Department of Political Science

Master's Degree in International Relations

Course of Comparative Public Law

PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT: COMPARATIVE PERSPECTIVES AND THE CHALLENGES OF ARTIFICIAL INTELLIGENCE

Professor Valentina Rita Scotti

SUPERVISOR

Professor Cristina Fasone

CO-SUPERVISOR

Arianna D'Anna - 657152

CANDIDATE

Academic Year 2024/2025

TABLE OF CONTENTS

INTRODUCTION

In the digital age, personal information have become the driving force of the economy, communication, and technological innovation but at the same time one of the most vulnerable areas for the protection of fundamental rights. The ability of new technologies to collect, process, and share personal information on a large scale has reached unprecedented levels: in this context, data protection can no longer be considered a technical or sectoral matter, but an essential safeguard of dignity, autonomy, and democracy, as well as a benchmark of legitimacy for legal institutions.

This thesis aims to examine the protection of personal data as an unalienable right though a comparative approach that highlights different regulatory responses developed at international level. In this perspective, this research will examine personal data protection by comparing the main regulatory models that have emerged worldwide. The analysis will be conducted from a historical, legal, and comparative approach, with the aim of identifying not only common features and divergences between legal systems, but also the consequences that such differences determine in the effective protection of rights. From a methodological perspective, the project will examine legal sources, case law, and soft law instruments, as well as policy documents and institutional initiatives. The comparative research will allow to observe how different legal traditions have responded to the challenge of data protection, offering diverse solutions yet united by the growing relevance of the issue.

The thesis is structured in five chapters.

The first chapter will trace the origins of the right to data protection, beginning with the contribution of Warren and Brandeis and the notion of the *right to be let alone*, before analyzing its evolution in the Italian legal system, through case law and legislative developments. This will be followed by an overview of international landscape and its instruments, from the role of the

United Nations and the Council of Europe to the OECD guidelines.

The second chapter will focus on the European Union model from the preliminary activities of the European Commission and Parliament that led to Directive 95/46/EC and the subsequent consolidation with Article 8 of the Charter of Fundamental Rights of the European Union. It will then analyze the innovations introduced by the General Data Protection Regulation, with particular attention to the fundamental principles of data processing, the rights of data subjects, the role of independent supervisory authorities, and the extraterritorial application of the Regulation.

The third chapter will be dedicated to the United States system, characterized by the absence of a comprehensive federal law and the coexistence of sectoral statutes. It will explore the role of the Federal Trade Commission as the de facto enforcement authority and the emergence of state-level legislation. Special attention will concern the divergences from the European model and to the impact of the *Schrems I* and *Schrems II* judgments, which invalidated the transatlantic data transfer mechanisms Safe Harbor and Privacy Shield, leading up to the new EU–US Data Privacy Framework adopted in 2023.

The fourth chapter will broaden the analysis beyond the Western context by comparing the models of China and Japan. For China, the focus will be on the role of state surveillance and the legislative reforms starting from 2017, culminating in the adoption of the Personal Information Protection Law in 2021. For Japan, the analysis will trace the trajectory that began with the Act on the Protection of Personal Information of 2003 and its subsequent reforms, which ultimately led to the European Commission's 2019 adequacy decision, signaling a significant convergence toward European standards.

In addition to the analysis of regulatory models, the thesis will also address the new challenges posed by artificial intelligence.

The fifth chapter will analyze how systems based on big data, machine learning, and biometrics

affect the right to data protection. It will examine major initiatives at the international level and compare the regulatory strategies adopted in the different geopolitical areas under study. In particular, the chapter will assess the European response through the GDPR and the new AI Act, as well as the approaches taken in the United States, China, and Japan, in order to highlight similarities, divergences, and common challenges.

The conclusions will draw together the findings of the analysis, emphasizing that personal data protection today constitutes a key area of confrontation between legal systems, governance models, and visions of the relationship between technology and rights. They will illustrate that, despite the different approaches, the centrality of data protection is increasingly affirmed as an indispensable element for building an international legal order grounded in the respect for human dignity in the digital age.

Chapter 1

Defining the Right to Personal Data Protection:

Evolution, Concept, and Legal Framework

1.1 At the origins of Data Protection: The Right to Be Let Alone

The protection of personal data has progressively become a pillar of fundamental rights in modern legal systems. The recognition of this right, however, is the outcome of a long historical evolution influences by technological advancements, shifting societal values, and the growing significance of information in both public and private spheres. The imperative to safeguard personal data has deep historical roots, initially emerging from the broader concept of privacy and the protection of personal correspondence, and later evolving into an autonomous right in response to the advent of automated data processing and the increasing digitalization of society.

The contemporary notion of privacy, particularly in its current form as information privacy, represents the most recent conceptual development of privacy itself, stimulated and necessitated by technological and social progress. Before the proliferation of computing technologies, which enables the rapid collection, processing, and dissemination of vast amounts of personal data for diverse purposes, the right to privacy largely coincided with "*the right to be left alone*", a principle rooted in the American legal tradition. This early understanding of privacy focused primarily on

an individual's entitlement to a private sphere shielded from external interference. Although originating in the United States, this conception of privacy was later embraced within European legal traditions, where it prevailed until the demands of technologically advanced societies required its reconsideration and reconceptualization[1].

In the mid-19th century American legal and social landscape, privacy was not conceived as an inherent natural right of every individual. Rather, it was understood as a privilege. Privacy, therefore, was fully recognized only as a legal entitlement, derived from a deliberative legislative act. It was within this evolving legal framework that concerns about privacy began to surface in the legal thought. In 1888, Judge Thomas Cooley, in his treatise on tort law, examined privacy as an essential component of personal security. Though he approached the subject within the context of legal wrongs rather than as an independent personal right, he introduced a phrase that would later become central to privacy discussions, describing privacy as "*a right of complete immunity: to be let alone*". While Cooley's formulation was not yet fully developed as a legal doctrine, it captured a fundamental idea that would soon gain traction.

Two years later, two prominent jurists, Samuel Warren and Louis Brandeis, built upon this emerging concept as they turned their attention to a series of emerging threats to individual privacy, particularly those posed by new technologies such as photography. These innovations enabled the widespread dissemination of private aspect of individuals' lives to the public, which has previously remained confined to the personal domain[2]. The aristocracy, which had long considered itself untouchable and deserving of deference from lower social classes, felt particularly threatened by technological advancements that eroded this perceived status. The rise of sensationalist journalism

[1] L Miglietti, Profili storico-comparativi del diritto alla privacy (2014) *Diritto Comparati – Comparare i diritti fondamentali in Europa* 3.
[2] M Iaselli and S Gorla, *Storia della privacy* (2015) 28.

further exacerbated this tension, as the public exposure of the elite's activities and vices was seen by them as an unjustified and aggressive intrusion[3]. At the time, the U.S. legal system in the 19th century already provided certain protections against the unauthorized publication of manuscripts and artistic works, primarily through copyright and unpublished rights doctrine. However, these mechanism only safeguarded the form of expression rather than preventing the publication of private facts. As a result, the mental distress and emotional harm caused by the disclosure of personal letters or private events were beyond the scope of existing copyright protections[4]. Indeed, copyright law protected intangible assets such as paintings, sculptures, musical compositions, and theatrical works, based on the same principle as private property[5].

In response, drawing from the flexibility of common law and emphasizing its adaptability to evolving social needs, Warren and Brandeis published their landmark article, "*The right to Privacy"*, which triggered a systematic and enduring legal discourse on the concept of privacy itself. Their work marked a watershed moment in privacy law, as it was the first comprehensive legal treatise to advocate for privacy as an autonomous legal right within American law, defined as "*the right to be let alone*". Warren and Brandeis' ultimate goal was to ensure that the law protected not only material interests, but also the more intangible and spiritual dimensions of human life[6]: they rejected the notion that its protection should depend solely on the potential for profit. According to them, what safeguarded writings and other personal creations was not merely the principle of private property, understood as protection from theft or physical appropriation, but

[3] M Surace, Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà (2005) *ADIR- L'altro diritto.*
[4] P Guarda and G Bincoletto, *Diritto comparato alla privacy* (Università degli Studi di Trento 2016) 21.
[5] M Surace (n 3).
[6] L Miglietti (n 1) 3.

rather the principle of personal inviolability[7]. Their approach represented a significant departure from traditional property-based legal reasoning, placing greater emphasis on the inviolability of the person itself. Their true innovation laid in their systemic critique of existing legal doctrines – such as property rights, breach of confidence, and physical trespass – all of which were deemed inadequate for safeguarding the evolving concept of privacy. Prior to this, the need to protect personal privacy, although increasingly felt within society, struggled to find clear legal recognition: for example, legal scholars often attempted to subsume privacy concerns under existing categories, such as the right to reputation or honor. The jurists argued that physical intrusion was no longer a necessary precondition for legal protection, shifting the focus from external acts to the value of personal autonomy itself. This person-centered approach, which placed individual dignity and autonomy at the core of privacy protection, anticipated many of the human dignity-based theories that would later emerge in European privacy law and international human rights discourse[8].

According to the authors, privacy was not to be regarded as an absolute right and had certain limitations. The first limitation concerned the publication of information deemed of public interest: facts of societal relevance could not remain confidential. In other words, the confidentiality of an act depended on the nature of the person involved: id it was a private individual, disclosure was not permitted; on the other hand, if the individual was a public figure or held a position of societal importance, publication was lawful. Therefore, the right to privacy protected what is known as private life. The second limitation identified by the jurists pertained to the relationship between privacy and defamation laws. The right to be left lone did not prevent the dissemination of private information if its publication occurred in circumstances permitted by common law. Thus, the right to privacy was not violated if facts were made public within judicial proceedings, by legislative

[7] M Surace (n 3).
[8] L Miglietti (n 1) 4.

bodies, or in other public contexts where disclosure was allowed by current laws. The authors also identified a third limitation: it was not possible to seek compensation for privacy violations in cases of oral communication that did not cause specific and demonstrable harm. This limitation was intended to protect freedom of expression. Finally, the right to privacy could not be invoked against the publication of facts made public by the individuals themselves or disclosed with their consent. Moreover, in cases where publication occurred without authorization, the truth of the facts or the absence of malice on the part of journalists or published did not constitute a valid justification. Regarding remedies for privacy violations, the jurist argued that the legal system should allow for civil actions for damages, aimed at obtaining monetary compensation, or an injunction, which is a court order to prevent further violations.

