). Kakie dannye yavlyayutsya personal'nymi: pozitsiya suda [Which Data Are Personal: Court Position]. *Zhurnal Kadrovaya sluzhba i upravlenie personalom predpriyatiya, 5*.

https://delo-press.ru/journals/staff/pravovoe-obespechenie-deyatelnosti/58624-kakie-dannye-yavlyayutsya-personalnymi-pozitsiya-suda/

47. Bygrave, L. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press. https://dokumen.pub/data-privacy-law-an-international-perspective-9780199675555.html

48. Bystrova, E. (2025, October 16). Lish' 3% rossiian bol'she ne reagiruiut na utechki personal'nykh dannykh [Only 3% of Russians no longer react to personal data breaches]. *Anti-Malware.ru*. https://www.anti-malware.ru/news/2025-10-16-111332/47730

49. Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

50. California Department of Justice, Office of the Attorney General. (n.d.). *Privacy legislation enacted in 2015*. Retrieved January 12, 2026, from https://oag.ca.gov/privacy/privacy-legislation/leg2015

51. California Privacy Protection Agency. (2024). *California Privacy Protection Agency announces 2025 increases for CCPA fines and penalties.* Retrieved January 10, 2026, from https://cppa.ca.gov/announcements/2024/20241217.html

52. California Privacy Protection Agency. (n.d.). *Updated monetary thresholds in the California Consumer Privacy Act (CCPA), Civil Code § 1798.199.95(d)*. Retrieved January 11, 2026, from https://cppa.ca.gov/regulations/cpi_adjustment.html

53. Capital Health. (2026). *Office policies – Primary Care Quakerbridge*. https://www.capitalhealth.org/our-locations/primary-care-quakerbridge/office-policies

54. Capital Health. (2026). *Primary Care Quakerbridge office policies.* Retrieved October 3, 2025, from https://www.capitalhealth.org/our-locations/primary-care-quakerbridge/office-policies

55. Carroll, J., Eisman, D., Freed, T., & Gerber, M. (2022). Privacy & cybersecurity update. *Skadden*. https://www.skadden.com/insights/publications/2022/06/privacy-cybersecurity-update

56. Castro, D., Dascoli, L., & Diebold, G. (2022, January 24). The looming cost of a patchwork of state privacy laws. *Information Technology and Innovation Foundation (ITIF)*. https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/

57. Cejas, O., Sannier, N., Abualhaija, S., Ceci, M., & Bianculli, D. (2024). GDPR-relevant privacy concerns in mobile apps research: A systematic literature review. *Cornell University, arXiv*. https://doi.org/10.48550/arXiv.2411.19142

58. Chander, A., & Sun, H. (Eds.). (2023). *Data sovereignty: From the Digital Silk Road to the return of the state*. Oxford University Press. https://doi.org/10.1093/oso/9780197582794.001.0001

59. Charfoos, A., Cooney, J., Coogan, D., & Powers, B. (2022, October 5). New comprehensive US state privacy laws are coming – Is your company ready? *Paul Hastings LLP Insights*. https://www.paulhastings.com/insights/client-alerts/new-comprehensive-us-state-privacy-laws-are-coming-is-your-company-ready

60. Chaum, D. (1983). Blind signatures for untraceable payments. In D. Chaum, R. Rivest, & A. Sherman (Eds.), *Advances in Cryptology* (pp. 199–203). Springer. https://doi.org/10.1007/978-1-4757-0602-4_18

61. Chaum, D. (1985). Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM, 28*(10), 1030–1044. https://doi.org/10.1145/4372

62. Chaum, D., Fiat, A., & Naor, M. (1990). Untraceable electronic cash. In S. Goldwasser (Ed.), *Advances in Cryptology — CRYPTO'88* (Vol. 403, pp. 319–327). Springer. https://doi.org/10.1007/0-387-34799-2_25

63. Chekharina, V. (2020). O konstitutsionalizatsii prava na zaschitu personal'nykh dannykh: Iz zarubezhnogo opyta [On the constitutionalization of the right to protection of personal data: From foreign experience]. *Mezhdunarodnyy zhurnal gumanitarnykh i yestestvennykh nauk, (3-2),* 223–228. https://cyberleninka.ru/article/n/o-konstitutsionalizatsii-prava-na-zaschitu-personalnyh-dannyh-iz-zarubezhnogo-opyta

64. Chernyshova, E. (2022, February 10). Zachem vlasti sozdayut "suverennyi Runet": Ot chego on zashchitit i chem grozit [Why authorities are creating a "sovereign

Runet": What it will protect against and what risks it poses]. *RBC Trendy*.https://trends.rbc.ru/trends/industry/609a52329a79471fba0f0837

65. Cifaldi, G. (2023). Evolution of concepts of privacy and personal data protection under the influence of information technology development. *Sociology and Social Work Review, 7*(1), 35–60. https://doi.org/10.58179/SSWR7103

66. Clarip. (2026). *History of data privacy in the United States*. Retrieved July 12, 2025, from https://www.clarip.com/data-privacy/us-history/

67. Clifford Chance. (2025, January). *Data Privacy Legal Trends 2025*. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/02/data-privacy-legal-trends-2025.pdf

68. CNIL. (n.d.). *CNIL publishes its European and international strategy for 2025-2028*. Retrieved August 7, 2025, from https://www.cnil.fr/en/cnil-publishes-its-european-and-international-strategy-2025-2028

69. Cohen, J. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press. https://juliecohen.com/configuring-the-networked-self/

70. Cohen, J. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press. https://academic.oup.com/book/37371

71. Cohn, C., & Jeschke, R. (2011, October 3). California's Reader Privacy Act signed into law [Press release]. Electronic Frontier Foundation. https://www.eff.org/press/archives/2011/10/03/californias-reader-privacy-act-signed-law

72. Collins, K., & Buchanan, L. (2018, April 11). How Facebook lets brands and politicians target you. *The New York Times*. https://www.nytimes.com/interactive/2018/04/11/technology/facebook-sells-ads-life-details.html

73. Confessore, N. (2018, March 17). Cambridge Analytica and Facebook: The scandal and the fallout so far. *The New York Times*. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

74. Conolly-Smith, P. (2009). "Reading between the lines": The Bureau of Investigation, the United States Post Office, and domestic surveillance during World War I. *Social Justice, 36*(1(115)), 7–24. http://www.jstor.org/stable/29768523

75. Conyers, J. (2003). The USA PATRIOT Act and the expansion of government surveillance powers. *Harvard Journal of Law & Public Policy, 26*(2), 345–370.

76. Cook, F. (1964). *The FBI nobody knows*. The Macmillan Company. https://archive.org/details/fbinobodyknows0000fred_j5i8

77. Cooley, T. (1888). *A treatise on the law of torts, or, the wrongs which arise independent of contract* (2nd ed.). Callaghan & Company.

78. Coppel, P. (Ed.). (2023). *Information rights: A practitioner's guide to data protection, freedom of information & other information rights*. London: Bloomsbury Publishing. https://doi.org/10.5040/9781509967339

79. Covington & Burling. (1974). *Legislative history of the Privacy Act of 1974: P.L. 93-579: 88 Stat. 1896: Dec. 31, 1974* (4 vols.). Washington, D.C.: Covington & Burling. https://lawcat.berkeley.edu/record/360881

80. Craig, P., & de Búrca, G. (2021). *The Evolution of EU Law* (3rd ed.). Oxford University Press. https://academic.oup.com/book/39246

81. Culnan, M. J. (2019). Data breaches and the responsibilities of large firms: Lessons from the Equifax case. *Journal of Information Privacy and Security, 15*(2), 65–78. https://doi.org/10.1080/15536548.2019.1623421

82. Data Privacy Office. (2023, October 12). *Data Privacy Framework — stali li SSHA "adekvatnoy" yurisdiktsiey?* [Has the USA become an "adequate" jurisdiction?]. https://data-privacy-office.com/data-privacy-framework/

83. De Hert, P. (2004). *Privacy and data protection concepts in Europe. Computers, Freedom & Privacy 2004* [Conference presentation]. Berkeley. https://cfp2004.org/program/materials/c14-deHert.pdf

84. De Hert, P., & Gutwirth, S. (2009). Data protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action. In S. Gutwirth, Y. Poullet, P. De Hert, J. Nouwt, & C. De Terwangne (Eds.), *Reinventing Data Protection?* (3–45). Springer. https://doi.org/10.1007/978-1-4020-9498-9_1

85. De Hert, P., & Papakonstantinou, V. (2013). Three scenarios for international governance of data privacy: Towards an international data privacy organization,

preferably a UN agency? *I/S: A Journal of Law and Policy for the Information Society, 9*(2), 271–324. https://www.semanticscholar.org/paper/Three-scenarios-for-international-governance-of-%3A-a-Hert-Papakonstantinou/bcf030dc2b671059cb29b152dbe4673d832e315c

86. DeepStrike. (n.d.). *Healthcare data breaches 2025 statistics: $10.22M cost*. Retrieved January 30, 2026, from https://deepstrike.io/blog/healthcare-data-breaches-2025-statistics

87. Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. L. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. MIT Press. https://watermark02.silverchair.com/book_9780262266031.pdf

88. Deloitte Belgium. (n.d.). *Deloitte's view on the implementation of Regulation (EU) 2018/1725 ("GDPR for European Union Institutions")*. Retrieved November 13, 2025, from https://www.deloitte.com/be/en/services/risk-advisory/research/gdpr-for-eu-institutions.html

89. Denisenko, A. (2025, August 25). Kiberpolitsiya v Rossii zakryla nelegal'nyy sait ili servis [Cyber-police in Russia shut down an illegal site or service]. *CNews.ru*. https://www.cnews.ru/news/top/2025-08-25_kiberpolitsiya_v_rossii_zakryla

90. Denisenko, A. (2025, January 10). Pravitel'stvo Evrosoiuza vpervye v istorii oshtrafovano za nesobliudenie sobstvennykh pravil zashchity dannykh [European Commission fined for the first time in history for breaching its own data protection rules]. *CNews.ru*. https://www.cnews.ru/news/top/2025-01-10_vpervye_vysshij_organ_ispolnitelnoj

91. Denisenko, A. (2025, May 15). V SShA hotyat povtorno prinyat' radikal'nyy zakon o zashchite detey v Internete [In the USA they seek to re-adopt a radical internet child protection law]. *CNews.ru*. https://www.cnews.ru/news/top/2025-05-15_v_ssha_hotyat_povtorno_prinyat

92. Denisenko, A. (2025, November 1). Kiberpolitsiya v Moskve zaderzhala vladel'tsa populiarnoho Telegram-bota dlia probiva lichnykh dannykh [Cyber-police in Moscow arrested the owner of a popular Telegram bot for probing personal data]. *CNews.ru*. https://www.cnews.ru/news/top/2025-11-01_kiberpolitsiya_v_moskve_zaderzhala

93. Dewitte, P. (2023). A brief history of data protection by design: From multilateral security to Article 25(1) GDPR. *Technology and Regulation*, 80–94. https://doi.org/10.26116/techreg.2023.008

94. Dimitrova, D., & De Hert, P. (2024). DPA independence and "indirect" access — illusory in Belgium, France and Germany? *Maastricht Journal of European and Comparative Law, 31*(1), 82–105. https://doi.org/10.1177/1023263X241237688

95. Ding, X., Huang, H., Shi, Z., & Wang, Y. (2025). Same text, different meaning: China's risk-based approach to data protection. *Humanities and Social Sciences Communications, 12(1821)*. https://www.nature.com/articles/s41599-025-06100-3

96. Dixon, H. (2025). GDPR is not loved, but does it work? *International Data Privacy Law*, 15(2), 101–107. https://doi.org/10.1093/idpl/ipaf019

97. Domshenko, V., & Sabirov, A. (2025, April 25). Empiricheskiy analiz sudebnoy praktiki ob utechkakh personal'nykh dannykh [Empirical Analysis of Judicial Practice on Personal Data Leaks]. Pravo.ru. https://pravo.ru/opinion/258425/

98. Dozhdev, D. V. (2008). *Rimskoe chastnoe pravo* [Roman private law]. Norma.

99. Dumiak, M. (2022, June 24). Federal privacy bill: Breaking down the ADPPA. *CompliancePoint*. https://www.compliancepoint.com/privacy/federal-privacy-bill-adppa/

100. Dunlap, L., Cummings, J., and Janicki, T. (2017). Information security and privacy legislation: Current state and future direction. Austin, TX: Information Systems & Computing Academic Professionals (ISCAP). *Proceedings of the Conference on Information Systems Applied Research, 10.* https://iscap.us/proceedings/conisar/2017/pdf/4506.pdf

101. Duportail, J. (2017, September 26). I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets. *The Guardian*. https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold

102. Edwards, L. (2018). *Data Protection: Enter the General Data Protection Regulation* (forthcoming in L. Edwards (Ed.), *Law, Policy and the Internet* (Hart Publishing, 2018). http://dx.doi.org/10.2139/ssrn.3182454

103. Ehrenfreund, M. (2013, June 10). *Edward Snowden says he leaked NSA surveillance program. The Washington Post.*

https://www.washingtonpost.com/world/national-security/edward-snowden-says-he-leaked-nsa-surveillance-program-complete-coverage/2013/06/10/1a6d525e-d1da-11e2-a73e-826d299ff459_story.html

104. Ehrenfreund, M. (2013, June 10). Edward Snowden says he leaked NSA surveillance program. *The Washington Post*. https://www.washingtonpost.com/world/national-security/edward-snowden-says-he-leaked-nsa-surveillance-program-complete-coverage/2013/06/10/1a6d525e-d1da-11e2-a73e-826d299ff459_story.html

105. Electronic Privacy Information Center. (n.d.). *U.S. privacy laws.* Retrieved October 23, 2025, from https://epic.org/issues/privacy-laws/united-states/

106. Equifax Inc. (2017, September 7). *Equifax announces cybersecurity incident involving consumer information* [Press release]. https://investor.equifax.com/news-events/press-releases/detail/240/equifax-announces-cybersecurity-incident-involving-consumer

107. Esguerra, R. (2007, December 11). Facebook Beacon roundup: Data collection methods still troubling. *Electronic Frontier Foundation Deeplinks Blog*. https://www.eff.org/deeplinks/2007/12/facebook-beacon-roundup

108. Eskens S. (2020). The personal information sphere: An integral approach to privacy and related information and communication rights. *Journal of the Association for Information Science and Technology, 71*(9), 1116–1128. https://doi.org/10.1002/asi.24354