Following the publication of this article, while the concept of inviolable personality did not again significant traction in the U.S. legal system, the thoughts of the jurists had a profound impact on legal thought, leading to the recognition and creation of a specific legal action violations within common law[9].

1.2 Personal Data Protection as a Fundamental Right

As a cornerstone of modern fundamental rights frameworks, once considered a technical or sectorial issue, data protection now constitutes a distinct and autonomous right, closely linked to the right to privacy, but also extending beyond it. The increasing digitalization of society, the pervasive role of technology, and the rise of data-driven decision-making have highlighted the necessity of ensuring legal safeguards over the collection, processing, and dissemination of personal information. Recognized today as a fundamental right both at national and supranational

[9] P Guarda and G Bincoletto (n 4) 22-23.

level, the right to personal data protection plays a crucial role in preserving individual dignity, autonomy, and democratic oversight.

1.2.1 The evolution of the Right to Privacy in the Italian legal system

The recognition of the right to privacy and the study of the legal instruments suitable for its protection in Italy have followed a progressive codification path, characterized not only, as is usually the case in the development of rights, by a fruitful dialogue between judicial interpretation and the legislative choices of the national legislator, but above all by the constant interplay between the national level and the European dimension. This supranational framework complements, intertwines with, and ultimately integrates into the domestic constitutional system[10]. The legal doctrine and jurisprudence have played a fundamental role in addressing the absence of a structured body of legal rules capable of providing a unified definition of this right. Given the lack of a general provision explicitly defining the right to privacy within the Italian legal system, one of the principal challenges has been the identification of a normative basis from which to derive the overarching protection of the interest in confidentiality. The Italian Constitution does not expressly regulate the right to private life protection. This omission is mainly due to the fact that privacy only gained increasing prominence within legal science and the Italian legal system from the 1960s onward, thus after the Constitution was enacted. In this context, the progressive recognition of privacy rights can be attributed to an initial doctrinal evolution, followed by significant jurisprudential developments, particularly through the decisions of the highest Court of Appeal.

The extensive doctrinal debate that has developed, characterized by the confrontation between

[10] L Califano, V Fiorillo and Federico Galli, *La protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale* (Giappichelli 2023) 15.

different theoretical approaches, originated within the field of private law doctrine in the 1930s. In 1937, Adolfo Ravà wrote that individuals should be guaranteed "*a certain sphere, relating to the most sensitive and intimate aspects of their being and their activity, into which no one should be allowed to interfere or intrude*"[11]. According to the framework reconstructed by Ravà, the right to privacy was established as a general right with multiple implications. Through an analogical reasoning approach[12] to legal provisions already present in the system[13], he reconstructed the right to privacy by adopting an interpretative path grounded in the protection of the fundamental attributes of the person. Precisely because they are linked to the very essence of personality and are considered essential elements for ensuring the full realization of the individual, these attributes, including privacy, deserved protection even in the absence of an explicit legislative provision. The existence of specific legal norms protecting particular aspects of the individual (such as image and correspondence) did not preclude the recognition of a general principle; rather, it responded to legislative technique considerations. Through this approach, the legislator chose to regulate certain rights in greater detail without denying the existence of broader and more general protection for the individual and their private sphere. By employing an analogical reasoning approach on existing legal provisions, Ravà reconstructs the right to privacy through an interpretative process rooted in the protection of the fundamental attributes of the person. Since these attributes are intrinsically linked to the very essence of individual personality and are considered essential for the full realization of the person, they warrant legal protection even in the absence of an explicit legislative

[11] M Iaselli and S Gorla (n 2) 49.
[12] This interpretative process is grounded in Article 12 of the Preliminary Provisions to the Civil Code (Preleggi), which allows for the application of analogy and the recourse to the general principles of the legal system to fill potential legislative gaps.
[13] Including Article 10 of the 1942 Civil Code, Articles 96 and 97 of the 1941 Copyright Law, as well as certain criminal provisions from the Rocco Code (Articles 616-623).

provision. The existence of specific legal norms safeguarding particular aspects of individual identity, such as image and correspondence, does not preclude the recognition of a broader general principle. Rather, it reflects a legislative technique through which the lawmaker has chosen to regulate certain rights in a more detailed manner without thereby negating the existence of a more extensive and overarching protection of the individual and their private sphere.

Ravà's approach was opposed by Pugliese's doctrine, which denied the possibility of recognizing this right through analogy. Pugliese argued that existing legal norms protected personality as a whole rather than merely safeguarding privacy. Moreover, he maintained that extending exceptional provisions by analogy, such as those limiting freedom of expression, would violate the prohibition set forth in Article 14 of the Preliminary Provisions of the Civil Code. A different perspective was offered by De Cupis, who recognized a plurality of personality rights, each possessing its own autonomy and deriving from a common need to protect the individual. However, this pluralistic view was later challenged by part of the doctrine in favor of a monistic conception, as advocated by Giampiccolo. According to this view, a single general right of personality existed, from which specific protections for image, domicile, and correspondence would derive. Inspired by the German model and later adopted by constitutional jurisprudence, this approach was considered capable of ensuring greater flexibility and adaptability to new forms of infringement upon the private sphere[14].

In its early stages, the legal doctrine encountered further obstacles in recognizing full protection for the right to privacy, particularly following the first ruling by the Court of Cassation on the matter, which explicitly denied the existence of such a right.

The first judicial decision on this issue dates back to 1953 and was issued by the Tribunal of Rome.

[14] M Surace (n 3).

In this ruling, the court affirmed the existence of the right to privacy, understood as the prohibition of any external interference in an individual's private sphere and any indiscretion regarding personal facts or behaviors not intended for public disclosure[15]. The Tribunal, while recognizing the right to privacy, highlighted the possibility of applying the legislation on image rights by analogy.

However, in 1956, the Highest Court of Appeal, ruling on the same case previously addressed by the Tribunal of Rome three years earlier, stated that no legal provision established a general and absolute protection of private life. The Court clarified that privacy was not protected unless the agent's actions, by harming a person's honor, dignity, or reputation, fell within the scope of an unlawful act[16]. According to the highest court of appeal, the issue could be resolved without the need to introduce new legal concepts, relying instead on the general principle of *neminem laedere*, as specified in Article 2043 of the Civil Code[17].

In 1963, with a ruling[18], the Highest Court revisited the issue, modifying its initial stance on the right to privacy. The court stated that, although no autonomous right to privacy existed, the unauthorized publication of personal data constituted a violation of the absolute right of personality, which safeguards individual self-determination and dignity, unless there was an overriding public interest.

[15] The case concerned an issue of freedom of artistic expression. The movie *Leggenda di una voce*, which depicted the life of the tenor Enrico Caruso, had been produced without the consent of his rightful heirs. They objected to the dissemination of information about the singer, some of which was inaccurate and allegedly violated his right to privacy.

[16] G Bruno, Diritto alla riservatezza: nascita ed evoluzione giurisprudenziale in Italia (2024) *Filodiritto.*

[17] M Surace (n 3).

[18] The relatives of Claretta Petacci, known for her relationship with Benito Mussolini, initiated legal action against the weekly magazine *Tempo* for publishing numerous articles that revealed detailed aspects of her romantic life with the Duce.

Finally, it was with ruling no. 2129 of 1975[19] that the highest court of appeal definitively overturned its previous position, providing a clear and comprehensive definition of an independent right to privacy. In this ruling, the Court established that the legal system recognizes the right to privacy, understood as the protection of situations and events of a strictly personal and family nature, even when they occur outside the domestic sphere, provided that such facts do not hold socially relevant interest for third parties. Furthermore, interferences, even if carried out through lawful means, for purposes beyond mere speculation, and without harming honor, reputation, or dignity, cannot be justified unless supported by an overriding public interest[20]. The Court identified a dual foundation, both implicit and explicit, for the right to privacy. On one hand, it recognized this right as implicitly derived from the set of constitutional and ordinary norms that protect specific aspects of the individual and that, as a consequence, cannot disregard the protection of their private sphere. On the other hand, it explicitly identified privacy in all provisions, particularly in special laws, that make direct reference to private life or, more specifically, to confidentiality. By doing so, the court provided a comprehensive interpretation of Article 2 of the Constitution, affirming that it also encompasses the right to privacy. This right is reflected in all expressions that refer to the protection of a personal and family dimension, ensuring individual intimacy even in relation to certain social interactions. It applies to all private moments that unfold within an ideal sphere of confidentiality, which does not necessarily coincide with physical spaces traditionally considered personal retreats[21]. With this decision, the right to privacy gained full recognition in Italian jurisprudence,

[19] The so-called *Soraya Case* involved the former Persian Empress Soraya Esfandiari, who had been repudiated and forced into exile. Photographs depicting her in intimate moments with a man, taken inside her villa in Rome, emerged and became the subject of public controversy.
[20] G Bruno (n 16).
[21] L Esposito, *L'evoluzione del diritto alla riservatezza nel panorama giurisprudenziale italiano ed europeo* (Tesi di laurea magistrale, LUISS Guido Carli, 2018) 28.

and the ruling became a leading case[22].

The progressive legal recognition of the right to privacy reached a turning point with the enactment of Law No. 675 of 1996[23], adopted in implementation of Directive 95/46/EC, which required European Union member states to regulate the processing of personal data in a clear and uniform manner. The directive recognized personal data as tools serving the individual and ensured the protection of their freedom and fundamental rights. Although Italy was complying with a European obligation, it did not merely transpose the directive but expanded the scope of protection by introducing innovative elements. Among these were the explicit reference to personal dignity and the extension of protection to personal identity, anticipating some of the later regulatory developments at the European level[24].

An important innovation introduced by Law No. 675/96 in Article 30 was the establishment of the Data Protection Authority (*Garante per la protezione dei dati personali*), an independent body tasked with overseeing the implementation of privacy legislation. This collegial authority, composed of four members elected by Parliament, operates with full autonomy and independence, serving a four-year term, which may be renewed only once. Its primary function is to ensure that the processing of personal data complies with legal provisions. It does so by monitoring data processing operations, handling reports and complaints, and issuing measures to rectify any violations. Additionally, the Garante is responsible for promoting awareness of privacy regulations, ensuring data security, prohibiting unlawful or improper data processing, and advising the government on legislative measures necessary to adapt the legal framework to technological and

[22] G Bruno (n 16).
[23] Law No. 675 of December 31, 1996, titled 'Protection of Individuals and Other Subjects with Regard to the Processing of Personal Data' (Italy).
[24] M Surace (n 3).

social developments[25].

The Law No. 675/96 had a significant impact in two main areas. On one hand, it codified two rights originally developed through jurisprudence: the right to privacy and the right to personal identity. On the other hand, it reinforced the principle that the protection of personal data is not limited to safeguarding the private sphere but also serves as a defense against potential distortions of social identity and the improper use of personal information in an increasingly digitalized world. The Italian legal system thus emphasized a dynamic rather than a static concept of privacy, redefining it as the right to informational self-determination. This approach grants individuals control over the use of their personal data, preventing discrimination and abuse while shaping a multifunctional right. Privacy is no longer conceived merely as the right to be left alone but rather as an active and dynamic right that allows individuals to access their personal information, verify its accuracy, correct errors, and monitor its use over time.

This evolution was further reinforced by Legislative Decree No. 196/2003, known as the Personal Data Protection Code, which formally established data protection as an autonomous right distinct from privacy in Articles 1 and 2. It recognized the right to personal data protection independently from the safeguarding of an individual's intimate sphere, family life, or social image. From this perspective, the right to privacy in Italy has moved beyond the traditional notion of merely protecting individual intimacy. It has evolved into a fundamental guarantee of personal freedom and dignity, especially in a social and economic environment increasingly driven by the management and circulation of digital information[26].

[25] As regulated by Article 31 of the aforementioned law.
[26] M Surace (n 3).

1.2.2 The protection of data in the International legal system

The international legal framework on data protection is shaped by the normative efforts of several international organizations. In particular, it is possible to identify the contributions of three major actors: the United Nations, the Council of Europe, and the Organization for Economic Co-operation and Development (OECD), each of which has played a crucial role in the development of international standards on personal data protection.

1.2.2.1 The role of the United Nations

At the international level, there is currently no multilateral treaty specifically devoted to the protection of personal data. Nonetheless, a number of international legal instruments may be identified which embody core principles pertaining to data protection.

Within the framework of the United Nations, the normative development of personal data protection may be traced chronologically through the adoption of various legal instruments. The first fundamental legal instrument in this regard is the Universal Declaration of Human Rights, adopted in 1948, which, under Article 12, enshrines the right to privacy:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".*

This provision prohibits any arbitrary or unlawful interference with an individual's private life, family, home, or correspondence, and guarantees the individual's right to legal protection against attacks upon their honor and reputation.

These principles were subsequently reiterated and reinforced in the 1966 International Covenant on Civil and Political Rights (ICCPR), which, in Article 17, reaffirms the right to protection against

arbitrary or unlawful interference with one's privacy, family, home, or correspondence, as well as the right to be safeguarded by law against such intrusions:

> *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".*

A significant interpretation of this article was provided in 1988 through General Comment No. 16 by the United Nations Human Rights Committee, which clarified that the right to privacy also encompasses the protection of personal data. In particular, it was established that any restriction of this right may be justified solely where the collection of personal data is deemed essential to the interests of society. However, in order for such limitations to be legitimate, both the collection and retention of data must be governed by specific legislation, which must ensure clearly defined limits and transparent conditions of use. Moreover, paragraph 10 of General Comment No. 16 emphasizes that every individual must have the right to access, correct, or delete data that is inaccurate or has been collected in violation of applicable legal provisions[27].

In the same year, the United Nations published the report entitled "*Guidelines for the Regulation of Computerized Personal Data Files*", drafted by Special Rapporteur Louis Joinet for the Sub-Commission on Prevention of Discrimination and Protection of Minorities[28]. This document represents one of the earliest international initiatives aimed at regulating the management of computerized personal data, in response to the growing digitalization of the time. It contributed to

[27] E Carpanelli, A Favi, M Inglese and L Pineschi, *La protezione dei dati nel diritto internazionale ed europeo: Il ruolo delle corti nazionali nell'applicazione della Carta dei Diritti Fondamentali* (Università di Parma, Centro Studi in Affari Europei e Internazionali (CSEIA)) 3.

[28] United Nations Economic and Social Council. Guidelines for the Regulation of Computerized Personal Data Files: Final Report Submitted by Mr. Louis Joinet, Special Rapporteur (1988).

the development of the first international standards on personal data protection, establishing that the guidelines were to apply to both the public and private sectors, with a primary focus on safeguarding the data of natural persons[29]. The guidelines set forth in the report articulated fundamental principles for the protection of privacy, including the lawfulness of data collection, the right of access and rectification, protection against discrimination, as well as security and transparency in the processing of personal information[30].

A key element of the document was its emphasis on the responsibility of international organizations in managing archives containing sensitive data, particularly in relation to human rights. Many such organizations had initiated efforts to internally regulate the processing of personal data. Interpol (ICPO), for instance, had adopted specific guidelines for data protection within its archives, with oversight entrusted to an independent commission composed of external members. Other organizations, such as UNHCR, UNESCO, IAEA, OECD, and the Council of Europe, developed internal regulations aimed at safeguarding the personal data of their employees as well as individuals involved in their programs – for example, refugees in the case of UNHCR. Likewise, Amnesty International and the International Committee of the Red Cross undertook initiatives to promote international standards on data protection, with particular attention to human rights and humanitarian activities, advocating for the inclusion of a "*humanitarian clause*" to ensure enhanced protection for the data of vulnerable individuals[31]. One issue that remained the subject of debate in 1988 concerned the appropriate entity to oversee the implementation of such guidelines within international organizations. Some experts, including Special Rapporteur Louis Joinet, advocated for the establishment of an independent supervisory body to ensure greater impartiality in

[29] United Nations Economic and Social Council (28) 7.
[30] Ibid. 4-6.
[31] Ibid. 8-9.

monitoring compliance with data protection standards, similar to the external oversight mechanism adopted by Interpol. Others, by contrast, maintained that responsibility for data protection should remain within the internal administrative bodies of each organization[32].

The principles set forth in the 1988 report constituted a fundamental starting point for the development of personal data protection policies.

Two years later, in 1990, the United Nations formalized these recommendations through General Assembly Resolution 45/95, thereby officially adopting the "*Guidelines for the Regulation of Computerized Personal Data Files*"[33]. This new document retained the fundamental principles outlined in Joinet's report, while reinforcing them within a more structured regulatory framework intended for implementation by Member States.

In particular, the text develops by reaffirming nine principles already present in the earlier version:

- *Principle of lawfulness and fairness*: Data must be collected and processed in a fair and lawful manner.
- *Principle of accuracy*: Data must be kept up to date and verified to ensure its accuracy.
- *Principle of purpose specification*: Data must be collected for a legitimate and explicitly stated purpose.
- *Principle of data subject access*: Every individual has the right to access, rectify, or erase their personal data.

[32] Ibid.

[33] United Nations General Assembly, Guidelines for the Regulation of Computerized Personal Data Files Resolution 45/95 (n 1990).

- *Principle of non-discrimination*: The collection of data likely to result in discrimination based on ethnic origin, religion, political opinions, or other sensitive characteristics is prohibited.
- *Power to make exceptions*: Exceptions are permitted only when necessary for reasons of national security, public order, or the protection of the rights and freedoms of others.
- *Principle of security*: Appropriate measures must be adopted to prevent accidental loss, unauthorized access, or fraudulent use of data.
- *Supervision and sanctions*: The establishment of oversight authorities is required, endowed with powers of supervision and the ability to impose sanctions in cases of non-compliance.
- *Transborder data flows*: The transfer of data across borders must be regulated to ensure an adequate level of privacy protection[34].

Compared to the 1988 version, the 1990 Guidelines consolidated and strengthened the regulatory framework governing personal data protection, introducing clearer rules on oversight, expanding the scope of application, and formally recognizing the principle of the *Humanitarian Clause*. While the 1988 document set out the fundamental principles for the regulation of personal data in both the public and private sectors, distinguishing between internal files and external files, it left unresolved the issue of supervisory authority. By contrast, the 1990 Guidelines clarified that each international organization must designate a competent authority to ensure compliance with the Guidelines, thereby resolving the debate between those advocating for the establishment of an independent supervisionary body and those favoring internal management. Another key distinction concerns the potential applicability of national legislation to international organizations, where not

[34] Ibid. 1-3.

precluded by their headquarters agreements. This provision introduced a greater degree of legal control compared to the 1988 version, which did not directly address this possibility. Moreover, the Humanitarian Clause, which in 1988 had merely been mentioned without specific elaboration, was formally recognized in the 1990 Guidelines, providing for explicit derogations from data protection constraints when the objective is the protection of human rights or the provision of humanitarian assistance. The 1990 document further recommends that national legal systems adopt similar provisions, thereby extending the applicability of the Guidelines not only to international organizations, but also to non-governmental organizations, contributing to the overall strengthening of the personal data protection framework[35].

More recently, in 2013, the United Nations General Assembly adopted a Resolution[36] addressing the issue of privacy in the digital age and the implications of surveillance technologies for the respect of human rights. The document reaffirms the right to privacy, as enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, emphasizing that arbitrary or unlawful interference with private life must be prevented and sanctioned[37]. It further establishes that the rights individuals enjoy offline must also be protected online, particularly the right to personal data protection and the confidentiality of digital communications[38]. Through the Resolution, the General Assembly called upon all States to review and reform their legislation on surveillance, interception, and personal data collection, to ensure compliance with international human rights obligations and it highlighted the necessity of establishing independent oversight mechanisms capable of ensuring transparency and

[35] Ibid.
[36] United Nations General Assembly, Resolution 68/167: The Right to Privacy in the Digital Age, A/RES/68/167 (2014).
[37] Ibid. 1.
[38] Ibid. 2.

accountability in the conduct of state surveillance activities[39].