109. Eskens, S., Timmer, J., Kool, L., and Van Est, R. (2016). Beyond control: Exploratory study on the discourse in Silicon Valley about consumer privacy in the Internet of Things. *Rathenau Instituut*. https://www.saraheskens.eu/publications/Eskens-ea-2016-iot.pdf

110. EuroCloud Europe. (2018, June 1). *A brief history of data protection: How did it all start?* https://eurocloud.org/news/article/a-brief-history-of-data-protection-how-did-it-all-start/

111. European Commission. (2011). *Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union*. Directorate-General for Communication. https://data.europa.eu/data/datasets/s1061_74_1_ebs359

112. European Commission. (2012, January 25). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

113. European Commission. (2013, January 28). *European Data Protection Day 2013: Full speed ahead towards reliable and modern EU data protection laws* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_13_57

114. European Commission. (2013, March 15). Data protection reform: Restoring trust and building the digital single market [Press release IP/13/57]. http://europa.eu/rapid/press-release_SPEECH-13-720_en.pdf

115. European Commission. (2021). *June infringement package: key decisions* [Press Corner]. https://ec.europa.eu/commission/presscorner/detail/en/inf_21_2743

116. European Commission. (n.d.). *Adequacy decisions: How the EU determines if a non-EU country offers an adequate level of data protection*. Retrieved November 23, 2025, from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

117. European Commission. (n.d.). *Data*. Retrieved December 13, 2025, from https://digital-strategy.ec.europa.eu/en/factpages/data

118. European Commission. (n.d.). *EU-US data transfers – how personal data transferred between the EU and the US is protected*. Retrieved October 15, 2025, from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_ga

119. European Court of Human Rights. (2024, February). *Factsheet – Personal data protection*. Council of Europe. https://www.echr.coe.int/documents/fs_data_eng.pdf

120. European Data Protection Supervisor (n.d.). *European Data Protection Supervisor – EU institution*. Retrieved October 14, 2025, from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-supervisor-edps_en

121. European Data Protection Supervisor. (n.d.). *About the European Data Protection Supervisor (EDPS)*. Retrieved January 30, 2026, from https://www.edps.europa.eu/about-edps_en

122. European Parliament & Council. (2025, June 16). *Data protection: Agreement on clarifying cross-border enforcement* [Press release 20250521IPR28537]. https://www.europarl.europa.eu/news/en/press-room/20250521IPR28537/data-protection-agreement-on-clarifying-cross-border-enforcement

123. European Parliamentary Research Service. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. EPRS Study PE 641.530. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

124. European Union Agency for Fundamental Rights, Council of Europe & European Data Protection Supervisor. (2018). *Handbook on European data protection law*.https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

125. Fair, L. (2019, July 24). $5 billion penalty and sweeping new privacy restrictions for Facebook. *Federal Trade Commission*. https://www.ftc.gov/business-guidance/blog/2019/07/5-billion-penalty-and-sweeping-new-privacy-restrictions-facebook

126. Fazlioglu, M. (2023, March 16). *US state privacy laws overview.* International Association of Privacy Professionals (IAPP). https://www.iapp.org/resources/article/us-state-privacy-laws-overview/

127. Federal Trade Commission. (2019, July 24). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

128. Federal Trade Commission. (n.d.). *How to comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*. Retrieved December 30, 2026, from https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

129. Feiner, L. (2024, March 20). House passes bill banning data brokers from selling personal data to foreign adversaries. *The Verge*. https://www.theverge.com/2024/3/20/24106991/house-data-broker-foreign-adversaries-bill-passes

130. Filonova, A. (2022). [Theoretical and historical aspects of information protection in the Russian Federation]. *Vestnik NIB*, (45). https://cyberleninka.ru/article/n/teoreticheskie-i-istoricheskie-aspekty-zaschity-informatsii-v-rossiyskoy-federatsii

131. Finck, M., & Pallas, F. (2020). They who must not be identified — distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11–36. https://doi.org/10.1093/idpl/ipz026

132. Fogelson, Yu. (2020). Rossiyskoe grazhdanskoe pravo s tochki zreniia sotsiologicheskoy iurisprudentsii (standarty dokazyvaniia, vozmeshchenie vreda zhizni ili zdorov'iu) [Russian civil law from the perspective of sociological jurisprudence (standards of proof, compensation for harm to life or health)]. *Zhurnal Zakon [Law Journal]*, (1). https://zakon.ru/publication/igzakon/8110

133. Fox, J. (2025, December 15). Top cybersecurity statistics for 2026. *Cobalt*. https://www.cobalt.io/blog/top-cybersecurity-statistics-for-2026

134. Froomkin, A. (1969). The death of privacy. *Stanford Law Review, 52*(6), 1462–1543. https://cyber.harvard.edu/privacy/Fromkin_DeathOfPrivacy.pdf

135. Fulton, M., & Witherspoon, M. (2025, October 1). Maryland Online Data Privacy Act now in effect. *Koley Jessen Insights*. https://www.koleyjessen.com/insights/publications/maryland-online-data-privacy-act

136. Gambino, L. (2025, October 1). US government shuts down after Senate fails to advance both parties' bills. *The Guardian*. https://www.theguardian.com/us-news/2025/oct/01/us-government-shuts-down

137. Gao, R. (2025). Forum shifting to regulate data privacy: The creation and evolution of EU data protection law. *Northwestern Journal of International Law & Business, 45*(3), 329-418. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1922&context=njilb

138. Gareis, C. (1877). The juridical nature of author's rights, as well as of tradename and trademark protection. *Primary Sources on Copyright (1450–1900)*. https://www.copyrighthistory.org/cam/tools/request/showRecord.php?id=record_d_1877

139. Garfinkel, S. (2004). *Vse pod kontrolem: Kto i kak sledit za toboi* [Everything Under Control: Who and How They Watch You]. Yekaterinburg: U-Faktoriia. https://royallib.com/book/garfinkel_simeon/vse_pod_kontrolem_kto_i_kak_sledit_za_toboy.html

140. Garnett, S. (2014, December 23). Privacy politics today. *Eurozine*. https://www.eurozine.com/privacy-politics-today/

141. GDPR Buzz. (2021, July 7). *Commission opens an infringement procedure against Belgium on the independence of its Data Protection Authority*. Retrieved January 9, 2026, from https://gdprbuzz.com/news/commission-opens-an-infringement-procedure-against-belgium-on-the-independence-of-its-data-protection-authority/

142. Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law & Security Review, 29*(5), 522–530. https://doi.org/10.1016/j.clsr.2013.07.005

143. Gellman, B., & Poitras, L. (2013, June 6). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

144. Gellman, R. (2014). Fair Information Practices: A basic history. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2415020

145. Giblin, A., & Medeiros, S. (2025, November 5). California tightens data breach notification timelines, imposes 30-day notice requirement. *Data Protection Report*. https://www.dataprotectionreport.com/2025/11/california-tightens-data-breach-notification-timelines-imposes-30-day-notice-requirement/

146. Gibson, Dunn & Crutcher LLP. (2021, November 11). *UK Supreme Court overturns Court of Appeal to disallow Google data privacy class action* (Client Alert). https://www.gibsondunn.com/uk-supreme-court-overturns-court-of-appeal-to-disallow-google-data-privacy-class-action/?pdf=display

147. Global Fact-Checking Network. (2025, April 18). *Smile-to-pay service in Russia — fake or real?* Retrieved September 13, 2025, from https://globalfactchecking.com/smile-to-pay-service-in-russia-fake-or-real/

148. González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham: Springer International Publishing. Law, Governance and Technology Series, Band XVI. https://doi.org/10.1007/978-3-319-05023-2

149. Gonzalez-Riedel, D., & Idema, S. (2024, September). Understanding the intersection between the EU's AI Act and privacy compliance. *Compact*. https://www.compact.nl/articles/understanding-intersection-between-eus-ai-act-and-privacy-compliance/

150. González, G., Van Brakel, R., & De Hert, P. (Eds.). (2022). *Research Handbook on Privacy and Data Protection Law*. Cheltenham, UK: Edward Elgar Publishing. https://doi.org/10.4337/9781786438515

151. Gordan, J. III (2006). *Judicial Notice*. White Plains, NY: Historical Society of the New York Courts, Issue 4. https://history.nycourts.gov/wp-content/uploads/2019/12/Judicial-Notice-04.pdf

152. Gorokhova, D. (2013). Konventsiia Soveta Evropy o zashchite fizicheskikh lits pri avtomatizirovannoi obrabotke personal'nykh dannykh [Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data]. *Vestnik Evraziiskogo gosudarstvennogo universiteta im. P. G. Demidova. Yuridicheskie nauki, 1*(17). https://doi.org/10.7256/2073-8560.2013.01.17

153. Graux, H., Garstka, K., Murali, N., Cave, J., & Botterman, M. (2025). Interplay between the AI Act and the EU digital legislative framework. *Brussels: European Parliament Think Tank. Policy Department for Transformation, Innovation and Health*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/778577/ECTI_ATA(2025)778577_EN.pdf

154. Greenberg, J. (2015, August 21). Ashley Madison hack exposes (wait for it) a lousy business. *Wired*. https://www.wired.com/2015/08/ashley-madison-hack-exposes-wait-lousy-business/

155. Greenwald, G., & MacAskill, E. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

156. Griffin, T. (n.d.). Security or data breach. *Arkansas Attorney General*. Retrieved September 12, 2025, from https://arkansasag.gov/divisions/public-protection/identity/security-or-data-breach/

157. Grossman, N. (2025, December 15). What to expect in 2026 for GDPR and data protection. *VinciWorks*. https://vinciworks.com/blog/what-to-expect-in-2026-for-gdpr-and-data-protection/

158. Gubenko, S. (2022). Tracing the expansive effect of the GDPR in the third countries: The cases of Russia, Ukraine and China. *Peace Human Rights Governance, 6*(06/2022), 79–96. https://doi.org/10.14658/pupj-phrg-2022-1-4

159. Gude, S. V., Arbuzov, P. V., & Karpika, A. G. (2015). Zashchita personal'nykh dannykh v Rossiiskoi Federatsii: istoricheskii aspekt i sovremennoe sostoianie [Personal data protection in the Russian Federation: Historical aspect and current state]. *Iuridicheskaia praktika*, (2(69)). https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-rossiyskoy-federatsii-istoricheskiy-aspekt-i-sovremennoe-sostoyanie

160. Gutwirth, S. (2002). Privacy in the information age. Rowman & Littlefield. *Persona Y Derecho*, *46*, 457-462.https://doi.org/10.15581/011.32089

161. Guynn, J. (2020, July 3). Facebook's troubles persist as #DeleteFacebook fizzles. *USA Today*. https://www.usatoday.com/story/tech/2020/07/03/facebook-privacy-issues-deletefacebook/5376044002/

162. Guzman, Z. (2015, July 9). US Office of Personnel Mgmt: Info on 21.5M people stolen. *CNBC*. https://www.cnbc.com/2015/07/09/us-office-of-personnel-mgmt-info-on-215m-people-stolen.html

163. Haie, A.-G. (2025, November 25). The European Commission published its proposed reform of the EU data protection, privacy, data, cyber incident reporting and AI framework. *StepTechToe Blog (Steptoe & Johnson LLP)*.https://www.steptoe.com/en/news-publications/steptechtoe-blog/the-european-commission-published-its-proposed-reform-of-the-eu-data-protection-privacy-data-cyber-incident-reporting-and-ai-framework.html

164. Harmeling, T. (2025, March 25). US state privacy laws overview. Global data privacy laws: Your 2025 guide. *Usercentrics*. https://usercentrics.com/guides/data-privacy/data-privacy-laws/

165. Harrington, D. (2025, June 23). U.S. privacy laws: The complete guide. *Varonis*. https://www.varonis.com/blog/us-privacy-laws

166. Haselton, T. (2017, September 7). Credit reporting firm Equifax says cybersecurity incident could potentially affect 143 million US consumers. *CNBC*. https://www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html

167. He, X., & Fay, R. (2023). Digital governance in China: Data, AI and emerging technologies, and digital trade [Conference Report – Virtual Workshop, November 28, 2022]. *Centre for International Governance Innovation (CIGI)*.https://www.cigionline.org/static/documents/2022_Workshop_Digital_Governance_in_China_NfVKbz9.pdf

168. Heinzke, P., Herbers, B., & Dreyer, J. (2023, February). The Data Governance Act – overview. *CMS Law-Now*. https://cms-lawnow.com/en/ealerts/2023/02/the-data-governance-act-overview

169. Herbers, B., Rappenglück, D., & Petrányi, D. (2025, November 20). The EU's Digital Omnibus: Simplification, consolidation and a sharper edge on compliance. *CMS Law-Now*. https://cms-lawnow.com/en/ealerts/2025/11/the-eu-s-digital-omnibus-simplification-consolidation-and-a-sharper-edge-on-compliance

170. Hijmans, H. (2016). *The European Union as a constitutional guardian of internet privacy and data protection* [Doctoral dissertation, University of Amsterdam]. University of Amsterdam Digital Academic Repository. https://hdl.handle.net/11245/1.511969

171. Horowitz, H. (2006). Coda: The Comstock Law of 1873. In *Attitudes toward Sex in Antebellum America* (pp. 157–159). Palgrave Macmillan. https://doi.org/10.1007/978-1-137-05413-5_4

172. Hughes, T. (2023, February 8). A short history of privacy in the US State of the Union addresses. *International Association of Privacy Professionals (IAPP)*. https://iapp.org/news/a/a-short-history-of-privacy-in-u-s-state-of-the-union-addresses/

173. Igo, S. (2015). The beginnings of the end of privacy. *The Hedgehog Review, 17*(1). https://hedgehogreview.com/issues/too-much-information/articles/the-beginnings-of-the-end-of-privacy

174. Ilinykh, N. (2022). Podkhody k opredeleniiu prava na neprikosnovennost' chastnoi zhizni v otechestvennom i zarubezhnom prave [Approaches to defining the right to privacy in domestic and foreign law]. *Tezisy doklada na konferentsii, Sibirskii iuridicheskii institut MVD Rossii*, pp. 101–104. https://elibrary.ru/item.asp?id=7644997https://doi.org/10.51980/978-5-7889-0327-9_2022_23_13_101

175. IncFine. (2025, April 23). Zakony SShA o konfidentsial'nosti dannykh [U.S. data privacy laws]. *IncFine*. https://incfine.com/zakony-ssha-o-konfidencialnosti-dannyh/

176. Information Technology and Innovation Foundation. (2022, January 24). 50-state patchwork of privacy laws could cost $1 trillion more than a single federal law, new ITIF report finds. *ITIF*. https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal/

177. Irwin, L. (2022, June 7). EDPB publishes new guidance on GDPR fines. *IT Governance Blog*. https://www.itgovernance.eu/blog/en/edpb-publishes-new-guidance-on-gdpr-fines

178. IT Governance. (2022, May 12). EDPB publishes new guidance on GDPR fines. *IT Governance Blog*. https://www.itgovernance.eu/blog/en/edpb-publishes-new-guidance-on-gdpr-fines

179. IT-World.ru. (2025, October 16). *Rossiyane vse chashche zabotyatsya o svoikh personal'nykh dannykh* [Russians increasingly care about their personal data]. https://www.it-world.ru/security/g0i0at3vpwgkskw8c4ocscco8sk4kkw.html

180. Ivanskii, V. P. (1998). Problemy garmonizatsii natsional'nykh zakonov v sfere zashchity transgranichnykh personal'nykh dannykh [Problems of harmonization of national laws in the field of protection of cross-border personal data]. *Vestnik RUDN*, (1).