An important step was the establishment, within the framework of the United Nations, of the mandate of a Special Rapporteur on the right to privacy by the Human Rights Council[40]. In 2018, in his report to the Human Rights Council on the right to privacy[41], Special Rapporteur Joseph A. Cannataci provided a comprehensive analysis of the threats to privacy in the digital age, outlining the actions required to strengthen its protection at the international level. The report emphasized the impact of emerging technologies on privacy, highlighting how the increasing collection and use of Big Data and Open Data by both governments and private entities is transforming the way personal information is processed[42]. Furthermore, the Special Rapporteur emphasized the need for an international legal instrument on government surveillance, aimed at regulating intelligence activities and ensuring that surveillance operations comply with the principles of necessity and proportionality, thereby safeguarding the fundamental rights of individuals[43].

Once again, the need for an international regulatory framework to ensure the ethical use of Artificial Intelligence (AI), to ensure that its development takes place in full compliance with human rights and the right to privacy, and to prevent technological progress from undermining the right to personal data protection was reaffirmed in the Resolution adopted in 2024 by the United Nations General Assembly[44]. This document acknowledged the potential of AI in advancing sustainable development[45], while simultaneously highlighting the risks associated with the

[39] Ibid. 2-3.
[40] E Carpanelli and others (n 27) 4.
[41] United Nations Human Rights Council, Report of the Special Rapporteur on the right to privacy, A/HRC/37/62 (2018).
[42] Ibid. 4.
[43] Ibid. 18.
[44] United Nations General Assembly, Resolution A/78/L.49: Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (2024).
[45] Ibid. 2.

unregulated use of personal data and the possibility that such technologies could be exploited for purposes of mass surveillance or discrimination[46].

1.2.2.2 The role of the Council of Europe

Additional international instruments for the protection of personal data can be found within the frameworks of the Council of Europe and the Organization for Economic Co-operation and Development, the first two international organizations among to initiate transnational legal instruments in the field of data protection, albeit through different normative approaches[47].

Within the framework of the Council of Europe, the European Convention on Human Rights of 1950 regulates, under Article 8, the right to respect for private and family life:

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".*[48]

The European Court of Human Rights has interpreted such article broadly, applying it to situations in which the text of the provision does not expressly recognize a specific right. In particular, the Court has given an expansive reading to the notions of "*private and family life*" and

[46] Ibid. 3.
[47] J Bing, "The Council of Europe Convention and OECD Guidelines on Data Protection" (1984) *5 Michigan Yearbook of International Legal Studies* 271.
[48] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (1950) 7.

"*correspondence*", encompassing a wide range of aspects relating to the personal sphere. This jurisprudence has laid the foundation for the formal recognition of the right to informational self-determination and to the protection of personal data, in all forms of their dissemination and use[49].

In this context, the European Court of Human Rights has affirmed that the protection of private life also extends to the management and control of personal data, thereby recognizing the principle of informational self-determination, clarifying that the protection of personal data constitutes an essential component of the right to private life, and that any limitation thereof must be subject to strict scrutiny in order to avoid unjustified violations of Article 8 of the ECHR. The principle of informational self-determination establishes that every individual must be able to decide how, and to what extent, their personal information is collected, processed, and disclosed. This right is not absolute and must be balanced against other legitimate interests, such as national security, freedom of expression, and the right to information. However, any restriction on the access to or management of personal data must comply with the principle of proportionality, avoiding excessive or arbitrary limitations. Importantly, this right is not extinguished even when the data in question is already in the public domain, as the massive or uncontrolled collection and dissemination of such data may still amount to a violation of the right to privacy, as established by the European Court of Human Rights in *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*.

To this end, the Court has held that States must ensure the existence of clear and accessible procedures enabling individuals to exercise their right of access to personal data, particularly where such information relates to fundamental aspects of personal identity, such as one's origins or family relationships (*Mikulić v. Croatia, Odièvre v. France*).

Moreover, where the denial of access to data is justified by the need to protect the privacy of third

[49] M Surace (n 3).

parties, the Court has found it necessary that an independent authority assess, on a case-by-case basis, the legitimacy of such restrictions (*Gaskin v. the United Kingdom*). Special attention has also been paid to the handling of data by security services. The Court has acknowledged that, under certain circumstances, States may lawfully restrict access to sensitive information for reasons of national security, as affirmed in *Segerstedt-Wiberg and Others v. Sweden* and *Big Brother Watch and Others v. the United Kingdom*. However, it has reiterated that such restrictions must be necessary and proportionate, and may not constitute an arbitrary obstacle to the right to privacy[50].

The "*Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*", now known as Convention 108+, was adopted in 1980, with a focus on the human rights dimensions of the traditional concept of privacy.

The Convention represents the first legally binding international instrument specifically dedicated to the protection of personal data. In 2018, it was modernized through Protocol CETS No. 223, and since then has been referred to as Convention 108+. It is currently signed by over 50 countries, including several non-member States of the Council of Europe, and gives legal expression to the principles enshrined in Article 8 of the European Convention on Human Rights[51].

The scope of the Convention is defined under Article 1, which provides:

> "*The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*".

[50] Ministero della Giustizia, Guida all'articolo 8 della Convenzione – Diritto al rispetto della vita privata e familiare (Corte Europea dei Diritti dell'Uomo 2021) 50-51.
[51] P Guarda and G Bincoletto (n 4) 102.

In Chapter II, which sets forth the "*Basic principles for data protection*", the Convention establishes that the processing of personal data must be proportionate to the legitimate purpose pursued, based on a fair balance between public and private interests, and grounded in the data subject's consent or another legitimate legal basis. It further requires that data be processed fairly and transparently, for specified and legitimate purposes, and that it be accurate, relevant, up to date, and retained only for as long as strictly necessary. The Convention also mandates the availability of appropriate sanctions and remedies for violations of domestic provisions implementing the fundamental data protection principles it enunciates. Particular attention is given to Article 6, which refers to so-called "*sensitive data*", such as information concerning racial origin, political opinions, religious or other beliefs, health, sexual life, and criminal convictions. With respect to such data, the Convention provides for enhanced safeguards, restricting their processing except in cases expressly authorized by law[52].

In 2001, an Additional Protocol to Convention 108 was adopted, introducing two significant innovations that strengthened both the effective protection of data subjects' rights and the control of international data flows, thereby broadening the scope of the Convention. First, the Protocol made it mandatory for each State Party to establish an independent supervisory authority, tasked with overseeing the application of domestic data protection legislation. Such authorities must be endowed with genuine investigative and intervention powers, operate with full independence, and ensure that their decisions are subject to judicial review.

Second, the Protocol introduced rules governing the transfer of personal data to third countries not party to the Convention, permitting such transfers only if the recipient ensures an adequate level of protection. Exceptions may be permitted where national law allows it for legitimate reasons, or

[52] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (1981) Chapter II.

where the data controller provides sufficient safeguards, deemed adequate by the competent supervisory authorities[53]. With the adoption of the Amending Protocol of 2018, known as Convention 108+[54], the Convention underwent a substantial revision aimed at addressing the challenges posed by digitalization and emerging technologies, aligning it more closely with the standards introduced by the General Data Protection Regulation (GDPR) and reinforcing the protection of personal data within a global context. Among the main innovations introduced is the extension of protection to all individuals, regardless of their nationality or residence, as provided in Article 1, and, in Article 2(c), the application of the Convention to non-automated processing of personal data, provided that such data are contained in structured filing systems. In addition to these amendments, the Protocol introduced four new articles of particular significance[55]. Article 8, entitled *Transparency of Processing*, reinforces the informational obligations imposed on the data controller, requiring the latter to provide data subjects with clear information concerning the identity of the controller, the legal basis for the processing, the purposes pursued, the categories of data processed, the potential recipients, and the means by which data subjects may exercise their rights[56]. Article 10, *Additional Obligations*, codifies the principle of accountability, requiring both controllers and processors to adopt appropriate technical and organizational measures, to carry out impact assessments, and to design data processing operations in a manner that prevents or mitigates risks to fundamental rights[57]. Article 15, titled *Supervisory Authorities*, consolidates and

[53] Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, ETS No. 181 (2001).
[54] Council of Europe, Amending Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), CETS No. 223 (2018).
[55] Ibid. 2.
[56] Ibid. 5.
[57] Ibid. 6-7.

strengthens the provisions already set forth in Article 1 of the 2001 Additional Protocol (ETS No. 181), by requiring each State to establish at least one independent supervisory authority endowed with effective powers of investigation, intervention, sanction, and advisory functions[58]. Finally, Article 17, *Forms of Co-operation*, governs international cooperation between supervisory authorities, promoting the exchange of information, the coordination of inspection activities, and the establishment of a formal network of collaboration[59]. The 2018 Amending Protocol also introduced substantial modifications to several provisions already contained in the 1981 Convention. In particular, Article 5, concerning the general principles of data processing, was reformulated in greater detail, explicitly incorporating the requirements of lawfulness, proportionality, transparency, data minimization, and storage limitation. Article 6, regarding special categories of data, was expanded to include, among such categories, biometric data, genetic data, and data relating to criminal convictions, all of which are subject to enhanced safeguards[60]. Article 9 (formerly Article 8), on data subject rights, was updated to include the right not to be subject to a decision based solely on automated processing which produces significant effects on the individual[61]. Finally, Article 14, concerning international data transfers, was revised to establish the principle of adequacy as a condition for transfers to third countries, as well as the possibility of relying on appropriate safeguards in the absence of a general adequacy decision[62].

[58] Ibid. 9.
[59] Ibid. 11.
[60] Ibid. 4.
[61] Ibid. 6.
[62] Ibid. 8.

1.2.2.3 The role of the Organisation for Economic Co-operation and Development

In addition to the contribution of the Council of Europe, a fundamental role in shaping international principles on data protection has also been played by the Organisation for Economic Co-operation and Development (OECD), which in 1980 adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, focusing on data protection and its impact on international trade and economic cooperation[63]. These Guidelines emerged in a context of increasing digitalization and cross-border data exchange, in which there was a growing need to ensure that privacy protection would not be misused as a barrier to free trade. The United States argued that European countries were erecting barriers to shield their markets from large U.S.-based providers of computer services. This concern influenced the orientation of the Guidelines[64] toward a balance between individual rights and economic flows, explicitly stating in both the Preamble and paragraph 18 that privacy legislation should not be used to unjustifiably hinder transborder data flows, except in clearly defined circumstances, such as the absence of equivalent safeguards or the particularly sensitive nature of the data being processed[65].

Although, as their very name suggests, the OECD Guidelines are not legally binding, they have nonetheless acquired a quasi-obligatory status in practice. Their wording, less stringent than that of binding legal instruments, reflects the intention to allow greater flexibility for States in their national implementation. However, the fact that certain countries accompanied their adoption of the Guidelines with formal reservations demonstrates the quasi-binding character attributed to this

[63] J Bing (n 47) 272.
[64] In particular, Convention 108+ also specifies, in Article 12, that a Contracting Party "*shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party*.
[65] J Bing (n 47) 283.

instrument. The Guidelines also illustrate various implementation approaches, consistent with the regulatory strategies adopted by different member States[66].

The Guidelines are structured into five parts. Part I defines the essential terms and outlines the scope of application, specifying that the Guidelines constitute minimum standards. Part II sets forth eight fundamental principles concerning the protection of privacy at the national level. Part III addresses principles of international application, with particular reference to relations between member States. Part IV discusses, in general terms, the methods by which the principles should be implemented, emphasizing the importance of non-discriminatory application. Finally, Part V deals with mutual cooperation between countries, through the exchange of information and the harmonization of national procedures in the field of data protection, and draws attention to potential conflicts of law that may arise in cases involving multinational data flows[67].

The fundamental principles, set out in paragraphs 7 to 14 of the Guidelines, represent the substantive core of Part II and define the essential criteria for the fair and consistent processing of personal data.

The *Collection Limitation Principle* (para. 7) provides that data must be collected within specified limits, by lawful and fair means, and, where appropriate, with the consent or at least the knowledge of the data subject.

Next is the *Data Quality Principle* (para. 8), which requires that personal data be relevant to the purposes for which they are processed and be kept accurate, complete, and up to date.

The *Purpose Specification Principle* (para. 9) states that the purposes of data collection must be specified not later than at the time of collection, and any subsequent use must be consistent with or

[66] Ibid. 284-285.

[67] Organization for Economic Co-operation Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Publishing 2002) 33.

compatible with those purposes.

The *Use Limitation Principle* (para. 10) establishes that data may not be used for purposes other than those specified, except with the consent of the data subject or as authorized by law.

The *Security Safeguards Principle* (para. 11) requires the implementation of appropriate security measures to protect personal data against unauthorized access, as well as loss, destruction, or unauthorized alteration.

The *Openness Principle* (para. 12) affirms the need for transparency: information must be made available concerning the purposes of data processing, the identity of the data controller, and the policies adopted.

The *Individual Participation Principle* (para. 13) recognizes the right of the data subject to access their personal data, to know their source, and, where appropriate, to request their rectification or erasure.

Finally, the *Accountability Principle* (para. 14) requires that the data controller be held responsible for compliance with the principles and be able to demonstrate that appropriate measures have been taken to ensure their implementation[68].

Five years after the adoption of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the member States of the Organisation adopted, in 1985, *the Declaration on Transborder Data Flows*, with the aim of promoting access to data and information services and of avoiding the introduction of unjustified barriers to the international exchange of information. Although the declaration does not directly address the protection of personal data, it acknowledges the growing economic significance of cross-border data flows and calls upon member countries to ensure regulatory transparency, cooperation, and the development of common solutions, with

[68] Ibid. 14-16.

particular attention to data related to international trade, information services, and intra-corporate flows[69]. In light of the expansion and increasing prevalence of digital technologies and electronic commerce, in 1998 the OECD member States adopted the *Declaration on the Protection of Privacy on Global Networks*. This declaration reaffirms the centrality of privacy protection in global networks and promotes the implementation of the principles set out in the 1980 OECD Guidelines, encouraging the adoption of transparent privacy policies, the use of privacy-enhancing technologies, and access to effective redress mechanisms. Particular attention is devoted to cooperation between governments, the private sector and international organizations, as well as to the development of contractual solutions for the regulation of cross-border data flows[70].

In 2013, the OECD Guidelines underwent a significant revision, aimed at enhancing their practical effectiveness and adapting them to the contemporary digital environment. While the fundamental principles set out in Part II remained unchanged, the revised version introduced several important innovations. In particular, a new Part III, entitled *Implementing Accountability*, was added. It requires data controllers to adopt a privacy management program proportionate to the nature and sensitivity of their activities. Such a program should include risk assessments, internal oversight mechanisms, incident response plans, and periodic reviews. The controller must also be able to demonstrate compliance with the Guidelines and, in the event of a significant breach, must notify both the competent authorities and, where appropriate, the data subjects concerned[71].

Parts IV, V, and VI, respectively dedicated to *Basic Principles of International Application, National Implementation, and International Co-operation and Interoperability*, were significantly

[69] Ibid. 53-55.
[70] Ibid. 59-63.
[71] Organization for Economic Co-operation Development, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Legal Instrument No. 0188 (2013) 8.

revised and expanded compared to the original 1980 version. Specifically, Part IV (paras. 16–18) clarifies that the data controller remains responsible for the data even after cross-border transfer, and that any restrictions must be based on concrete risk assessments and the absence of equivalent protection in the recipient country[72]. Part V (para. 19) calls upon member States to adopt coherent national strategies, to strengthen independent supervisory authorities, and to promote educational and technical initiatives aimed at more effective data protection[73]. Finally, Part VI (paras. 20–23) emphasizes the need for sustained cooperation between data protection authorities and promotes the development of interoperability mechanisms between different regulatory regimes, highlighting the importance of transparency and of measuring the effective implementation of the Guidelines[74].

1.3 Concept and Definition of Personal Data Protection

In privacy law, the term personal data generally refers to "*any information relating to an identified or identifiable natural person ('data subject')*". This is the definition adopted in Article 4(1) of Regulation (EU) 2016/679, in line with definitions already found in previous legal instruments[75]. Notably, the legal notion of personal data has been intentionally broad and flexible over time, in order to adapt to technological and societal developments. The 1980 OECD Guidelines represent one of the earliest international standards and already opted for a similarly comprehensive definition in paragraph 1(b): "*personal data means any information relating to an identified or*

[72] Ibid. 8.
[73] Ibid. 9.
[74] Ibid.
[75] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 33.

identifiable individual (data subject)[76]". Similarly, Convention No. 108 of the Council of Europe provides in Article 2(a) that personal data means "*any information relating to an identified or identifiable individual*[77]*".* Following this approach, Directive 95/46/EC incorporated these principles and, in Article 2(a), defined personal data in a similar manner, as encompassing any information relating to an identified or identifiable individual[78]. This approach, in particular, reflects a deliberate choice on the part of the European legislator. As stated in the original proposal by the European Commission, "*as in Convention 108, a broad definition is adopted in order to cover all information which may be linked to an individual*". The subsequently amended version further clarified that "*the amended proposal meets Parliament's wish that the definition of 'personal data' should be as general as possible, so as to include all information concerning an identifiable individual*", a position that was also taken into account by the Council in its common position[79].

The current definition of personal data is found in Article 4(1) of the EU General Data Protection Regulation (GDPR), which provides:

> *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,*

[76] Organization for Economic Co-operation Development (67) 13.
[77]Council of Europe (n 52) 1.
[78] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 8.
[79] Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, WP 136 (2007) 4.

physiological, genetic, mental, economic, cultural or social identity of that natural person".[80]

While Article 2 of Directive 95/46/EC limited itself to identifying elements such as the physical, physiological, mental, economic, cultural, and social identity of an individual, the GDPR has expanded the scope of the definition to include contextual forms of identification as the ability to distinguish a person within a group even without knowing their name, including not only names or identification numbers, but also location data, online identifiers, and other types of information relating to an individual's overall identity[81]. In this respect, personal data is a dynamic concept: even seemingly, neutral or isolated pieces of information may qualify as personal data if, when combined with other elements, they allow the identification of a data subject[82]. Recital 26 clarifies that identifiability must be assessed by taking into account all means reasonably likely to be used either by the controller or by third parties, while Recital 30 specifies that even digital identifiers, such as IP addresses, cookies, and RFID tags, may be used to track and identify individuals[83]. This reflects a protective notion of personal data, which is not limited to civil status or identity records, but extends to any information that makes it possible, directly or indirectly, to identify a natural person[84].

The content of Article 4(1) GDPR largely reflects the conceptual framework already developed in the opinions of the Article 29 Working Party, which over the years had provided an evolving and

[80] Regulation (EU) 2016/679 (n 75).
[81] The definitions set out in Article 4 of the GDPR clarify that the notion of personal data also encompasses *genetic data* (Article 4(13)), *biometric data* (Article 4(14)), and *data concerning health* (Article 4(15)), as well as data that are subject to *automated profiling* (Article 4(4)) or have undergone *pseudonymisation* (Article 4(5)).
[82] B Saetta, "Dato personale e categorie di dati" (2025) *Protezionedatipersonali.it*.
[83] C Colapietro, "I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale" (2018) *Federalismi.it n. 22,* 16-17.
[84] B Saetta (n 82).

contextual interpretation of the notion of personal data. In Opinion 4/2007, the Article 29 Working Party conducted an in-depth analysis of the definition of personal data contained in Directive 95/46/EC, highlighting the European legislator's intent to adopt a broad, though not unlimited, definition of personal data, aimed at ensuring effective protection of fundamental rights, particularly the right to privacy, in the context of data processing, affirming that "*the scope of the data protection rules should not be overstretched, but unduly restricting the concept of personal data should also be avoided*"[85].

In analyzing the first element of the definition of personal data ("any information") the Article 29 Working Party adopts a broad interpretation of the concept, affirming that it applies "*regardless of the nature or content of the information, and the technical format in which it is presented*," and therefore includes "*both objective and subjective information about a person in whatever capacity […] irrespective of the technical medium"*[86]. Within this framework, biometric data deserve particular mention. Although not expressly referred to in Directive 95/46/EC, biometric data were clearly classified by the Article 29 Working Party as personal data, thereby anticipating their subsequent formal recognition. In Opinion 4/2007, the Working Party acknowledged their identifying nature and the potential impact on an individual's private sphere, noting that "*fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns or even some deeply ingrained skill or other behavioral characteristic*" possess the ability to uniquely identify a natural person[87]. The Working Party highlights the dual nature of biometric data: they are at once information relating to a person and technical means of identification. It further notes that biological samples (such as blood or tissue) are not, in themselves, personal data, but become

[85] Article 29 Data Protection Working Party (n 79) 25.
[86] Ibid.
[87] Ibid. 8.

so once identifying information is extracted from them[88].