181. Ivanskii, V. P., & Mel'nichuk, G. V. (2017). Gosudarstvennyi kontrol' (nadzor) — instrument protivodeistviia ugrozam natsional'noi bezopasnosti v informatsionnoi sfere ili sredstvo zashchity neprikosnovennosti chastnoi zhizni: sootnoshenie chastnogo i publichnogo interesov [State control (supervision) as an instrument of countering threats to national security in the information sphere or a means of protecting the inviolability of private life: Correlation between private and public interests]. *Vestnik Rossiiskogo universiteta druzhby narodov. Seriia: Iuridicheskie nauki (RUDN Journal of Law)*, 21(1), 136–152. https://doi.org/10.22363/2313-2337-2017-21-1-136-152

182. Izmailova, N. (2008). Neprikosnovennost' chastnoy zhizni v anglo-amerikanskoy i rossiyskoy pravovykh doktrinakh [The inviolability of private life in Anglo-American and Russian legal doctrines]. *Moskovskiy zhurnal mezhdunarodnogo prava*, (1), 172–185. https://doi.org/10.24833/0869-0049-2008-1-172-185

183. Javed, Y., & Sajid, A. (2024). A systematic review of privacy policy literature. *ACM Computing Surveys, 57*(2), 1–43. https://dl.acm.org/doi/10.1145/3698393

184. Jesdanun, A. (2006, September 26). Subscribers sue AOL over data release. *NBC News*. Retrieved July 12, 2025, from https://www.nbcnews.com/id/wbna15004643

185. Johnson, G. (2022). Economic research on privacy regulation: Lessons from the GDPR and beyond (NBER Working Paper No. 30705). *National Bureau of Economic Research*. https://doi.org/10.3386/w30705

186. Jones, M., & Kaminski, M. (2020). An American's Guide to the GDPR. U. of Colorado Law Legal Studies Research Paper No. 20-33. *Denver Law Review, 98*(1), 93 (2021). https://ssrn.com/abstract=3620198

187. Kalyanpur, N., & Newman, A. L. (2019). The MNC-Coalition Paradox: Issue salience, foreign firms and the General Data Protection Regulation. *Journal of Common Market Studies, 57*(3), 448–467. https://doi.org/10.1111/jcms.12810

188. Kaminski, M., & Malgieri, G. (2019). Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations. *International Data Privacy Law.* University of Colorado Law Legal Studies Research Paper No. 19-28. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456224

189. Kamitdinov, N. (2021, June 17). Za "Glazom Boga": kto sozdal glavnyi v Rossii servis dlya poiska personal'nykh dannykh i pochemu ego ne zakryvaiut [Behind "Eye of

God": who created Russia's main service for searching personal data and why it isn't shut down]. *Forbes.ru.* https://www.forbes.ru/karera-i-svoy-biznes/432271-za-glaz-boga-kto-sozdal-glavnyy-v-rossii-servis-dlya-poiska-personalnykh-dannykh

190. Kelman, A. (2000). Database Nation: The Death of Privacy in the 21st Century (Book Review). *Journal of Information, Law and Technology (JILT), 2000*(1). https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_1/kelman/

191. Khalil, M. (2025, August 5). Healthcare data breaches 2025: Stats, costs & real-world risks. *DeepStrike.* https://deepstrike.io/blog/healthcare-data-breaches-2025-statistics

192. Klishas, A. (2021, February 12). Zachem nuzhen zakon ob ustoichivosti Runeta [Why the law on the sovereign Runet is needed]. *Parlamentskaia gazeta*. https://www.pnp.ru/politics/zachem-nuzhen-zakon-ob-ustoychivosti-runeta.html

193. Kohl, U. (2023). The right to be forgotten in data protection law and two Western cultures of privacy. *International and Comparative Law Quarterly, 72*(3), 737–769. https://doi.org/10.1017/S0020589323000258

194. Kohler, J. (1906). Urheberrecht an Schriftwerken und Verlagsrecht [Copyright in Literary Works and Publishing Law]. *Stuttgart: F. Enke, 12*. https://archive.org/details/UrheberrechtAnSchriftwerkenUndVerlag

195. Kondratieva, I. (2020, September 2). Verkhovnyy sud nauchil rassmatrivat' iski o zashchite personal'nykh dannykh [The Supreme Court taught how to consider claims for the protection of personal data]. *Pravo.ru*.https://pravo.ru/story/224425/

196. Koops, B.-J., & Sluijs, J. (2012). Network neutrality and privacy according to Art. 8 ECHR. *European Journal of Law and Technology, 3*(2). https://ejlt.org/index.php/ejlt/article/view/90

197. Korevo, N. (1897). *Ob izdaniiakh zakonov; Kratkii obzor Svoda zakonov Rossiiskoi imperii i pravila dlia upotrebleniia ego na praktike* [On the publication of laws; Brief review of the Digest of Laws of the Russian Empire and rules for its practical use] (A. I. Pakharnayev, Comp.). Saint Petersburg.

198. Kornstein, D. (2006). *The Roberson privacy controversy*. The Historical Society of the Courts of the State of New York. https://history.nycourts.gov/publications/roberson-privacy-controversy/

199. Korzhov, V. (2011, September 1). Istoriia FZ No. 152 "O zashchite personal'nykh dannykh" [History of Federal Law No. 152 "On Personal Data Protection"]. *Anti-Malware.ru*. https://www.anti-malware.ru/analytics/Technology_Analysis/History-of-the-Federal-Law-152

200. Kostunov, I. (2025, July 17). "Glaz Boga": kak odin Telegram-bot stal simvolom tsifrovogo shpionazha i slezhki v Rossii ["Eye of God": how one Telegram bot became a symbol of digital espionage and surveillance in Russia]. *Ruposters.ru*. https://ruposters.ru/news/17-07-2025/glaz-boga

201. Kowalski, B. (Director). (1966). *The Intruders* [Television movie]. Qualis Productions; 20th Century Fox Television.https://www.imdb.com/title/tt0650744/

202. Kramer, J., & Hoar, S. (2017). GDPR, Part I: History of European Data Protection Law. *Lewis Brisbois Data Privacy & Cybersecurity Insights*. https://files.lewisbrisbois.com/production/general/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf

203. Kranenborg, H. (2016). Review of O. Lynskey, The Foundations of EU Data Protection Law. *International Data Privacy Law, 6*(4), 324–326. https://doi.org/10.1093/idpl/ipw017

204. Kukushkin, Iu., & Chistiakov, O. (1980). *Ocherk istorii Sovetskoi Konstitutsii* [Essay on the history of the Soviet Constitution]. Izdatel'stvo politicheskoi literatury.

205. Kuner, C. (2007). *European data protection law : corporate compliance and regulation* (2nd ed.). Oxford University Press.

206. Lawne, R. (2023, January 3). GDPR vs. U.S. state privacy laws: How do they measure up. *Fieldfisher Insights*. https://www.fieldfisher.com/en/insights/gdpr-vs-u-s-state-privacy-laws-how-do-they-measure

207. Le Monde. (1974, March 21). Justice: Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements… "Safari" ou la chasse aux Français [Justice: While the Ministry of the Interior develops the centrization of its information... "Safari" or the hunt for French]. *Le Monde, 9*. https://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg

208. Lein, L. (2013, August). Social media and municipal employees. *The Alabama Municipal Journal*. https://almonline.org/Assets/Files/LegalServices/LegalPublicationsAndResources/Social_Media_and_Municipal_Employees_Article.pdf

209. Lenin, V. (1969). Polnoe sobranie sochinenii (5 izd.) [Complete Works (5th ed.)]. *Moskva: Izdatel'stvo Politicheskoi Literatury,*. https://crystalbook.ru/wp-content/uploads/2021/05/Lenin-PSS-tom36.pdf

210. Levi, S., Ridgway, W., Simon, D., Slawe, M., & Oh, A. (2024, April 5). Utah becomes first state to enact AI-centric consumer protection law. *Skadden Insights*. https://www.skadden.com/insights/publications/2024/04/utah-becomes-first-state

211. Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2023). Mapping the empirical evidence of the GDPR (in-)effectiveness: A systematic review. *arXiv*. https://doi.org/10.48550/arXiv.2310.16735

212. Lieshout, M., Grossi, L., Spinelli, G., & Helmus, S. (2008). RFID technologies: Emerging issues, challenges and policy options. *Institute for Prospective Technological Studies*. https://www.researchgate.net/publication/235218448_RFID_Technologies_Emerging_Issues_Challenges_and_Policy_Options

213. Likhachev, D. S. (1979). *Poetika drevnerusskoi literatury* [Poetics of Old Russian literature] (3rd ed.). Nauka.

214. Lim, S., & Oh, J. (2025). Navigating privacy: A global comparative analysis of data protection laws. *IET Information Security, (1)*. https://doi.org/10.1049/ise2/5536763

215. Lissens, S. (2024, January 30). The foundations of EU personal data protection law: Privacy and human dignity. *EU-RENEW*. https://eu-renew.eu/the-foundations-of-eu-personal-data-protection-law-privacy-and-human-dignity/

216. Long, E. (1967). *The intruders: The invasion of privacy by government and industry*. Praeger.

217. Lozano, E., Joyce, A., Schiemann, R., Ting, A., & Yahyavi, D. (n.d.). WikiLeaks and whistleblowing (background overview). *Stanford University*.

https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/WikiLeaks/background.html

218. Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198718239.001.0001

219. MacDonald, D. (Director). (1964). *The FBI Nobody Knows* [Film]. Danziger Productions Ltd. https://www.imdb.com/title/tt0741333/

220. Madden, M. (2021, July 14). Colorado enacts comprehensive consumer data privacy legislation. *Consumer Financial Services Blog*. https://consumerfsblog.com/2021/07/colorado-enacts-comprehensive-consumer-data-privacy-legislation/

221. Mahoney, J., & Thelen, K. (Eds.). (2010). *Explaining institutional change: Ambiguity, agency and power*. Cambridge University Press. https://doi.org/10.1017/CBO9780511806414

222. Malik, O. (2023, March 10). Joe Biden's SOTU: The US's long & complicated history with data privacy. *Securiti.ai*. https://securiti.ai/blog/history-of-privacy-in-us/

223. Malik, R. (1971, March 4). The databank society: Can we cope? *New Scientist and Science Journal*, 498.

224. Mallon, L., Haie, A.-G., & Reid, S. (2025, January 13). European Commission fined for unlawful transfer of personal data to the United States. *Steptoe StepTechToe Blog*. https://www.steptoe.com/en/news-publications/steptechtoe-blog/european-commission-fined-for-unlawful-transfer-of-personal-data-to-the-united-states.html

225. Manancourt, V., Ng, A., Scott, M., & Geller, E. (2022, September 27). U.S. expected to publish the Privacy Shield executive order next week. *Politico*. https://www.politico.eu/article/us-expected-to-publish-privacy-shield-executive-order-next-week/

226. Margolis, S. (2024). The disarray of U.S. data privacy and protection laws: History repeats. *FTI Technology Digital Insights & Risk Management Blog*. https://www.ftitechnology.com/resources/blog/the-disarray-of-us-data-privacy-and-protection-laws-history-repeats

227. Margolis, S. (2026). The disarray of U.S. data privacy and protection laws: History repeats. *FTI Technology Digital Insights & Risk Management Blog*.

https://www.ftitechnology.com/resources/blog/the-disarray-of-us-data-privacy-and-protection-laws-history-repeats

228. Markomenko, V. (1997). Informatsionnoe obshchestvo i problemy ego bezopasnosti [Information society and problems of its security]. *Federalizm*, (4).

229. Mathews, W. (1975). A critique of traditional drug education programs. *Journal of Drug Education: Substance Use Research and Prevention, 5*(1), 57–64. https://doi.org/10.2190/BRW6-EXG6-8QTJ-XDTX

230. Matuzov, N. I. (1966). *Sub"ektivnye prava grazhdan SSSR* [Subjective rights of citizens of the USSR]. Saratov.

231. Matuzov, N. I. (1972). *Lichnost'. Pravo. Demokratiia. Teoreticheskie problemy sub"ektivnogo prava* [Personality. Law. Democracy. Theoretical problems of subjective law]. Saratov State Law Institute.

232. Mayfield, M. (2023). Talk data to me: Why Michigan should adopt a comprehensive data protection statute. *Wayne State University Journal of Business Law, 6,* 1–23. https://www.dykema.com/a/web/vVjYRfZrchTW5bziYDuKuj/7F8Gqz/talk-data-to-me-why-michigan-should-adopt-a-comprehensive-data-protection-statute.pdf

233. McMullan, T. (2015, July 15). The world's first hack: the telegraph and the invention of privacy. *The Guardian.* https://www.theguardian.com/technology/2015/jul/15/first-hack-telegraph-invention-privacy-gchq-nsa

234. Meredith, S. (2018, April 10). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. *CNBC.* https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

235. Meredith, S. (2018, April 10). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. *CNBC.* https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

236. Migranova, D. (2024). Vvedenie metricheskikh knig sredi yazycheskogo naseleniya Orenburgskoy gubernii [Introduction of metric books among the pagan population of the Orenburg Governorate]. *Vestnik Akademii nauk Respubliki*

Bashkortostan, Tom 25, 3(115), 21–18. https://cyberleninka.ru/article/n/vvedenie-metricheskih-knig-sredi-yazycheskogo-naseleniya-orenburgskoy-gubernii

237. Mikhajlova, A. (2018). Big data: How can information technologies help the statistics service to increase efficiency of calculation of the consumer price index. *Vestnik Universiteta*, (4), 110–113. https://doi.org/10.26425/1816-4277-2018-4-110-113

238. Mildebrath, H. (2025, October). New GDPR procedural rules for cross-border cases. *Brussels: European Parliament Think Tank. At a Glance, PE 777.953.* https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/777953/EPRS_ATA(2025)777953_EN.pdf

239. Miller, A. (1970, September 6). The surveillance society: Just how far can it go? *Los Angeles Times*, C1–C2.

240. Morrison, S. (2022, July 21). The end of Roe could finally convince Americans to care more about privacy. *Vox.* https://www.vox.com/recode/23271323/roe-dobbs-abortion-data-privacy

241. Mukherjee, R., & Samarajiva, R. (1993). The customer web: Transaction generated information and telecommunication. *Media International Australia, 67*(1), 51–61. https://doi.org/10.1177/1329878X9306700107

242. Myre, G. (2019, April 12). How much did WikiLeaks damage U.S. national security? *NPR.* https://www.npr.org/2019/04/12/712659290/how-much-did-wikileaks-damage-u-s-national-security

243. Myre, G. (2019, April 12). How much did WikiLeaks damage U.S. national security? *NPR.* https://www.kclu.org/world/2019-04-12/how-much-did-wikileaks-damage-u-s-national-security/

244. Nersesiants, V. S. (1993). *Istoriia idei pravovoi gosudarstvennosti* [History of the ideas of the rule-of-law state] (M. M. Slavin, Ed.). Izdatel'stvo IGiP RAN.

245. New York State Department of Financial Services. (2023). *23 NYCRR 500.3 – Cybersecurity program: Policies and procedures.* https://www.dfs.ny.gov/industry_guidance/cybersecurity/23-nycrr-500

246. New York State Department of Financial Services. (2025, June 25). *23 NYCRR 500.3 – Cybersecurity policy (Part 500: Cybersecurity Requirements for Financial Services Companies).* https://regulations.justia.com/states/new-york/title-23/chapter-i/part-500/section-500-3

247. Newman, A. (2008). *Protectors of privacy: Regulating personal data in the global economy.* Cornell University Press. https://www.jstor.org/stable/10.7591/j.ctv2n7f1b

248. Ng, A. (2018, June 22). Supreme Court says warrant necessary for phone location data. *CNET.* https://www.reuters.com/article/technology/supreme-court-restricts-police-on-cellphone-location-data-idUSKBN1JI1WT/

249. Nihill, C. (2025, March 18). House Democrat wants to modernize privacy law in light of DOGE data access. *FedScoop.* https://fedscoop.com/lori-trahan-modernize-privacy-act-doge-data-access/

250. Nikolaichik, V. M. (1973). *SShA: "Bill' o pravakh" i politseiskoe rassledovanie* [USA: The "Bill of Rights" and police investigation]. Nauka.

251. Nissenbaum, H. (2004). *Privacy as contextual integrity.* Washington Law Review, 79(1), 119–158. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

252. Nixon, R. (1974, January 30). 1974 State of the Union Address. *Watergate.info.*https://www.watergate.info/1974/01/30/nixon-1974-state-of-the-union-address.html

253. Novoselov, V. I. (1976). *Pravovoe polozhenie grazhdan v sovetskom gosudarstvennom upravlenii* [Legal status of citizens in Soviet public administration]. Saratov.

254. noyb.eu. (2023, July 10). *European Commission gives EU-US data transfers third round at CJEU.* https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

255. noyb.eu. (n.d.). *Fines resulting from noyb litigation*. Retrieved July 7, 2025, from https://noyb.eu/en/fines-resulting-noyb-litigation

256. Office of Legislative Research. (1998). 98-R-1455: The evolution of privacy: A look at the past, present, and future. *Connecticut General Assembly, Office of Legislative Research.* https://www.cga.ct.gov/PS98/rpt/olr/htm/98-R-1455.htm

257. Office of the Director of National Intelligence. (2015, November 27). Fact Sheet: Implementation of the USA FREEDOM Act of 2015. https://www.intelligence.gov/ic-on-the-record-database/results/fact-sheet/fact-sheet-implementation-of-the-usa-freedom-act-of-2015

258. Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*, 1701–1777. https://epic.org/wp-content/uploads/privacy/reidentification/ohm_article.pdf

259. Own Your Data Foundation. (2020). *Democratizing digital intelligence*. Retrieved January 12, 2026, from https://ownyourdata.foundation

260. Packard, V. (1966). The challenge of computer-based record systems to privacy and civil liberties. Retrieved February 12, 2026, from https://simson.net/ref/1966/Packard_Privacy_Stuff.pdf

261. Packard, V. (1967, January 8). Don't Tell it to the Computer: "Bureaucratic efficiency could put us in chains of plastic tape." *The New York Times Magazine.* https://www.nytimes.com/1967/01/08/archives/dont-tell-it-to-the-computer-dont-tell-it-to-the-computer-cont.html

262. Palmer, V. (2011). Three milestones in the history of privacy in the United States. *Tulane European and Civil Law Forum, 26(1),* 67–97. https://doi.org/10.37381/73a8mx39

263. Pandectes Expert. (2024, September 25). An overview of the rights and requirements in US data privacy laws. *Pandectes.* https://pandectes.io/blog/an-overview-of-the-rights-and-requirements-in-us-data-privacy-laws/

264. Pazyuk, A., & Sokolova, M. (2015). Zashchita personal'nykh dannykh: vvedenie v problematiku [Protection of Personal Data: Introduction to the Issue]: Uchebnoe posobie [Textbook]. *Minsk: Tsentr pravovoi transformatsii.* https://www.lawtrend.org/wp-content/uploads/2015/12/Zashhita-personalnyh-dannyh_Uchebnoe-posobie.pdf

265. Peretti, K., & Austin, A. (2025). Key breach notification updates in California and Oklahoma for 2026. *Alston & Bird Privacy, Cyber & Data Strategy Blog*. https://www.jdsupra.com/legalnews/key-breach-notification-updates-in-california-and-oklahoma-for-8786861/

266. Perez, J. (2007, December 3). CA: Facebook's Beacon more intrusive than previously thought. *Computerworld.* https://www.computerworld.com/article/1594438/ca-facebook-s-beacon-more-intrusive-than-previously-thought.html

267. Perreau, E.-E.-H. (1909). Des droits de la personnalité [On the rights of personality]. *L. Larose et L. Tenin*. https://books.google.ru/books/about/Des_Droits_de_la_personnalit%C3%A9_par_M_E_H.html?id=uUpBQwAACAAJ

268. Phang, K., & Kaabi, J. (2025). Privacy in Flux: A 35-Year Systematic Review of Legal Evolution, Effectiveness, and Global Challenges (U.S./E.U. Focus with International Comparisons). *Journal of Cybersecurity and Privacy, 5*(4). https://doi.org/10.3390/jcp5040103

269. Pittman, F. Paul, Anderson, H., & Hafiz, A. M. (2026, January 20). US Data Privacy Guide. *White & Case LLP.* https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide

270. Plugina, I. (2025, November 2). MVD otchitalos' o presechenii raboty Telegram-bota dlia probiva Userbox [The Ministry of Internal Affairs reported stopping the operation of a Telegram bot for "probiv" Userbox]. *RBC.ru*.https://www.rbc.ru/rbcfreenews/6906fe619a7947866a60fba6

271. Poltavskaia, E. (2020, September 29). "Dokhod moshennikov — bolee 75 mln rublei v mesiatc" [Fraudsters' income exceeds 75 million rubles per month]. *Izvestiia*. https://iz.ru/1066654/elena-poltavskaia/dokhod-moshennikov-bolee-75-mln-rublei-v-mesiatc

272. Poltavskaia, E. (2020, September 29). Dokhod moshennikov — bolee 75 mln rublei v mesiats [Income of fraudsters — more than 75 million rubles per month]. *Izvestia.* https://iz.ru/1066654/elena-poltavskaia/dokhod-moshennikov-bolee-75-mln-rublei-v-mesiatc

273. Popov, V. (2015). Pasportnaia sistema sovetskogo krepostnichestva [The passport system of Soviet serfdom]. *History.ru*. https://history.ru/read/articles/vviedieniie-pasportnoi-sistiemy-event

274. Popova, T. (2022). Legal essence, types and features of legal liability for violation of privacy in the information sphere.*Courier of Kutafin Moscow State Law University (MSAL)*, (4), 100–108. https://doi.org/10.17803/2311-5998.2022.92.4.100-108

275. Potter, Y., Corren, E., Garrido, G., Hoofnagle, C., & Song, D. (2023). An overview of privacy attacks and defenses in large language models. *arXiv.* https://doi.org/10.48550/arXiv.2312.01511

276. Pranitskaia, T. (2010). *Konstitutsionno-pravovoi mekhanizm obespecheniia neprikosnovennosti chastnoi zhizni* [Constitutional and legal mechanism for ensuring the inviolability of private life] [Doctoral dissertation, Belgorod State University]. Belgorod. https://www.dissercat.com/content/konstitutsionno-pravovoi-mekhanizm-obespecheniya-neprikosnovennosti-chastnoi-zhizni

277. Prinz, R., & Hille, C. (2025, July 1). Europe's digital future: eIDAS 2.0's impact on privacy, anti-money laundering. *McDermott Will & Emery Insights.* https://www.mwe.com/insights/europe-eidas-2-0-privacy-anti-money-laundering-impact/

278. Privacy Protection Study Commission. (1977). *Personal privacy in an information society: The report of the Privacy Protection Study Commission*. https://archive.epic.org/privacy/ppsc1977report/

279. PrivacyWorld. (n.d.). *Overview of privacy & data protection laws: United States.* Retrieved December 12, 2025, from https://www.privacyworld.blog/summary-of-data-privacy-protection-laws-in-the-united-states/

280. Prokopenko, A. (2019, April 19). Russia's sovereign Internet law will kill innovation. *Carnegie Endowment for International Peace.* https://carnegie.ru/commentary/78946

281. Prosser, W. (1960). Privacy. *California Law Review, 48*(3). https://lawcat.berkeley.edu/record/1109651?v=pdf

282. Puckett, C. (2009). *The story of the social security number* (SSRN Scholarly Paper No. 1425130). Social Science Research Network. https://doi.org/10.2139/ssrn.1425130

283. Pylaev, I. (2025, July 24). Mintsifry: na "Gosuslugakh" uzhe zaregistrirovano bolee 117 mln pol'zovateley [Ministry of Digital Development: more than 117 million users already registered on the "Gosuslugi" portal]. *ComNews*. https://www.comnews.ru/content/240369/2025-07-24/2025-w30/1009/mincifry-gosuslugakh-uzhe-zaregistrirovano-bolee-117-mln-polzovateley

284. Raymond, M., & Sherman, J. (2024, October 2). Russia's UN cyber treaty is a warning for the future of the internet. *Binding Hook*. https://bindinghook.com/russias-un-cyber-treaty-is-a-warning-for-the-future-of-the-internet/

285. Reals, T. (2010, July 28). WikiLeaks reportedly outs 100s of Afghan informants. *CBS News*. https://www.cbsnews.com/news/wikileaks-reportedly-outs-100s-of-afghan-informants/

286. Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). Review of the European Data Protection Directive. *RAND Europe, Information Commissioner's Office*. https://www.researchgate.net/publication/265450064_Review_of_the_European_Data_Protection_Directive

287. Rosenkoetter, E. (2021, July 14). Colorado enacts comprehensive consumer data privacy legislation. *insideARM*. https://www.insidearm.com/news/00047529-colorado-enacts-comprehensive-consumer-da/

288. Rossi Dal Pozzo, F., & Zoboli, L. (2021). To protect or (not) to protect: Definitional complexities concerning personal (and non-personal) data within the EU. *EUROJUS, (1),* 1–16. https://www.ehcl.eurojus.it/wp-content/uploads/2022/07/To-protect-or-not-to-protect_-definitional-complexities-concerning-personal-and-non-personal-data-within-the-EU-.pd

289. RTM Group. (2023). *Obrabotka personal'nykh dannykh v Rossii: sudebnaya praktika i normativnaya ramka* [Processing of personal data in Russia: court practice and regulatory framework]. https://rtmtech.ru/research/obrabotka-pdn-v-rossii/

290. Ruihua, C. (2025). The social scientific transformation of legal studies. In P. Hao (Ed.), *Handbook of Contemporary Chinese Social Sciences (Handbooks in Asian Studies)*. Singapore: Springer. https://doi.org/10.1007/978-981-97-4026-0_11

291. Ryzhov, R. (2011). Federal'nyy zakon "Ob informatsii, informatizatsii i zashchite informatsii" dlya sovremennoy sistemy pravovogo regulirovaniya informatsionnykh otnosheniy v Rossiyskoy Federatsii [The Federal Law "On Information, Informatization, and Information Protection" for the Modern System of Legal Regulation of Information Relations in the Russian Federation]. *Zhurnal Mir sovremennoy nauki.* Moskva: Izdatel′stvo Pero. https://cyberleninka.ru/article/n/federalnyy-zakon-ob-informatsii-informatizatsii-i-zashchite-informatsii-dlya-sovremennoy-sistemy-pravovogo

292. Sabin, S. (2023, June 30). Colorado, Connecticut data privacy laws go into effect July 1. *Axios.* https://www.axios.com/2023/06/30/privacy-laws-enforcement-colorado-connecticut

293. Safe Computing (University of Michigan). (2025). *2025: State AI laws — State AI regulatory landscape (U-M Safe Computing timeline)*. https://safecomputing.umich.edu/privacy/history-of-privacy-timeline/15485

294. Saglam, B-S., Altuncu, E., Lu, Y., & Li, S. (2022). A systematic literature review of the tension between the GDPR and public blockchain systems. *arXiv Preprint*. https://arxiv.org/abs/2210.04541

295. Sammit Rossiya–Evropeyskiy Soyuz, Sovmestnoye soobshcheniye dlya pechati (2024, November 25) [Russia–European Union Summit, Joint Press Statement]. *Kremlin.ru,* Supplement No. 2093. http://kremlin.ru/supplement/2093

296. Saveliev, A. (2019, April 22). Na puti k kontseptsii regulirovaniia dannykh v usloviiakh tsifrovoi ekonomiki [On the way to a concept of data regulation in the conditions of the digital economy]. *Zakon.ru*. https://www.zakon.ru/publication/igzakon/7841

297. Scarcella, M. (2025, February 7). Facebook defends $725 million privacy settlement in US appeals court. *Reuters.* https://www.reuters.com/legal/litigation/facebook-defends-725-million-privacy-settlement-us-appeals-court-2025-02-07/

298. Schneider, H. A. (2016). Katz v. United States: The untold story. *McGeorge Law Review, 40*(1), 13–23. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

299. Schuler, M. (2025, June 18). How the EU AI Act supplements GDPR in the protection of personal data. *International Trademark Association (INTA).*

https://www.inta.org/perspectives/features/how-the-eu-ai-act-supplements-gdpr-in-the-protection-of-personal-data/