This interpretation anticipates what would later be formally established by the GDPR, which classifies biometric data among the special categories of personal data[89]. With regard to the second element, "*relating to*", the Article 29 Working Party specifies that data may relate to a natural person not only when it directly describes their characteristics or condition (*content*), but also when it is processed with the intention of influencing or evaluating that person's behavior (*purpose*), or when it produces tangible effects on the individual (*result*)[90]. As for the third element, "*identified or identifiable*", the Opinion acknowledges that identification may occur not only through direct data, but also indirectly, by means of combinations of information, taking into account the means reasonably likely to be used to identify the data subject[91]. From this perspective, the Working Party further clarifies that *pseudonymised data*, including key-coded data, must be regarded as personal data. Such data fall within the category of *indirectly identifiable data* where there is a realistic possibility of re-identification by the controller or by third parties with access to the key[92]. As in the case of biometric data, this interpretation anticipates what was later formally incorporated in Article 4(5) and Recital 26 of the GDPR.

The conceptual evolution of the notion of personal data as an interpretative bridge between Directive 95/46/EC and the GDPR, initiated with Opinion 4/2007, continued with Opinion 13/2011. This document focuses on the growing use of geolocation services embedded in smart mobile devices connected to the Internet and equipped with location-sensitive sensors, such as GPS. The Opinion analyses the three main geolocation infrastructures (GPS, GSM cell towers, and

[88] Ibid. 8-9.
[89] In particular to art. 4(1) and art. 9(1).
[90] Article 29 Data Protection Working Party (n 79) 10-12.
[91] Ibid. 12.
[92] Ibid. 18.

Wi-Fi networks) with particular attention devoted to new technologies based on the localization of Wi-Fi access points, which have become increasingly widespread[93]. Within this framework, the Working Party affirms that: *"Since location data derived from base stations relate to an identified or identifiable natural person, they are subject to the provisions on the protection of personal data laid down in Directive 95/46/EC of 24 October 1995"*[94]. It is highlighted how smart mobile devices are closely linked to the user's personal sphere, to the point that they may be considered extensions of their identity. The individual nature of their use, combined with the presence of highly sensitive data, enables location service providers to collect detailed information on the habits, movements, and social interactions of the data subject, thereby constructing in-depth behavioral profiles. Such profiles may indirectly reveal data belonging to special categories, such as political opinions, religion, health status, or sexual orientation, depending on the places visited[95].

Particular attention is devoted to unique identifiers, notably MAC addresses (Media Access Control Addresses), which, when combined with location coordinates and other contextual data, may enable the identification of a user even in the absence of their real name. When associated with a geographical location, these identifiers may, in fact, be traced back to the user's place of residence, especially in low-density areas. In such cases, the combination of a MAC address with calculated location data is assimilated to personal data, since the data controller is typically unable to distinguish between situations where the owner of the access point is identifiable and those where they are not. The Working Party clarifies that: "*It is important to recall that it is not necessary that the purpose of the processing of these geolocation data is to identify the users. Whether it requires an unreasonable effort to identify the owners of the Wi-Fi access points is strongly influenced by*

[93] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation Services on Smart Mobile Devices, 881/11/EN WP 185 (2011) 3.
[94] Ibid. 8.
[95] Ibid. 7.

the technical possibilities for the controller or any other person to identify them"[96]. This approach was later explicitly incorporated into the GDPR, which in Article 4(1) and Recitals 26 and 30 recognizes that online identifiers and technical data, when combined with other information, may constitute personal data, even if the identification is neither direct nor intentional.

Finally, along the same interpretative line, the Court of Justice of the European Union (CJEU), in the *Breyer judgment* (Case C-582/14), recognized that even a dynamic IP address might constitute personal data, where the data controller has means reasonably likely to be used, including through third parties, to identify the data subject[97]. The Court applied the relative or subjective criterion, holding that the mere technical or legal possibility of tracing back to a natural person is sufficient for an IP address to fall within the scope of personal data under Directive 95/46/EC. Through this judgment, the Breyer case jurisprudentially consolidated a technologically updated and precautionary interpretation of the notion of personal data, fully consistent with the approach subsequently adopted by the GDPR[98].

[96] Ibid. 10-11.
[97] C Colapietro (n 83).
[98] T Minárik and A Garcia, 'CJEU Determines Dynamic IP Addresses Can Be Personal Data but Can Also Be Processed for Operability Purposes' (2016) *CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence*.

Chapter 2

The European Model: The General Data Protection Regulation

2.1 The protection of data as a fundamental right in the EU

The evolution of the concept of privacy and the protection of personal data within the European context is closely linked to the gradual recognition of these issues as fundamental rights. While in an initial phase the protection of private life was regarded as a general corollary of the right to respect for private life enshrined in Article 8 of the European Convention on Human Rights (ECHR), over time the European Union has come to acknowledge the autonomous legal significance of personal data protection.

The European Union, originally established as the European Economic Community (ECC), was founded with the primary aim of creating a common market based on the free movement of persons, goods, services and capital. As a project primarily designed for economic integration, the original Community legal framework did not include specific provisions concerning fundamental rights, much less with regard to the protection of privacy. This normative gap, however, began to be addressed from the early 1970s, largely due to the intervention of the Court of Justice of the European Communities. Drawing inspiration from the common constitutional traditions of the Member States and the principles enshrined in the ECHR, as interpreted by the European Court of Human Rights in Strasbourg, the Court progressively incorporated the protection of fundamental

rights into Community law. As a result, even before the adoption of binding normative instruments, Europe ensured the protection of individual rights primarily through judicial interpretation[99]. In order to ensure a more comprehensive and coherent protection of fundamental rights within a so-called "multi-level" legal system, discussions regarding the possibility of the European Union formally acceding to the European Convention on Human Rights began as early as the 1990s. However, such accession was initially not feasible, as the founding treaties lacked an explicit legal basis for it[100].

A decisive step was taken with the transformation of the ECC into the European Union with the Maastricht Treaty of 1992, which entered into force in 1993. With the Treaty, for the first time, the EU formally assumed the obligation to respect fundamental rights, enshrining the commitment in Article F.2 if the Treaty on European Union (later renumbered as Article 6), which provided as follows:

> *"1. The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.*
>
> *2. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law.*
>
> *3. The Union shall respect the national identities of its Member States.*

[99] L Miglietti (n 1) 7-8.
[100] E Carpanelli and others (n 27) 7.

4. The Union shall provide itself with the means necessary to attain its objectives and carry through its policies".[101]

This provision formally codified the jurisprudential developments of the Court of Justice, which, since the 1970s, had progressively recognized fundamental rights as general principles of Union law. However, at that stage, there was still no reference to the Charter of Fundamental Rights, nor was any provision made for the Union's accession to the ECHR.

A crucial milestone in the process of consolidating the protection of fundamental rights within the EU legal order was reached with the proclamation of the Charter of Fundamental Rights of the European Union, adopted in Nice in 2000. Initially of political nature and lacking binding legal effect, the Charter was later granted legally binding status with the entry into force of the Treaty of Lisbon in 2009, which conferred upon it the same legal value as the Treaties of the Union. Article 6 TUE specifically provides:

"1. The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties. The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.

2. The Union shall accede to the European Convention for the Protection of Human Rights

[101] Treaty on European Union (Consolidated Version) [1997] OJ C340/145, art 6.

and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.

3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law"[102].

The recognition of the Charter does not entail an automatic expansion of the Union's competences. Article 6 TEU, read in conjunction with Article 51 of the Charter, explicitly clarifies that the Charter cannot constitute an independent source of new competences, nor can it extend those already conferred by the Treaties. The Charter applies to the institutions and bodies of the Union, as well as to the Member States only when they are implementing Union law. Consequently, while an act adopted by the Union may be subject to judicial review for breach of fundamental rights enshrined in the Charter, Member States are equally bound by the Charter when acting within the scope of EU law, for instance, when transposing directives, issuing European Arrest Warrants, or making decisions concerning immigration and return. In this context, the European Commission systematically conducts ex ante fundamental rights impact assessments as part of the legislative drafting process[103].

Among the fundamental rights recognized by the Charter are, alongside those already enshrined in the European Convention on Human Rights, new forms of protection that have emerged prominently in the information society. In particular, Article 7 of the Charter guarantees the right to respect for private and family life:

[102] Treaty on European Union (Consolidated Version) [2012] OJ C326/13, art 6.
[103] E Carpanelli and others (n 27) 7.

"Everyone has the right to respect for his or her private and family life, home and communications" [104].

This provision is of particular significance as it guarantees the protection of private life and individual communications, serving as a crucial safeguard against arbitrary interference by public authorities or third parties. It is closely linked to Article 8 of the Charter, which explicitly recognizes the right to the protection of personal data elevating data protection to the status of a separate and autonomous right, although the two provisions differ in both scope and purpose. According to the Explanations relating to the Charter, Article 7 reflects the content of Article 8 of the European Convention on Human Rights (ECHR), although with updated terminology, replacing the term "correspondence" with "communications", in order to account for technological and digital developments. The same Explanations affirm that limitations on this right must comply with the principles of proportionality, necessity, and the pursuit of a legitimate aim, in line with the case law of the European Court of Human Rights.

It is important to emphasize that, although often invoked together; Articles 7 and 8 of the Charter are not identical in their interpretation. While Article 7 mirrors the language of Article 8 ECHR, focusing on private life, family, home, and communications, Article 8 introduces specific procedural guarantees, such as the requirement of fair and lawful processing, purpose limitation, consent or legitimate legal basis, and independent oversight mechanisms: the former protects the general sphere of private life, while the latter focuses specifically on personal data, thus constituting a separate and autonomous right.

This distinction has been clearly affirmed by the Court of Justice of the European Union, for instance in the Digital Rights Ireland judgment, where the Court held that data retention may

[104] Charter of Fundamental Rights of the European Union [2000] OJ C364/1, art 7.

amount to interference under Article 7 without necessarily infringing the essence of the right, provided it does not involve access to the content of communications[105].

From this perspective, Article 8 of the Charter complements and reinforces the protection of private life by establishing a genuine fundamental right to the protection of personal data:

> *"1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
>
> *3. Compliance with these rules shall be subject to control by an independent authority"*[106].