300. Schwartz, P. (1995). Privacy and participation: Personal information and public sector regulation in the United States. *Iowa Law Review, 80,* 471–496. https://lawcat.berkeley.edu/record/1115037/files/fulltext.pdf

301. Schwartz, P. (2013). The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. UC Berkeley Public Law Research Paper No. 2290261. *Harvard Law Review, 126,* 1966–2009. https://ssrn.com/abstract=2290261

302. Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *SSRN*. https://ssrn.com/abstract=1909366

303. Sekste, Ia. A., & Markevich, A. S. (2020). Problemy stanovleniia i razvitiia instituta zashchity personal'nykh dannykh v RF: istoriko-pravovoi aspekt [Problems of the formation and development of the institute of personal data protection in the Russian Federation: Historical and legal aspect]. *Voprosy bezopasnosti*, (4). https://cyberleninka.ru/article/n/problemy-stanovleniya-i-razvitiya-instituta-zaschity-personalnyh-dannyh-v-rf-istoriko-pravovoy-aspekt

304. Shastri, S., Wasserman, M., & Chidambaram, V. (2019). GDPR anti-patterns: How design and operation of modern cloud-scale systems conflict with GDPR. *Cornell University, arXiv.* https://doi.org/10.48550/arXiv.1911.00498

305. Shatz, S., & Lysobey, P. (2024, May 28). State privacy law updates—an ever-growing list of states. *Business Law Lawyer, American Bar Association.* https://www.americanbar.org/groups/business_law/resources/business-lawyer/2024-spring/state-privacy-law-updates-an-ever-growing-list-of-states/

306. Shoop, T. (2025, October 27). That time one agency shut down for one day and changed government forever. *Government Executive.* https://www.govexec.com/management/2025/10/time-one-agency-shut-down-one-day-and-changed-government-forever/409087/

307. Simitis, S. (1995). The EU Directive on the Protection of Personal Data. *DigitalGeorgetown: Georgetown University Library.* https://repository.library.georgetown.edu/handle/10822/882431

308. Skan, O. (2025, February 13). Evinaia sistema ZAGS zarabotala vo vsekh novykh sub'ektakh RF [Unified civil registry system began operating in all new federal subjects of the Russian Federation]. *CNews.ru.* https://www.cnews.ru/news/1794992/

309. Smith, L. (2013). Jonesing for a Test: Fourth Amendment Privacy in the Wake of United States v Jones. *Berkeley Technology Law Journal, 28,* 1003–1034. https://doi.org/10.2139/ssrn.2283972

310. Solove, D. (2004). *The Digital Person: Technology and Privacy in the Information Age.* NYU Press. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&context=faculty_publications

311. Solove, D. (2006). A brief history of information privacy law. *George Washington University Law School.* https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications

312. Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154,* 477–560. https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1

313. Solove, D. (2008). *Understanding privacy*. Harvard University Press. https://scholarship.law.gwu.edu/faculty_publications/922/

314. Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. *Columbia Law Review, 114,* 583. https://doi.org/10.2139/ssrn.2312913

315. Solove, D., & Citron, D. K. (2018). Risk and anxiety: A theory of data breach harms. *Texas Law Review, 96,* 737–786. https://scholarship.law.bu.edu/faculty_scholarship/616

316. Spears, V. (2008). The case that started it all: Roberson v. The Rochester Folding Box Company. *Privacy & Data Security Law Journal,* 1043–1050. https://www.meyerowitzcommunications.com/pdf/roberson-vs-the-rochester.pdf

317. Squire Patton Boggs. (2018, July 8). Supreme Court takes another step to keep up with the digital times: Criminal procedure and cell-phone records in Carpenter. *Privacy World Blog.* https://www.privacyworld.blog/2018/07/supreme-court-takes-another-step-to-keep-up-with-the-digital-times-criminal-procedure-and-cell-phone-records-in-carpenter/

318. State Senator Cindy Friedman (2025, September 25). *Senate unanimously passes the Massachusetts Data Privacy Act*. https://cindyfriedman.org/2025/09/25/senate-unanimously-passes-the-massachusetts-data-privacy-act/

319. Statewatch. (2012, March 28). EU-USA PNR: US changes the privacy rules to exemption access to personal data. *Statewatch.* https://www.statewatch.org/news/2007/september/statewatch-news-online-eu-usa-pnr-us-changes-the-privacy-rules-to-exemption-access-to-personal-data/

320. Stebivko, A. (2023). The genesis of personal data: Informational and legal aspect. *Legal Concept = Pravovaya paradigma, 22*(4), 82–89. https://doi.org/10.15688/lc.jvolsu.2023.4.10

321. Stein, C., & Pilkington, E. (2025, October 1). U.S. expected to publish Privacy Shield executive order next week. *The Guardian.* https://www.politico.eu/article/us-expected-to-publish-privacy-shield-executive-order-next-week/

322. Stepanov, D. (2020, July 17). Evropa zapreshchaet khranit' v SShA dannye svoikh grazhdan [Europe bans storing its citizens' data in the USA]. *CNews.ru.* https://www.cnews.ru/news/top/2020-07-17_evropa_razorvala_dogovor

323. Stepanov, S., & Ivanova, E. (2023). Problema "suverennogo interneta" v Rossii [The problem of "sovereign internet" in Russia]. *Vestnik Rossiyskogo universiteta druzhby narodov. Seriia: Gosudarstvennoe i munitsipal'noe upravlenie, 2*. https://cyberleninka.ru/article/n/problema-suverennogo-interneta-v-rossii

324. Stetsovskiy, Yu. (2000). Pravo na svobodu i lichnuyu neprikosnovennost′: normy i deystvitel′nost′ [The right to freedom and personal inviolability: norms and reality]. Moskva: *Delo*.

325. Stevens, G. M. (2003). Compliance with the HIPAA medical privacy rule (CRS Report for Congress). *Congressional Research Service*. https://www.everycrsreport.com/files/20030424_RS21505_8bd705784da4f3124d5051b6f781480ea7dccc2d.pdf

326. Story, L., & Helft, M. (2007, April 14). Google buys DoubleClick for $3.1 billion. *The New York Times.* https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html

327. Streinz, T. (2021). The Evolution of European Data Law. In *The Evolution of EU Law* (3rd ed., pp. 902–936). Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780192846556.003.0029

328. Strömholm, S. (1967). *Right of privacy and rights of the personality: A comparative survey* (Working paper prepared for the Nordic Conference on Privacy organized by the International Commission of Jurists, Stockholm, May 1967). Stockholm: P. A. Norstedt & Söners Förlag. https://www.icj.org/wp-content/uploads/1967/06/right-to-privacy-working-paper-publication-1967-eng.pdf

329. Szabó, A. (2016). The European Union and the United States of America from the perspective of data privacy. *Acta Technica Corviniensis - Bulletin of Engineering, 9*(1), 101–104. https://www.proquest.com/docview/1767584932?sourcetype=Scholarly%20Journals

330. Szeftel, M. (1958). Personal inviolability in the legislation of the Russian absolute monarchy. *American Slavic and East European Review, 17*(1), 1–24. https://doi.org/10.2307/3004299

331. TASS. (2022, December 21). *"Yandeks Edu" priznali poterpevshey po delu ob utechke dannykh klientov* ["Yandex Eda" recognized as a victim in a case about client data leak]. https://tass.ru/ekonomika/16655005

332. TASS. (2022, July 28). *V Rossii vladel'tsa Snapchat oshtrafovali na 1 mln rublei* [In Russia, the owner of Snapchat was fined 1 million rubles]. https://tass.ru/obschestvo/15330249

333. TASS. (2022, July 28). *WhatsApp oshtrafovali na 18 mln rubley za narushenie zakona o lokalizatsii dannykh rossiyan* [WhatsApp fined 18 million rubles for violating the law on localization of Russians' data]. https://tass.ru/proisshestviya/15330479

334. TASS. (2022, March 1). *"Yandex.Eda" vyiavila utechku lichnykh dannykh pol'zovatelei, kotorye ne kasalis' platezhei* [Yandex.Eda identified a leak of users' personal data not related to payments]. https://tass.ru/ekonomika/13921381

335. TASS. (2025, October 16). *Rossiyane vse chashche zabotyatsya o svoikh personal'nykh dannykh* [Russians increasingly care about their personal data]. https://tass.ru/obschestvo/15192205

336. Taylor, A., Friedman, C., & Fishel, G. (2025, May 19). State AGs fill the AI regulatory void. *Reuters*. https://www.reuters.com/legal/legalindustry/state-ags-fill-ai-regulatory-void-2025-05-19/

337. The Washington Post. (2017, December 1). *The Washington Post partners with Facebook in an experiment to help users identify breaking news stories.* https://www.washingtonpost.com/pr/wp/2017/12/01/the-washington-post-partners-with-facebook-in-an-experiment-to-help-users-identify-breaking-news-stories/

338. TheBestVPN.com. (2026, January 16). How many data breaches happen every day? TheBestVPN. https://thebestvpn.com/statistics/how-many-data-breaches-happen-every-day/

339. TrueVault. (n.d.). *Colorado Privacy Act: An introduction.* Retrieved December 12, 2026, from https://www.truevault.com/learn/cpa-introduction

340. TrustArc. (n.d.). *European Union data privacy: What's next for 2025*. Retrieved February 4, 2026, from https://trustarc.com/resource/european-union-data-privacy-whats-next-for-2025/

341. Turgarinov, V. (1965). *Lichnost' i obshchestvo* [Personality and society]. Mysl'.

342. U.S. Department of Commerce. (2023, July 17). Data Privacy Framework Program launches new website enabling U.S. companies to participate in cross-border data transfers. *U.S. Department of Commerce*. https://www.commerce.gov/news/press-releases/2023/07/data-privacy-framework-program-launches-new-website-enabling-us

343. U.S. Department of Education. (2000). *Which educational agencies or institutions does FERPA apply to?*https://studentprivacy.ed.gov/faq/which-educational-agencies-or-institutions-does-ferpa-apply

344. U.S. Department of Health and Human Services. (2025). *Privacy Impact Assessments (PIAs) & Resources*. https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/pias-and-resources/index.html

345. U.S. Department of Justice, Office of Privacy and Civil Liberties. (2020). *Overview of the Privacy Act of 1974: 2020 edition – Introduction*. https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction

346. U.S. Department of Justice. (2007). *Overview of the USA PATRIOT Act: Legislative history and provisions*. https://www.justice.gov/archive/ll/highlights.htm

347. Undisputed Legal. (n.d.). *Privacy of genetic information in the United States.* Retrieved January 22, 2026, from https://undisputedlegal.com/privacy-of-genetic-information-in-the-united-states/

348. United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Practice and Procedure. (1967). *Government dossier: survey of information contained in Government files*. Washington: U.S. Govt. Print. Off.

349. University of Michigan Information and Technology Services. (n.d.). History of privacy timeline. *Safe Computing*. Retrieved November 11, 2026, from https://safecomputing.umich.edu/privacy/history-of-privacy-timeline/15485

350. Vigilev, A. N. (1990). *Istoriia otechestvennoi pochty* [History of the national postal service] (2nd ed.). Sviaz'.

351. Vilisova, I., & Grishin, D. (2022). Zarozhdenie i razvitie Zakona o personalnykh dannykh v Rossii [The emergence and development of the Law on Personal Data in Russia]. *Voprosy rossiyskogo i mezhdunarodnogo prava*, *12*(3A), 315–319. https://doi.org/10.34670/AR.2022.70.63.036

352. Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st ed.). Cham: Springer International Publishing AG. https://doi.org/10.1007/978-3-319-57959-7

353. Voinikanis, E., Mashukova, E., & Stepanov-Egiants, V. (2014). Neprikosnovennost' chastnoy zhizni, personal'nye dannye & otvetstvennost' za nezakonnyy sbor i rasprostranenie svedeniy o chastnoy zhizni i personal'nykh dannykh: problemy sovershenstvovaniya zakonodatel'stva [Inviolability of private life, personal data & liability for unlawful collection & dissemination of private life & personal data: problems of improving legislation]. *Zakonodatel'stvo*, (12), 74–80. https://istina.msu.ru/publications/article/7644997/

354. Volini, A. (2023). The right to data privacy: Revisiting Warren & Brandeis. *Northwestern Journal of Technology and Intellectual Property, 21*. https://scholarlycommons.law.northwestern.edu/njtip/vol21/iss1/1

355. Volkov, A. (1990). Perepis' naseleniia 1937 goda: vymysly i pravda [The 1937 population census: fiction & truth]. In *Perepis' naseleniia SSSR 1937 goda. Istoriia i materialy Ekspress-informatsiia. Seriia "Istoriia statistiki"*, Moskva: Vypusk 3-5 (Chast' II), 6–63. https://www.demoscope.ru/weekly/knigi/polka/gold_fund08.html

356. Voss, A. (2025, February 17). We should revise the GDPR to unlock Europe's digital future. *CEPS*. https://www.ceps.eu/we-should-revise-the-gdpr-to-unlock-europes-digital-future/

357. Wahl, T. (2021, December 22). Commission adopted adequacy decision for South Korea. *eucrim – European Criminal Law Associations' Forum*. https://eucrim.eu/news/commission-adopted-adequacy-decision-for-south-korea/

358. Waldman, A. (2021). Data Protection by Design? A Critique of Article 25 of the GDPR. Northeastern University School of Law Research. Paper No. 411-2021. *Cornell International Law Journal, 53,* 22–43.https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773143

359. Wallace, R. (1964, April 10). What happened to our privacy? *Life*, 10.

360. Warburton, M. (2024, June 26). Federal data privacy laws gain support in US Congress, but critics remain. *Reuters*. https://www.reuters.com/world/us/federal-data-privacy-laws-gain-support-us-congress-critics-remain-2024-06-26/

361. Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160

362. Westin, A. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166–182. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

363. Whitman, J. (2004). The two Western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, *113*(6), 1151–1221. https://yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty

364. Wieacker, F., Weir, T., & Zimmermann, R. (1996). *A History Of Private Law In Europe: with particular reference to Germany*. Oxford University Press. https://academic.oup.com/book/55010

365. Wiewiórowski, W. (2024, January 17). Two decades of protecting privacy & data protection to fuel the future. *European Data Protection Supervisor*. https://www.edps.europa.eu/press-publications/press-news/blog/two-decades-protecting-privacy-and-data-protection-fuel-future

366. Wold, J. (2025, March 3). Deafening Commission silence with no credible EU-US data oversight left. *Euractiv*. https://www.euractiv.com/news/deafening-commission-silence-with-no-credible-eu-us-data-oversight-left/

367. Xavier, S., Frey, A., & Phillips, S. (2025, January 2). Protecting reproductive health data: state laws against geofencing. *Reuters*. https://www.reuters.com/legal/legalindustry/protecting-reproductive-health-data-state-laws-against-geofencing-2025-01-02/

368. Zaguir, N., de Magalhães, G., & de Mesquita Spinola, M. (2024). Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions. *IEEE Access, 12*, 81608–81630. https://doi.org/10.1109/ACCESS.2024.3406724

369. Zang, D. (2024). The Privacy Act of 1974: The American Bill of Rights on data & its unfinished business. *University of Pittsburgh Law Review*, *85*. https://digitalcommons.law.uw.edu/faculty-articles/1111

370. Zharova, A., & Elin, V. (2017). Istochniki ponyatiy "personal′nye dannye" & chastnaya zhizn' litsa v rossiyskom prave [Sources of the concepts "personal data" & private life of a person in Russian law]. *Vestnik Akademii prava i upravleniia*, *46*(1). https://cyberleninka.ru/article/n/istochniki-ponyatiy-personalnye-dannye-i-chastnaya-zhizn-litsa-v-rossiyskom-prave

371. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791

372. Zweifel-Keegan, C. (2024, October 25). A view from DC: The beginning of the end of the free flow of data. *International Association of Privacy Professionals*.

https://iapp.org/news/a/a-view-from-dc-the-beginning-of-the-end-of-the-free-flow-of-data/

2. Legal Sources: Legislation and Case Law

a. U.S.A

1. California Senate. (2003). *Senate Bill 1386* (SB 1386). http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

2. California Senate. (2005). *Shine the Light Act* (Cal. Civil Code Section 1798.83).https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV

3. California Senate. (2011). *Reader Privacy Act* (SB 602). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201120120SB602

4. California Senate. (2013). *California Generative Artificial Intelligence Training Data Transparency Act* (AB 2013). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2013

5. California Senate. (2015). *California Electronic Communications Privacy Act* (Cal. Penal Code Section 1546). https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1546.&lawCode=PEN

6. California Senate. (2018). *California Consumer Privacy Act* (Cal. Civil Code Sections 1798.100 - 1798.199.100). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

7. California Senate. (2020). *California Privacy Rights Act* (Proposition 24, Cal. Civil Code Sections 1798.100–1798,). https://thecpra.org

8. California Senate. (2025). *California Senate Bill 446* (SB 446). https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB446

9. Colorado Senate. (2023). *Colorado Privacy Act* (SB 21-190). https://leg.colorado.gov/bills/sb21-190

10. Colorado Senate. (2024). *Colorado Artificial Intelligence Act* (SB 24-205). https://leg.colorado.gov/bills/sb24-205

11. Connecticut Senate. (2023). *Connecticut Data Privacy Act* (SB 6). https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act

12. Federal Trade Commission. (1999, February 5). In the matter of GeoCities, File No. 982-3015; Docket No. C-3850. *Federal Trade Commission decision and order*. https://www.ftc.gov/legal-library/browse/cases-proceedings/982-3015-geocities

13. Federal Trade Commission. (1999, February). *Complaint: In the matter of GeoCities* (Docket No. C-3850). https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015cmp.htm

14. Federal Trade Commission. (1999, February). *Decision and order: In the matter of GeoCities* (DocketNo. C-3850). https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do_.ht

15. Federal Trade Commission. (2007, December 20). *Statement of the Federal Trade Commission concerning Google/DoubleClick* (FTC File No. 071-0170). https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-federal-trade-commission-concerning-googledoubleclic

16. Illinois Senate. (2008). *Illinois Biometric Privacy Act* (SB 2400). https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57

17. Maryland Senate. (2024). *Maryland Online Data Privacy Act* (SB 541). https://mgaleg.maryland.gov/2024RS/bills/hb/hb0567e.pdf

18. Massachusetts Senate. (2024). *Massachusetts Privacy Act* (SB 2619). https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://malegislature.gov/Bills/194/S2619&ved=2ahUKEwjEgcibxt2SAxUd_rsIHY-_AewQFnoECBsQAQ&usg=AOvVaw3Pe0envZwVacahL0Ldo1yK

19. Obama, B. (2011, October 7). *Executive Order 13587—Structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information*. Federal Register, 76(197), 63811–63813. https://www.govinfo.gov/content/pkg/FR-2011-10-13/pdf/2011-26729.pdf

20. Obama, B. (2014, January 28). *State of the Union address*. The White House. https://obamawhitehouse.archives.gov/state-union-2014

21. Obama, B. (2015, January 12). *Remarks by the President at the Federal Trade Commission*. The White House. https://obamawhitehouse.archives.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission

22. Obama, B. (2015, January 20). *State of the Union address*. The White House. https://obamawhitehouse.archives.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015

23. Oklahoma Senate. (2025). *An act amending the Security Breach Notification Act* (SB 626). https://www.oklegislature.gov/BillInfo.aspx?Bill=SB626&Session=2500

24. The White House. (2022, February 15). *Executive Order 14086: Enhancing Safeguards for United States Signals Intelligence Activities*. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/02/15/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

25. U.S. Congress. (1872). *Senate Bill, S.1572* — 42nd Cong. http://www.congress.gov/42/llsb/S.1572v3.pdf

26. U.S. Congress. (1968, May 7). *Congressional Record*: *Senate*, Vol. 114, Part 9, pp. 11975–12062 (Permanent bound edition). Government Publishing Office. https://www.congress.gov/90/crecb/1968/05/07/GPO-CRECB-1968-pt9-7-1.pdf

27. U.S. Congress. (1970). *Fair Credit Reporting Act*, H.R.6354 — 91st Congress. https://www.congress.gov/bill/91st-congress/house-bill/6354

28. U.S. Congress. (1974). *Family Educational Rights and Privacy Act*, H.R.69 — 93rd Congress. https://www.congress.gov/bill/93rd-congress/house-bill/69

29. U.S. Congress. (1975, November 11). *Congressional Record: Proceedings and debates of the 94th Congress*, First Session (Vol. 121, Part 28, pp. 35773–35929). Government Publishing Office. https://www.govinfo.gov/content/pkg/GPO-CRECB-1975-pt28/pdf/GPO-CRECB-1975-pt28-1-1.pdf

30. U.S. Congress. (1975). *Congressional Record: Bound edition*, part 28. Government Publishing Office. https://www.govinfo.gov/content/pkg/GPO-CRECB-1975-pt28/pdf/GPO-CRECB-1975-pt28-1-1.pdf

31. U.S. Congress. (1986). *Electronic Communications Privacy Act*, H.R.347 — 99th Congress. https://www.congress.gov/bill/99th-congress/house-bill/347

32. U.S. Congress. (1991). *Telephone Consumer Protection Act and the National "Do Not Call" Registry*, H.R.1304 — 102nd Congress. https://www.fcc.gov/general/telemarketing-and-robocalls

33. U.S. Congress. (1994). *Driver's Privacy Protection Act*, H.R.3365 — 103rd Congress. https://www.congress.gov/bill/103rd-congress/house-bill/3365

34. U.S. Congress. (1999). *Gramm-Leach-Bliley Act*, H.R.10 — 106th Congress. https://www.congress.gov/bill/106th-congress/house-bill/10

35. U.S. Congress. (2001). *USA PATRIOT Act* (Public Law No. 107-56). https://www.fincen.gov/resources/statutes-and-regulations/usa-patriot-act

36. U.S. Congress. (2002). *E-Government Act*, H.R.2458 — 107th Congress. https://www.congress.gov/bill/107th-congress/house-bill/2458

37. U.S. Congress. (2014). *Federal Information Security Modernization Act*, H.R.1163 — 113th Congress. https://www.congress.gov/bill/113th-congress/house-bill/1163

38. U.S. Congress. (2015). *Cybersecurity Information Sharing Act and the National Cybersecurity Protection Advancement Act*, S.754 — 114th Congress. https://www.congress.gov/bill/114th-congress/senate-bill/754

39. U.S. Congress. (2015). *USA Freedom Act*, H.R.2048 — 114th Congress. https://www.congress.gov/bill/114th-congress/house-bill/2048

40. U.S. Congress. (2018). *Data Breach Prevention and Compensation Act*, H.R.2545 — 116th Congress. https://www.congress.gov/bill/116th-congress/house-bill/2545

41. U.S. Congress. (2021). *Data Care Act*, S.744 — 118th Congress. https://www.congress.gov/bill/118th-congress/senate-bill/744

42. U.S. Congress. (2022). *Consumer Data Privacy and Security Act*, S.1494 — 117th Congress. https://www.congress.gov/bill/117th-congress/senate-bill/1494

43. U.S. Congress. (2024). *Protecting Americans from Foreign Adversary Controlled Applications Act*, H.R.7521 — 118th Congress. https://www.congress.gov/bill/118th-congress/house-bill/7521

44. U.S. Congress. House. Committee on Government Operations. Special Subcommittee on Invasion of Privacy. (1966, July 26–28). *The computer and invasion of privacy: Hearings before a Subcommittee* — 89th Congress, second session (Vols. 74-77). U.S. Government Printing Office. https://books.google.ru/books/about/The_Computer_and_Invasion_of_Privacy.html?id=2IAHJna7A1cC&redir_esc=y

45. U.S. Department of Health & Human Services. (1996). *HIPAA Privacy Rule*. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

46. U.S. Department of Health, Education & Welfare. (1973, July). *Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (OHEW Publication No. (OS) 73-94). https://www.justice.gov/opcl/docs/rec-com-rights.pdf

47. U.S. Department of Health, Education, and Welfare. (1973). *The Code of Fair Information Practices*. https://www.justice.gov/opcl/fair-information-practices

48. U.S. Government Publishing Office. (2010). *Federal Trade Commission Act* (15 U.S.C. §§ 41-58). https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act

49. U.S. President. (2011). *Executive Order 13587 on Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*. https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

50. U.S. President. (2022). *Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities* (87 Fed. Reg. 62283). https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

51. U.S. Supreme Court. (1902). *Roberson v. Rochester Folding Box Co* (171 U.S. 538). https://supreme.justia.com/cases/federal/us/171/538/

52. U.S. Supreme Court. (1928). *Olmstead v. United States* (277 U.S. 438). https://supreme.justia.com/cases/federal/us/277/438/

53. U.S. Supreme Court. (1965). *Griswold v. Connecticut* (381 U.S. 479). https://supreme.justia.com/cases/federal/us/381/479/

54. U.S. Supreme Court. (1967). *Katz v. United States* (389 U.S. 347). https://supreme.justia.com/cases/federal/us/389/347/

55. U.S. Supreme Court. (1968). *Terry v. Ohio* (392 U.S. 1). https://supreme.justia.com/cases/federal/us/392/1/

56. U.S. Supreme Court. (1972). *Eisenstadt v. Baird* (405 U.S. 438). https://supreme.justia.com/cases/federal/us/405/438/

57. U.S. Supreme Court. (1972). *United States v. U.S. District Court* (407 U.S. 297). https://supreme.justia.com/cases/federal/us/407/297/

58. U.S. Supreme Court. (1973). *Roe v. Wade* (410 U.S. 113). https://supreme.justia.com/cases/federal/us/410/113/

59. U.S. Supreme Court. (1976). *United States v. Miller* (425 U.S. 435). https://supreme.justia.com/cases/federal/us/425/435/

60. U.S. Supreme Court. (1977). *Nixon v. General Services Administration* (433 U.S. 425). https://supreme.justia.com/cases/federal/us/433/425/

61. U.S. Supreme Court. (1977). *Whalen v. Roe* (429 U.S. 589). https://supreme.justia.com/cases/federal/us/429/589/

62. U.S. Supreme Court. (1979). *Smith v. Maryland* (442 U.S. 735). https://supreme.justia.com/cases/federal/us/442/735/

63. U.S. Supreme Court. (1992). *Planned Parenthood v. Casey* (505 U.S. 833). https://supreme.justia.com/cases/federal/us/505/833/

64. U.S. Supreme Court. (2004). *Doe v. Chao* (540 U.S. 614). https://supreme.justia.com/cases/federal/us/540/614/

65. U.S. Supreme Court. (2011). *NASA v. Nelson* (562 U.S. 134). https://supreme.justia.com/cases/federal/us/562/134/

66. U.S. Supreme Court. (2011). *Sorrell v. IMS Health* (564 U.S. 552). https://supreme.justia.com/cases/federal/us/564/552/

67. U.S. Supreme Court. (2016). *Spokeo, Inc. v. Robins* (578 U.S. 330). https://supreme.justia.com/cases/federal/us/578/330/

68. U.S. Supreme Court. (2018). *Carpenter v. United States* (585 U.S. 296). https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

69. U.S. Supreme Court. (2021). *TransUnion LLC v. Ramirez* (594 U.S. 413). https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf

70. U.S. Supreme Court. (2022). *Dobbs v. Jackson Women's Health Organization* (597 U.S. 215). https://www.supremecourt.gov/opinions/21pdf/19-1392_6j37.pdf

71. U.S. Supreme Court. (2025). *TikTok, Inc. v. Garland* (604 U.S. 56). https://www.supremecourt.gov/opinions/24pdf/24-656_ca7d.pdf

72. United States House Committee on House Administration. (2022, February 16). *Big data: Privacy risks and needed reforms in the public and private sectors (House Hearing)*. U.S. Government Publishing Office. https://www.congress.gov/117/chrg/CHRG-117hhrg49431/CHRG-117hhrg49431.pdf

73. Utah Senate. (2024). *Utah Artificial Intelligence Policy Act* (SB 149). https://le.utah.gov/~2024/bills/static/SB0149.html

74. Virginia Senate. (2021). *Virginia Consumer Data Protection Act* (Va. Code § 59.1-575 et seq). https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

b. Russia

1. Federation Arbitrazhnyy sud Moskovskogo okruga [Arbitration Court of the Moscow District]. (2023, March 30). *Postanovleniye No. F05-4354/2023 po delu No. A40-139096/22* [Decision No. F05-4354/2023 In re No. A40-139096/22]. https://normativ.kontur.ru/document?moduleId=7&documentId=464882

2. Arbitrazhnyy sud Moskovskogo okruga. (2023). *Postanovlenie No. Ф05-4354/2023* [Resolution No. Ф05-4354/2023]. https://normativ.kontur.ru/document?moduleId=7&documentId=464882

3. Arbitrazhnyy sud Zapadno-Sibirskogo okruga. (2023, May 10). *Postanovleniye No. F04-1436/2023 po delu No. A27-13261/2022* [Decision No. F04-1436/2023 In re No. A27-13261/2022].