The Explanations to the Charter identify, among the sources of inspiration for Article 8, not only Article 8 of the European Convention on Human Rights, but also, on the side of Union law, Article 16 TFEU, Directive 95/46/EC, Regulation 45/2001, and, notably, Article 39 TEU, which is situated within the context of the Common Foreign and Security Policy. Article 8 thus acquires systemic significance by codifying the fundamental principles governing the processing of personal data, including fairness, specified purposes, consent or another legitimate legal basis, and by recognizing key procedural rights such as the right of access and the right to rectification. Furthermore, it provides for oversight by an independent authority: a safeguard implemented at the Union level through the European Data Protection Supervisor, and at the national level through independent data protection authorities, such as the Italian Garante[107].

[105] E Carpanelli and others (n 27) 8.
[106] Charter of Fundamental Rights of the European Union (n 104), art 8.
[107] E Carpanelli and others (n 27) 9.

From a critical standpoint, the scope of the Charter raises concerns about the fragmented and conditional effectiveness of fundamental rights, particularly in areas where Member States act autonomously. Although the Charter has symbolic and normative importance, its scope of application, limited to the implementation of EU law, means that significant areas of state action may remain outside its reach.

Article 51(1) confines the applicability of the Charter to instances where Member States are implementing Union law. This means that Article 8 does not apply in purely domestic situations, such as legislation on national security or other sovereign competencies where no link to EU law exists[108]. The CJEU has repeatedly affirmed this interpretation, notably in Åkerberg Fransson (C-617/10), where it held that fundamental rights of the Charter are not applicable outside the scope of EU law[109], and later in Privacy International (C-623/17), excluding the Charter's applicability to national intelligence activities[110].

Such a limitation, while consistent with the division of competences within the EU legal order, raises some important questions. In particular, it suggests that the effective protection of personal data, although formally elevated to the level of fundamental right, may still depend on the nature and source of the national measure involved. This inevitably creates a degree of legal fragmentation: the same individual may enjoy differing levels of protection depending on whether the context is governed by Union law. From this perspective, one might ask whether the Charter, as currently framed, is capable of fulfilling its ambition to offer a unified standard of fundamental rights protection throughout the EU.

---

[108] K Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8(3) *European Constitutional Law Review* (*EuConst)* 377.

[109] Court of Justice of the European Union, 'Field of Application of the Charter of Fundamental Rights of the European Union' (Fact Sheet, 2018) 4.

[110] Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2020] ECLI:EU:C:2020:790, para 3.

The recognition of data protection as a distinct and autonomous fundamental right is further reinforced by Article 16 of the Treaty on the Functioning of the European Union, which states:

> **"***1. Everyone has the right to the protection of personal data concerning them.*
>
> *2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union*[111]*".*

2.2 The Regulatory Evolution

Article 8 of the Charter codifies and consolidates the fundamental principles developed at the European level regarding the processing of personal data, elevating them to the status of fundamental rights. However, the recognition of the right to the protection of personal data within the Charter of Fundamental Rights represents the culmination of a complex evolutionary process, which began with the adoption of Directive 95/46/EC and gradually outlined a distinct European model for data protection[112].

For a long time, within the European Economic Community, it was believed that the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of

[111] Treaty on the Functioning of the European Union (Consolidated Version) [2012] OJ C326/47, art 16.
[112] L Miglietti (n 1) 9.

Personal Data (Convention 108) provided an adequate level of protection. Nonetheless, by the end of that decade, it became increasingly clear that this instrument had neither ensured widespread protection nor achieved genuine harmonization among Member States: by September 1990, only seven EEC countries had ratified the Convention, and, at least one had not yet enacted domestic data protection legislation. Furthermore, the national laws of the signatory states varied significantly in both scope and underlying principles[113].

This regulatory fragmentation conflicted with the overarching goal of the then-European Community, which sought to guarantee the free movement of goods, services, capital, and people within the single market by progressively harmonizing national legal frameworks. Within this context, during the International Conference of Data Protection and Privacy Commissioners held in Berlin in 1989, the European Commission announced its intention to harmonize the legal framework governing the telecommunications sector. This announcement underscored the pressing need for the Union to adopt a common and binding regulatory regime in the field of data protection. In response to these concerns, in September 1990 the Commission published an ambitious document: Communication COM (90) 314 final, addressed to the Council and the European Parliament. It presented a comprehensive package of legislative proposals aimed at ensuring a high level of protection for personal data within the so-called First Pillar of the European Community. This document laid the first institutional and structured foundation for the drafting of what would later become Directive 95/46/EC[114].

[113] For example, in Italy, data protection legislation was limited exclusively to the employment context, whereas in Spain, despite the Constitution recognizing the right to data protection, a comprehensive and organic legislative framework was still absent.

[114] D Korff and M Georges, *The DPO Handbook: Guidance for Data Protection Officers in the Public and Quasi-Public Sectors on How to Ensure Compliance with the European Union General Data Protection Regulation* (2019) 13-14.

2.2.1 Preparatory activities: towards a unified European Regulatory framework

In the introductory section of the proposal, the European Commission highlighted how the growing impact of information technologies and the widespread expansion of open telecommunications networks were making the processing of personal data a routine and crosscutting practice across various sectors of economic and social activity. According to the European executive, this new centrality of personal data required regulatory intervention aimed not only at safeguarding fundamental rights, but also at preserving the integrity of the internal market in the process of completion.

The Commission noted that, despite the shared objectives, the national legislations then in force displayed substantial differences concerning their scope of application (such as the inclusion of manual data or the protection of legal persons), the conditions for lawful data processing (including requirements for notification, consent, and the handling of sensitive data), and the mechanisms for supervision. This heterogeneity, exacerbated by the incomplete ratification of Council of Europe Convention 108, resulted in an uneven level of protection among Member States. Such disparity was potentially in breach of the principle of non-discrimination and could justify unilateral restrictions on the free movement of data. In this regard, the Commission recalled that, beyond national provisions, two international reference instruments were already available: on the one hand, the 1980 OECD Council Recommendation containing guidelines on privacy protection and transborder flows of personal data; on the other, the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. However, the former, being a recommendation, was not legally binding, while the latter, although representing the only binding international legal instrument in the field, allowed broad discretion in

implementation and had not been ratified by all Community members. By 1990, only seven Member States had ratified the Convention, and at least one of them had not yet enacted domestic legislation in this area. This situation was causing growing concern. Since 1976, the European Parliament had repeatedly expressed its alarm, urging the Commission to take action to harmonize national laws. The lack of coordination among legal systems endangered not only the effective protection of personal data, but also the proper functioning of the internal market, posing a threat to the free movement of information. This sense of urgency was reiterated by the European Council meeting in Strasbourg in December 1989, which emphasized the need to ensure, as a matter of priority, the protection of personal data in the context of administrative cooperation between Member States[115].

The 1990 proposal thus aimed to address this gap by introducing a unified regulatory framework based on a high level of protection applicable to both the public and private sectors. The legal basis for this initiative was identified in Article 100A of the EEC Treaty, which authorized the adoption of measures intended to harmonize national legislations in order to facilitate the completion of the internal market[116].

From this perspective, the proposal envisaged a multi-instrument regulatory and strategic framework, each component designed to ensure effective and coherent protection of personal data across different sectoral and institutional contexts, with the ultimate aim of promoting a high level of data protection throughout the Community.

In particular:

[115] Commission, 'Communication on the protection of Individuals in relation to the processing of personal data in the Community and Information security' (Communication) COM (90) 314 final 1-5.

[116] Ibid 12-15.

- *A general Directive on the processing of personal data (SYN 287)*, aimed at ensuring a high and equivalent level of protection in both the public and private sectors subject to Community law. It addressed the principles of lawful processing, the rights of data subjects (access, information, rectification, objection), data quality, information security, and the establishment of a working party on data protection[117];
- *A complementary Directive on the protection of data and privacy in the context of public digital telecommunications networks, specifically ISDN and mobile networks (SYN 288)*, intended to integrate data protection measures into next-generation telecommunications services and ensure a higher level of protection[118];
- *A Recommendation for the European Community's accession to Council of Europe Convention 108*, aimed at strengthening international cooperation and ensuring the respect of data protection principles in relations with third countries;
- *A biennial action plan on information security*, conceived as a tool for developing a comprehensive strategy on cyber security through risk assessment, standard-setting, integration of security functions into systems, and cooperation at the technological and pre-competitive levels[119].

The 1990 proposal for a Directive on the processing of personal data did not merely aim to address existing gaps, but rather presented a comprehensive and structured vision of what would become the European model of personal data protection, based on a balance between fundamental rights, legal certainty, and economic freedom. . The draft directive was organized into ten chapters and thirty articles, clearly outlining the fundamental principles and operational mechanisms of the

[117] Ibid 6-7.
[118] Ibid 8.
[119] Ibid.

future European data protection system.

From Article 1 onwards, the objective of ensuring a high and equivalent level of protection across all Member States was made explicit, with the aim of eliminating any obstacles to the free flow of information[120].

The subsequent articles introduced, in an innovative manner, key concepts such as "*processing*," "*controller*," and the distinction between the public and private sectors, while precisely defining the scope of application of the proposed legislation[121].

Particularly significant were the provisions on the lawfulness of processing (Chapters II and III), which identified the permissible legal bases and clearly differentiated between public and private sector contexts. Equally important were the provisions concerning data subject rights, including the right to information, access, rectification, objection, and blocking of data, along with specific obligations imposed on data controllers[122]. The proposal also anticipated, with remarkable foresight, many of the issues that would later become central in the data protection debate, particularly concerning data quality and security. It established stringent requirements relating to accuracy, purpose limitation, proportionality, and storage limitation, to be implemented through appropriate technical and organizational safeguards. Particularly noteworthy was the general prohibition on the automated processing of sensitive data, unless based on the data subject's explicit consent or a clearly defined legal basis[123].

To complete the framework, the draft included provisions on liability and sanctions, rules governing international data transfers, the establishment of independent supervisory authorities,

[120] Commission, 'Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data' COM (90) 314 final (1990), art 1, 49.
[121] Ibid arts 2-4, 50-52.
[122] Ibid arts 5-15, 53-57.
[123] Ibid arts 16-18, 61-63.

the creation of the Working Party on Data Protection, and the delegation of implementing powers to the Commission for the adoption of technical measures[124].