4. Chrezvychaynyy VIII Vsesoyuznyy s″ezd Sovetov. (1936). *Konstitutsiya (Osnovnoy zakon) Soyuza Sovetskikh Sotsialisticheskikh Respublik* [Constitution (Fundamental Law) of the USSR]. https://www.marxists.org/history/ussr/government/constitution/1936/1936-constitution.pdf

5. Council of the European Union. (2004, November 25). *Fourteenth Russia–EU Summit. Joint press release (15061/04, Presse 333).* https://ec.europa.eu/commission/presscorner/detail/en/pres_04_333

6. Federal′naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSTEK Rossii). (2008). *Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh* [Basic Threat Model for Personal Data Security in Information Systems]. https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/bazovaya-model-ot-15-fevralya-2008-g

7. Federal′naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSTEK Rossii). (2013). *Prikaz N 21 "Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer…"* [Order No. 21 "On Approval of Organizational and Technical Measures…"]. https://www.consultant.ru/document/cons_doc_LAW_146520/

8. Federal′naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSTEK Rossii). (2021). *Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh…* [Methodology for Determining Current Threats to Personal Data Security].

9. Federal′naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu (FSTEK Rossii). (2023, December 14). *Bank dannykh ugroz bezopasnosti informatsii FSTEK Rossii* [Information Security Threat Data Bank of FSTEC of Russia]. https://fstec.ru/gniii-ptzi-fstek-rossii/produkty/bank-dannykh-ugroz-bezopasnosti-informatsii-fstek-rossii

10. Federal′noye agentstvo po tekhnicheskomu regulirovaniyu i metrologii. (2006). *GOST R 50922-2006. Zashchita informatsii. Osnovnyye terminy i opredeleniya* [National Standard of the Russian Federation GOST R 50922-2006. Information Protection. Basic Terms and Definitions]. https://docs.cntd.ru/document/1200058320

11. Federal′noye agentstvo po tekhnicheskomu regulirovaniyu i metrologii. (2012). *GOST R ISO/MEK 27002-2012. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informatsionnoy bezopasnosti* [National Standard of the Russian Federation GOST R ISO/IEC 27002-2012. Information Technology. Security Techniques. Code of Practice for Information Security Management]. https://docs.cntd.ru/document/1200103619

12. Federal′nyy portal proektov normativno-pravovykh aktov. (n.d.). *O vnesenii izmeneniy v otdel'nye zakonodatel'nye akty* (ID proekta 89871) [On amendments to certain legislative acts (Project ID 89871)]. Retrieved January 26, 2026, from https://regulation.gov.ru/

13. Federation Council of the Federal Assembly of the Russian Federation. (2003). *Federal'nyy zakon N 126-FZ "O svyazi"* [Federal Law No. 126-FZ "On Communications"]. https://www.consultant.ru/document/cons_doc_LAW_43224/

14. Federation Council of the Federal Assembly of the Russian Federation. (2014). *Federal'nyy zakon N 242-FZ "O vnesenii izmeneniy v otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii v chasti utochneniya poryadka obrabotki personal'nykh dannykh v informatsionno-telekommunikatsionnykh setyakh"* [Federal Law No. 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Procedure for Processing Personal Data in Information and Telecommunication Networks"]. https://www.consultant.ru/document/cons_doc_LAW_165838/

15. Gosudarstvennaya Duma Federal′nogo Sobraniya Rossiyskoy Federatsii. (2024). *Poyasnitel'naya zapiska k proektu federal'nogo zakona № 679980-8 "O vnesenii izmeneniy v stat'yu 9 Federal'nogo zakona "O personal'nykh dannykh" i stat'yu 10 Zakona Rossiyskoy Federatsii "O zashchite prav potrebiteley"* [Explanatory note to Draft Federal Law No. 679980-8 "On amendments to Article 9 of the Federal Law "On Personal Data" and Article 10 of the Law of the Russian Federation "On Protection of Consumer Rights"]. https://base.garant.ru/76865062/

16. Gosudarstvennaya Duma Rossiyskoy Federatsii. (2005). *Proekt federal'nogo zakona N 217352-4 "O personal'nykh dannykh"* [Draft Federal Law No. 217352-4 "On Personal Data"]. https://docs.cntd.ru/document/901988739

17. Gosudarstvennaya Duma Rossiyskoy Federatsii. (2024). *Poyasnitel'naya zapiska k proektu federal'nogo zakona N 679980-8* [Explanatory Note to Draft Federal Law No. 679980-8]. https://sozd.duma.gov.ru/bill/679980-8

18. Izvestiya TsK KPSS. (1991). *No. 2*, p. 204. https://imwerden.de/publ-9916

19. Mirovoy sudya sudebnogo okruga No. 456 (Danilovskiy rayon g. Moskvy). (2023). *Postanovlenie No. 05-1415/456/2023* [Decision No. 05-1415/456/2023]. https://mos-sud.ru/456/cases/admin/details/1e630656-51e5-4dc1-afa1-76c2830a57ae?caseNumber=05-1415/456/2023

20. Mirovoy sudya sudebnogo uchastka No. 244 (Donskoy rayon g. Moskvy). (2023). *Postanovlenie No. 05-1048/244/2023* [Decision No. 05-1048/244/2023]. https://mos-sud.ru/244/cases/admin/details/9337e0b6-dfe8-4986-92d1-8f07156a122d?caseNumber=05-1048/244/2023

21. Mirovoy sudya sudebnogo uchastka No. 54 (Konkovo rayon g. Moskvy). (2023). *Postanovlenie No. 05-0309/54/2023* [Decision No. 05-0309/54/2023]. https://mos-sud.ru/244/cases/admin/details/9337e0b6-dfe8-4986-92d1-8f07156a122d?caseNumber=05-1048/244/2023

22. Moskovskiy gorodskoy sud. (2019, August 2). *Apellyatsionnoye opredeleniye po delu No. 33-35187/2019* [Appellate Ruling In re No. 33-35187/2019]. https://www.mos-gorsud.ru/mgs/services/cases/appeal-civil/details/b2b71bba-4821-4670-b1e4-4f6e51764920?caseNumber=33-35187/2019

23. Moskovskiy rayonnyy sud g. Kaliningrada. (2017, April 19). *Resheniye po delu No. 2-688/2017* [Decision No. 2-688/2017].

24. Pravitel′stvo Rossiyskoy Federatsii. (2005). *Proekt federal'nogo zakona N 217355-4 "O vnesenii izmeneniy v otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii…"* [Draft Federal Law No. 217355-4 "On Amendments to Certain Legislative Acts of the Russian Federation…"]. https://base.garant.ru/5198911/

25. Pravitel′stvo Rossiyskoy Federatsii. (2008). *Postanovlenie N 687 "Ob utverzhdenii Polozheniya ob osobennostyakh obrabotki personal'nykh dannykh, osushchestvlyaemoy bez ispol'zovaniya sredstv avtomatizatsii"* [Resolution No. 687 "On Approval of the Regulation on the Specifics of Personal Data Processing without Automation Tools"]. https://base.garant.ru/193875/

26. Pravitel′stvo Rossiyskoy Federatsii. (2012). *Postanovlenie N 1119 "Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh"* [Resolution No. 1119 "On Approval of Requirements for Personal Data Protection in Information Systems"]. https://www.consultant.ru/document/cons_doc_LAW_137356/

27. President of the Russian Federation. (2016). *Ukaz Prezidenta Rossiyskoy Federatsii № 646 "Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii"* [Decree No. 646 "On the Approval of the Doctrine of Information Security of the Russian Federation"]. https://kremlin.ru/acts/bank/41460

28. Presnenskiy rayonnyy sud (Gorod Moskva). (2023, March 21). *Resheniye po delu No. 02-0522/2023 [02-9418/2022; M-8559/2022]* [Decision In re No. 02-0522/2023 [02-9418/2022; M-8559/2022]].

29. Prezident Rossiyskoy Federatsii. (1997). *Ukaz N 188 "Ob utverzhdenii Perechnya svedeniy konfidentsial'nogo kharaktera"* [Decree No. 188 "On Approval of the List of Confidential Information"]. https://www.consultant.ru/document/cons_doc_LAW_13532/

30. Prezident Rossiyskoy Federatsii. (2016, December 5). *Ukaz No. 646 "Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii"* [Decree No. 646 "On Approval of the Information Security Doctrine of the Russian Federation"]. http://kremlin.ru/acts/bank/41460

31. Roskomnadzor. (2009, September 9). *Pis'mo No. SS-05-3/6055 vrio Ministra svyazi i massovykh kommunikatsiy Rossiyskoy Federatsii* [Letter No. SS-05-3/6055 to the Acting Minister of Communications and Mass Media of the Russian Federation].

32. Roskomnadzor. (2017, May 30). *Prikaz No. 94 "Ob utverzhdenii Metodicheskikh rekomendatsiy po uvedomleniyu upolnomochennogo organa o nachale obrabotki personal'nykh dannykh i o vnesenii izmeneniy v ranee predstavlennyye svedeniya"* [Order No. 94 "On Approval of Methodological Recommendations on Notifying the Authorized Body about the Commencement of Personal Data Processing and Amendments to Previously Submitted Information"]. https://docs.cntd.ru/document/456088345

33. Roskomnadzor. (2017). *Prikaz № 94 "Ob utverzhdenii metodicheskikh rekomendatsiy…"* [Order No. 94 "On the Approval of Methodological Recommendations…"]. https://base.garant.ru/71752212/

34. Samarskiy oblastnoy sud. (2019, October 17). *Apellyatsionnoye opredeleniye No. 33-12118/2019* [Appellate Ruling No. 33-12118/2019]. http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SOPV&n=419375

35. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (1995). *Federal'nyy zakon N 24-FZ "Ob informatsii, informatizatsii i zashchite informatsii"* [Federal Law No. 24-FZ "On Information, Informatization and Protection of Information"]. https://www.consultant.ru/document/cons_doc_LAW_5887/

36. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (1996). *Ugolovnyy kodeks Rossiyskoy Federatsii N 63-FZ* [Criminal Code of the Russian Federation No. 63-FZ]. https://www.consultant.ru/document/cons_doc_LAW_10699/

37. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (2001). *Kodeks Rossiyskoy Federatsii ob administrativnykh pravonarusheniyakh N 195-FZ* [Code of Administrative Offenses of the Russian Federation No. 195-FZ]. https://www.consultant.ru/document/cons_doc_LAW_34661/

38. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (2005). *Federal'nyy zakon N 160-FZ "O ratifikatsii Konventsii Soveta Evropy o zashchite fizicheskikh lits pri avtomatizirovannoy obrabotke personal'nykh dannykh"* [Federal Law No. 160-FZ "On Ratification of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"]. https://base.garant.ru/12143756/

39. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (2006). *Federal'nyy zakon N 152-FZ "O personal'nykh dannykh"* [Federal Law No. 152-FZ "On Personal Data"]. https://www.consultant.ru/document/cons_doc_LAW_61801/

40. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (2006). *Federal'nyy zakon N 149-FZ "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii"* [Federal Law No. 149-FZ "On Information, Information Technologies and Protection of Information"]. https://www.consultant.ru/document/cons_doc_LAW_61798/

41. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (2017). *Federal'nyy zakon N 242-FZ "O vnesenii izmeneniy v otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii po voprosam primeneniya informatsionnykh tekhnologiy v sfere okhrany zdorov'ya"* [Federal Law No. 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Application of Information Technologies in Healthcare"]. https://www.consultant.ru/document/cons_doc_LAW_221184/

42. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (2014). *Federal'nyy zakon N 242-FZ "O vnesenii izmeneniy v otdel'nye zakonodatel'nye akty Rossiyskoy Federatsii v chasti utochneniya poryadka obrabotki personal'nykh dannykh v informatsionno-telekommunikatsionnykh setyakh"* [Federal Law No. 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Procedure for Processing Personal Data in Information and Telecommunication Networks"]. http://publication.pravo.gov.ru/Document/View/0001201407220042

43. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (2019). *Federal'nyy zakon N 90-FZ "O vnesenii izmeneniy v Federal'nyy zakon 'O svyazi' i Federal'nyy zakon 'Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii'"* [Federal Law No. 90-FZ "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Protection of Information'"]. https://www.consultant.ru/document/cons_doc_LAW_323815/

44. Sovet Federatsii Federal′nogo Sobraniya Rossiyskoy Federatsii. (2003). *Federal'nyy zakon N 126-FZ "O svyazi"* [Federal Law No. 126-FZ "On Communications"]. https://www.consultant.ru/document/cons_doc_LAW_43224/

45. Sudebnyy uchastok No. 101 Zamoskvoretskogo sudebnogo rayona g. Moskvy. (2022, April 21). *Postanovlenie po delu No. 05-0413/101/2022* [Decision No. 05-0413/101/2022].

46. Sudebnyy uchastok No. 348 Savyolovskogo sudebnogo rayona g. Moskvy. (2023, June 27). *Postanovlenie po delu No. 05-0612/348/2023* [Decision No. 05-0612/348/2023].

47. Sudebnyy uchastok No. 374 Taganskogo sudebnogo rayona g. Moskvy. (2023, March 1). *Postanovlenie po delu No. 05-0195/374/2023* [Decision No. 05-0195/374/2023].

48. Sudebnyy uchastok No. 387 Basmannogo sudebnogo rayona g. Moskvy. (2023, May 10). *Postanovlenie po delu No. 05-0463/387/2023* [Decision No. 05-0463/387/2023].

49. Sudebnyy uchastok No. 398 Zamoskvoretskogo sudebnogo rayona g. Moskvy. (2023, April 27). *Postanovlenie po delu No. 05-0436/398/2023* [Decision No. 05-0436/398/2023].

50. Sudebnyy uchastok No. 422 Taganskogo sudebnogo rayona g. Moskvy. (2022, July 28). *Postanovlenie po delu No. 05-1344/422/2022* [Decision No. 05-1344/422/2022].

51. Sudebnyy uchastok No. 425 Khamovnicheskogo sudebnogo rayona g. Moskvy. (2022, December 12). *Postanovlenie po delu No. 05-1728/425/2022* [Decision No. 05-1728/425/2022].

52. Sverdlovskiy oblastnoy sud. (2019, September 19). *Apellyatsionnoye opredeleniye No. 33-15137/2019* [Appellate Ruling No. 33-15137/2019]. https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SOUR&n=248543

53. Tsentral′nyy bank Rossiyskoy Federatsii. (2009, September 14). *Pis'mo No. 23-5-2-5/1914 v Ministerstvo svyazi i massovykh kommunikatsiy Rossiyskoy Federatsii* [Letter No. 23-5-2-5/1914 to the Ministry of Communications and Mass Media of the Russian Federation].

54. Tsentral′nyy komitet KPSS. (1955). *Postanovlenie Tsentral'nogo komiteta KPSS* [Resolution of the Central Committee of the CPSU].

55. Tsentral′nyy komitet VKP(b). (1936). *Polozhenie o provedenii vsesoyuznoy perepisi naseleniya 1936 goda. Instruktsiya k zapolneniyu perepisnogo lista* [Regulation on Conducting the All-Union Population Census of 1936. Instruction for Completing the Census Form]. https://istmat.org/files/uploads/50577/rgae_1562.329.143_l.25-35.pdf

56. Upravlenie Rospotrebnadzora po gorodu Moskve. (2018). *Itogi 1 polugodiya 2018 goda* [Results of the First Half of 2018]. http://77.rospotrebnadzor.ru/index.php/napravlenie/zpp/6402-upravlenie-rospotrebnadzora-po-g-moskve-zashchishchaet-prav-potrebitelej-itogi-1-polugodiya-2018-goda

57. Verkhovnyy Sovet RSFSR. (1961). *Ugolovnyy kodeks RSFSR* [Criminal Code of the RSFSR]. https://base.garant.ru/57412177/

58. Verkhovnyy Sovet SSSR. (1977). *Konstitutsiya (Osnovnoy zakon) Soyuza Sovetskikh Sotsialisticheskikh Respublik* [Constitution (Fundamental Law) of the USSR]. https://www.marxists.org/history/ussr/government/constitution/1977/constitution-ussr-1977.pdf

59. Verkhovnyy Sud Rossiyskoy Federatsii. (2020). *Opredelenie Sudebnoy kollegii po grazhdanskim delam ot 14.07.2020 N 58-KG20-2* [Ruling of the Judicial Collegium for Civil Cases of 14 July 2020 No. 58-KG20-2]. https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-grazhdanskim-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-14072020-n-58-kg20-2/

60. Verkhovnyy Sud Rossiyskoy Federatsii. (2023, July 21). *Opredeleniye No. 305-ES23-12160 po delu No. A40-139096/2022* [Ruling No. 305-ES23-12160 In re No. A40-139096/2022].

61. Vsenarodnoye golosovaniye (referendum). (1993). *Konstitutsiya Rossiyskoy Federatsii* [Constitution of the Russian Federation]. http://www.constitution.ru/en/10003000-01.htm

62. Vserossiyskiy Tsentral′nyy Ispolnitel′nyy Komitet (VTsIK). (1926). *Ugolovnyy kodeks RSFSR* [Criminal Code of the RSFSR]. https://docs.cntd.ru/document/901757374

63. Vserossiyskiy Tsentral′nyy Ispolnitel′nyy Komitet. (1926). Ugolovnyy kodeks RSFSR [Criminal Code of the RSFSR]. http://museumreforms.ru/node/13973

64. Vtoroy kassatsionnyy sud obshchey yurisdiktsii. (2022, February 11). *Postanovleniye po delu No. 16-707/2022* [Decision In re No. 16-707/2022].

65. Vtoroy kassatsionnyy sud obshchey yurisdiktsii. (2022, September 23). *Postanovlenie po delu No. 16-4474/2022* [Decision In re No. 16-4474/2022].

66. Zyuzinskiy rayonnyy sud (Gorod Moskva). (2023, April 24). *Resheniye po delu No. 02-1758/2023 [M-8517/2022]* [Decision In re No. 02-1758/2023 [M-8517/2022]].

c. Europe

1. Bundesgerichtshof. (2025). *Urteil VI ZR 109/23* [Judgment VI ZR 109/23]. https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=28.01.2025&Aktenzeichen=VI%20ZR%20109/23

2. Bundesgerichtshof. (2025). *Urteil VI ZR 183/22* [Judgment VI ZR 183/22]. https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=28.01.2025&Aktenzeichen=VI%20ZR%20183/22

3. Bundesverfassungsgericht. (1983). *Urteil des Ersten Senats – Volkszählungsurteil 1 BvR 209/83 et al.* [Judgment of the First Senate – Census Act Case 1 BvR 209/83 et al.]. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

4. Bundesverfassungsgericht. (2010). *Beschluss des Ersten Senats zur Verfassungsmäßigkeit der Vorratsdatenspeicherung 1 BvR 256/08 et al.* [Order of the

First Senate on the constitutionality of data retention 1 BvR 256/08 et al.]. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html

5. Bundesverfassungsgericht. (2020). *Beschluss des Ersten Senats – Anforderungen an die Vorratsdatenspeicherung 1 BvR 2835/17* [Order of the First Senate – Requirements for data retention 1 BvR 2835/17]. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html

6. Conseil constitutionnel. (2018). *Décision No. 2018-765 DC (Loi relative à la protection des données personnelles)* [Law on the Protection of Personal Data). https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm

7. Corps législatif. (1804). *Code civil des Français* [French Civil Code]. https://www.fd.ulisboa.pt/wp-content/uploads/2014/12/Codigo-Civil-Frances-French-Civil-Code-english-version.pdf

8. Council of Europe, Committee of Ministers. (1973). *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*. https://rm.coe.int/1680502830

9. Council of Europe, Committee of Ministers. (1974). *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. https://rm.coe.int/16804d1c51

10. Council of Europe. (1950). *European Convention for the Protection of Human Rights and Fundamental Freedoms* (as amended by Protocols Nos. 11, 14 and 15; supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16). https://www.echr.coe.int/documents/d/echr/convention_ENG

11. Council of Europe. (1968, January 31). *Parliamentary Assembly Recommendation 509 on human rights and modern scientific and technological developments.* https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14546&lang=en

12. Council of Europe. (1974). *Resolution (74) 29 on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Public Sector*. https://rm.coe.int/16804d1c51

13. Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (No. 108). https://rm.coe.int/1680078b37

14. Court of Justice of the European Union. (2010). *Volker und Markus Schecke GbR v. Land Hessen & Hartmut Eifert v. Land Hessen* (Joined Cases C-92/09 & C-93/09). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62009CJ0092

15. Court of Justice of the European Union. (2014). *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (Joined Cases C-293/12 and C-594/12).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293

16. Court of Justice of the European Union. (2014). *Google Spain SL & Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/12).https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131

17. Court of Justice of the European Union. (2014). *YS v. Minister voor Immigratie, Integratie en Asiel & Minister voor Immigratie, Integratie en Asiel v. M & S* (Joined Cases C-141/12 & C-372/12). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0141

18. Court of Justice of the European Union. (2015). *Maximillian Schrems v. Data Protection Commissioner* (Case C-362/14). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362

19. Court of Justice of the European Union. (2017). *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA "Rīgas satiksme "* (Case C-13/16). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0013

20. Court of Justice of the European Union. (2019). *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV* (Case C-40/17). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0040

21. Court of Justice of the European Union. (2019). *GC and Others v. Commission nationale de l'informatique et des libertés (CNIL)* (C-136/17). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0136

22. Court of Justice of the European Union. (2020). *Data Protection Commissioner v Facebook Ireland Ltd & Maximillian Schrems* (C-311/18). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

23. Court of Justice of the European Union. (2020). *Orange Romania SA v. Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)* (Case C-61/19). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62019CC0061

24. Court of Justice of the European Union. (2022). *Österreichische Post AG, Opinion of Advocate General Campos Sánchez-Bordona* (Case C-300/21). https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=266842&doclang=EN

25. Court of Justice of the European Union. (2023). *Meta Platforms Inc & Others v. Bundeskartellamt* (Case C-252/21). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0252

26. Court of Justice of the European Union. (2023). *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v. Valstybinė duomenų apsaugos inspekcija* (Case C-683/21). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0683

27. Court of Justice of the European Union. (2023). *UI v. Österreichische Post AG* (Case C-300/21). https://infocuria.curia.europa.eu/tabs/document?source=document&docid=280623&doclang=EN

28. Court of Justice of the European Union. (2023). *VB v. Natsionalna agentsia za prihodite* (Case C-340/21). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0340

29. Court of Justice of the European Union. (2024). *JU and SO v. Scalable Capital GmbH* (Joined Cases C-182/22 & C-189/22). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0182

30. Court of Justice of the European Union. (2025). *Anklagemyndigheden v. ILVA A/S* (Case C-383/23). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62023CJ0383

31. Court of Justice of the European Union. (2025). *CK v. Magistrat der Stadt Wien* (Case C-203/22). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0203

32. Court of Justice of the European Union. (2025). *European Data Protection Supervisor (EDPS) v. Single Resolution Board (SRB)* (Case C-413/23 P). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0413

33. Deutscher Bundestag. (1968). *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz)* [Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (Article 10 Act)]. https://opinioiuris.de/kommentar/gg/10

34. European Commission. (2010, November 4). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union* (COM (2010) 609 final). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

35. European Commission. (2012). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (COM (2012) 11, 2012/0011(COD)). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011

36. European Commission. (2013). *Commission Regulation (EU) No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC*. https://data.europa.eu/eli/reg/2013/611/oj

37. European Commission. (2019, January 23). *European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows* [Press release No. IP/19/421]. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_421

38. European Commission. (2023). *Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework* (OJ L 231, 20.9.2023, pp. 118–229). https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj/eng

39. European Commission. (2023). *Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679* (COM (2023) 348 final, 2023/0202(COD)). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0348

40. European Commission. (2025). *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557* (COM (2025) 837). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837

41. European Court of Human Rights. (1987). *Leander v. Sweden, Application* (No. 9248/81). https://hudoc.echr.coe.int/eng?i=001-57519

42. European Court of Human Rights. (2000). *Rotaru v. Romania, Application* (No. 28341/95). https://hudoc.echr.coe.int/eng?i=001-58586

43. European Court of Human Rights. (2006). *Segerstedt-Wiberg & Others v. Sweden* (Applications Nos. 62332/00 & 67021/01). https://hudoc.echr.coe.int/eng

44. European Court of Human Rights. (2012). *M.M. v. the United Kingdom* (Application No. 24029/07). https://hudoc.echr.coe.int/eng?i=001-114517

45. European Court of Human Rights. (2015). *Roman Zakharov v. Russia* (Application No. 47143/06). https://hudoc.echr.coe.int/eng

46. European Court of Human Rights. (2017). *Aycaguer v. France* (Application No. 8806/12). https://hudoc.echr.coe.int/eng?i=001-175007

47. European Court of Human Rights. (2017). *Satakunnan Markkinapörssi Oy & Satamedia Oy v. Finland* (Application No. 931/13). https://hudoc.echr.coe.int/fre?i=001-175121

48. European Court of Human Rights. (2018). *Big Brother Watch & Others v. The United Kingdom* (Application Nos. 58170/13, 62322/14 & 24960/15). https://hudoc.echr.coe.int/eng?i=001-210077

49. European Data Protection Board. (2023, July 18). *Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023*. https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf

50. European Economic Community. (1957). *Treaty establishing the European Economic Community (Treaty of Rome)*. https://eur-lex.europa.eu/eli/treaty/teec/sign/eng

51. European Federation of Data Protection Officers. (2023). *The German Census Judgment of 1983: A landmark judgment turns 40*. https://www.efdpo.eu/wp-content/uploads/2023/12/The-German-Census-Judgement.pdf

52. European Parliament and the Council of the European Union. (2002). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. http://data.europa.eu/eli/dir/2002/58/oj

53. European Parliament and the Council of the European Union. (2018). *Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.* Official Journal of the European Union, L 295, 39–98.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0039.01.ENG

54. European Union. (2006). *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks* (OJ L 105, 13.4.2006, pp. 54–63). https://eur-lex.europa.eu/eli/dir/2006/24/oj

55. European Union. (2012). *Charter of Fundamental Rights of the European Union* (OJ C 326, 26.10.2012, pp. 391–407). https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng

56. European Union. (2012). *Consolidated version of the Treaty on the Functioning of the European Union.* Official Journal of the European Union, C 326, 47–390. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

57. European Union. (2016). *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*(General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

58. European Union. (2018). *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons*

with regard to the processing of personal data by the Union institutions, bodies, offices and agencies. https://eur-lex.europa.eu/eli/reg/2018/1725/oj

59. European Union. (2024). *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*. https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng

60. European Union. (2024). *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence* (Artificial Intelligence Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

61. French Parliament. (1978). *Loi No. 78-17 relative à l'informatique, aux fichiers et aux libertés* [Law No. 78-17 on Information Technology, Data Files and Civil Liberties]. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

62. Hessischer Landtag. (1970, October 7). *Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Hessisches Datenschutzgesetz)* [Act on Protection against Misuse of Personal Data in Data Processing (Hessian Data Protection Act)]. Gesetz- und Verordnungsblatt für das Land Hessen. https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-06/HDSIG_digital.pdf

63. High Court of Chancery. (1849). *Prince Albert v. Strange* (EWHC Ch J20 1849). https://privacylibrary.ccgnlud.org/case/prince-albert-vs-strange

64. House of Lords. (1993). *Regina (R) v. Brown* (2 All ER 75; UKHL 19). https://opencasebook.org/casebooks/5386-gender-sexuality-and-the-law/resources/5.3-regina-v-brown-1993-2-all-er-75/

65. International Conference of Data Protection and Privacy Commissioners. (1989). *Berlin Resolution*. https://globalprivacyassembly.com/wp-content/uploads/2015/02/11th-ICDPPC-Berlin-1989-Berlin-Resolution.pdf

66. Supreme Court of the United Kingdom. (2021). *Lloyd v. Google LLC* (UKSC 2019/0213). https://www.supremecourt.uk/cases/uksc-2019-0213.html

67. Sveriges Riksdag. (1877). *Statute concerning the Swedish Copyright Act of 1877*. https://www.copyrighthistory.org/cam/pdf/d_1877_1.pdf

68. Sveriges Riksdag. (1973). *Datalag* [Data Act] *(1973:289).* https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalagen-1973289_sfs-1973-289

69. United Kingdom Parliament. (1969, May 6). *Data Surveillance* (HC Deb vol. 783, cc 285–288). https://hansard.parliament.uk/Commons/1969-05-06/debates/98fdc483-159a-4bea-afeb-02cdeec29acd/DataSurveillance

70. United Kingdom Parliament. (2024, March 13). *Digital Markets, Competition and Consumers Bill: Lords debate* (Vol. 836). Hansard. https://hansard.parliament.uk/Lords/2024-03-13/debates/7D63CD77-0842-4100-8592-7E6BEAB72FF3/DigitalMarketsCompetitionAndConsumersBill

71. United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights* (Resolution 2200A (XXI), entered into force 1976).