This body of legislation, though still at the drafting stage, consistently and systematically anticipated the structure of what would become Directive 95/46/EC, serving as its essential political and legal foundation.

The lengthy process that led to the adoption of Directive 95/46/EC was accompanied by an extensive body of preparatory work developed among the Commission, the Parliament, and the Council, beginning with the COM(90) 314 final proposal of 1990 and culminating in the approval of the final text in 1995. The process involved multiple versions of the proposal, opinions from the Economic and Social Committee, legal contributions, compromises negotiated within the Council, requests for terminological clarifications, and in-depth debates concerning the legal basis and the exemptions relating to national security. Among the issues that most frequently emerged during the working group discussions were, inter alia, the debate over the distinction between the public and private sectors, the definition of the Directive's legal basis, the degree of independence and the actual powers to be conferred upon supervisory authorities, the exceptions related to national security and public order, as well as the conditions governing international data transfers. The role of the European Parliament also proved to be decisive, through multiple proposed amendments aimed at strengthening data subject rights and enhancing the effectiveness of the system of safeguards[125].

[124] Ibid arts 21-30, 64-69.

[125] Centre for Intellectual Property and Information Law, *Complete Travaux Préparatoires of the Data Protection Directive (95/46/EC)* (Cambridge University 2001).

2.2.2 The 95/46/EC and 97/66/EC Directives: A first step towards harmonization

The 95/46/EC Directive, adopted on 24 October 1995, represented the first comprehensive legislative act of the European Union in the field of personal data protection. With this instrument, the European legislator marked a decisive turning point in recognizing personal data protection as a fundamental right, placing the protection of natural persons, regarding both data processing and the free movement of such data, at the heart of the regulatory framework. As the outcome of an extensive preparatory process, the Directive aimed to harmonize national legislations while ensuring a high level of fundamental rights protection and enabling the free flow of personal data within the internal market. In its initial recitals, the Directive stressed the urgency of preventing the free movement of personal data, essential to the completion of the internal market, from undermining individuals' fundamental rights. The text thus sought to reconcile two potentially conflicting objectives: on the one hand, the economic imperative linked to the free movement of goods, services, capital, and persons; on the other, the protection of individual rights, in particular the right to privacy. In this perspective, the Directive introduced a common framework based on minimum protection standards, binding upon all Member States, and introduced the innovative approach of placing the individual, not merely the administrative or economic function of processing, at the center of the regulatory system[126].

The 95/46/EC Directive was structured into ten chapters, each addressing a specific aspect of the legal regime applicable to the processing of personal data.

Chapter I, "*General Provisions"* (Articles 1–4), set out the objectives of the Directive, namely, the protection of fundamental rights and the free movement of data, and introduced the key definitions,

[126] L Miglietti (n 1) 9.

as well as the scope of application and the applicable national law[127].

Chapter II, "*General Rules on the Lawfulness of the Processing of Personal Data"* (Articles 5–21), established the principles of data quality (Section I), the legal grounds for lawful processing (Section II), rules for the processing of sensitive categories of data (Section III), information obligations (Section IV), and the rights of access, rectification, and objection (Sections V–VII). It also included provisions on confidentiality and data security (Section VIII), and the requirement of prior notification to the supervisory authority (Section IX)[128].

Chapter III, "*Judicial Remedies, Liability and Sanctions"* (Articles 22–24), governed the right to judicial redress, the liability of data controllers, and the imposition of sanctions in cases of violations[129].

Chapter IV, "*Transfer of Personal Data to Third Countries*" (Articles 25–26), regulated the transfer of data to third countries, making it conditional upon the existence of an adequate level of protection or the applicability of specific derogations[130].

Chapter V, "*Codes of Conduct*" (Article 27), encouraged the adoption of sector-specific codes of conduct[131], while Chapter VI, "*Supervisory authority and working party on the protection of individuals with regard to the processing of personal data*", established independent national supervisory authorities and the Article 29 Working Party[132].

Chapter VII, "*Community Implementing Measures*" (Art. 31), conferred upon the Commission the power to adopt technical implementing provisions[133].

---

[127] Directive 95/46/EC (n 78) 11-12.
[128] Ibid 13-20.
[129] Ibid 20.
[130] Ibid 20-22.
[131] Ibid 22.
[132] Ibid 22-24.
[133] Ibid 24.

Finally, Chapters VIII to X set out the final and coordination provisions[134].

Although the adoption of the Directive represented an important step forward, not only within the Union but also as one of the most comprehensive and influential international instruments in the field of data protection[135], it inherently allowed for national divergence. As acknowledged in Recital 9, Member States were granted a margin for maneuver in transposition, which could lead to substantial disparities in implementation.

This outcome ultimately hindered the uniformity of data protection across the Union and exposed the structural limitations of minimum harmonization.

In parallel with Directive 95/46/EC, the European legislator also intervened in the telecommunications sector by adopting Directive 97/66/EC, aimed at ensuring respect for privacy in the field of electronic communications, functioning as a lex specialis in relation to the lex generalis represented by Directive 95/46/EC. The relationship between the two directives was clarified in Article 1(2), which specified that the provisions of the new directive were intended to "*particularize and complement*" those laid down in the general directive. A general review of the regulatory framework for electronic communications was launched by the Commission in 1999 in response to technological developments and emerging business models. As a result, in 2000, a proposal was introduced to replace the 1997 directive with a new legal instrument specifically tailored to the electronic communications sector. This led, in July 2002, to the adoption of Directive 2002/58/EC, commonly referred to as the "*e-Privacy Directive*", which reaffirmed its subsidiary and complementary nature in relation to Directive 95/46/EC, in the same terms already expressed by the earlier legislative instrument. The 2002 directive was subsequently amended in 2009 by

[134] Ibid 25.

[135] MD Birnhack, 'The EU Data Protection Directive: An Engine of a Global Regime' (2008) 24(6) *Computer Law & Security Report* 512.

Directive 2009/136/EC, commonly known as the "*Cookie Law*", which introduced more stringent rules on consent in relation to online tracking activities. Although Directive 95/46/EC was later repealed and replaced by the GDPR, the e-Privacy Directive remains in force, pending its replacement by a namesake regulation that is currently under negotiation[136].

Article 1, as amended by Directive 2009/136/EC, clarifies that the purpose of the legislation is to ensure an equivalent level of protection for the fundamental rights and freedoms of individuals, particularly the right to privacy and confidentiality, with regard to the processing of personal data in the electronic communications sector. Article 2 introduces, alongside the existing definitions, the notion of a personal data breach defined as any security breach leading to the destruction, loss, alteration, or unauthorized access to data. This concept directly anticipates what would later be formally codified by the GDPR and lays the groundwork for the development of a coherent European framework for the management of security incidents. The provision also specifies that location data, processed to determine the geographic position of a user's terminal, are to be subject to enhanced protection measures[137].

The scope of the Directive, as defined in Article 3, was extended to include electronic communications over public networks, including those supporting data collection and identification devices, such as Internet of Things technologies. Article 4 imposes strict obligations on providers of electronic communications services concerning the security of processing, requiring the adoption of appropriate technical and organizational measures to protect data against

[136] D Korff and M Georges (n 114) 29-30.

[137] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11, 19.

unauthorized access, destruction, or alteration. One of the most significant innovations introduced by the 2009 amendment is the obligation to notify personal data breaches, both to the competent national authorities and, in cases where there is a potential negative impact, to the affected individuals. This obligation may be waived only if the data in question have been encrypted or otherwise rendered unintelligible through effective technical safeguards[138].

One of the most emblematic aspects of the Directive is the principle of confidentiality of communications, enshrined in Article 5. Member States are required to ensure that communications and traffic data are not subject to interception, surveillance, or storage, except with the explicit consent of users or in cases authorized by law[139]. Paragraph 3 of the same article, widely recognized as the legal foundation of the so-called Cookie Law, prohibits the storage of, or access to, information stored in users' terminal equipment without their prior informed consent, subject only to limited exceptions related to technical transmission or services explicitly requested by the user[140].

The processing of traffic data is governed by Article 6, which stipulates that such data may be processed solely for purposes necessary for transmission or billing. Any further use, such as for marketing activities or the provision of value-added services, requires the explicit consent of the data subject, which may be withdrawn at any time[141]. Article 8 addresses the issue of caller line identification, requiring service providers to ensure that users have the ability to withhold or display information relating to their own line or that of the calling party. Article 9 strengthens protection with regard to the processing of location data other than traffic data, which may be used only if

[138] Ibid 19-20.
[139] 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 [2002] OJ L201/37, 7-8.
[140] Directive 2009/136/EC (n 137) 20.
[141] Ibid 21.

anonymized or with the specific consent of the user, who must be granted the ability to object at any time[142].

Article 12 governs the inclusion of subscribers in public directories, providing that such inclusion may occur only with the data subject's consent. The user must be informed of the purposes of the listing, the possibility to rectify or delete their data, and the intended uses of the directories themselves[143]. Particularly significant is Article 13, which regulates unsolicited communications for marketing purposes. The version updated in 2009 establishes that the use of email, fax, or automated calling systems for marketing is permissible only with the recipient's explicit consent (*opt-in*), with a limited exception for situations in which a prior commercial relationship exists and a simple and free right to object is guaranteed (*soft opt-in*). The provision explicitly prohibits unfair practices such as concealing the sender's identity or failing to provide a valid address for opting out[144]. The e-Privacy Directive also mandates the implementation of effective enforcement mechanisms. Article 15a requires Member States to establish sanctions that are effective, proportionate, and dissuasive, to grant competent authorities adequate investigative powers, and to ensure mechanisms for cross-border cooperation. Authorities must be empowered to order the cessation of infringements and to act upon complaints lodged by private parties, including service providers[145].

[142] Directive 2002/58/EC (n 139) 8-9.
[143] Ibid.
[144] Directive 2009/136/EC (n 137) 21.
[145] Ibid 21-22.

2.2.3 From the Treaty of Lisbon to the General Data Protection Regulation (GDPR)

With the entry into force of the Treaty of Lisbon in 2009, the legal framework of the European Union underwent a substantial transformation in terms of fundamental rights protection, marking a turning point for the right to personal data protection. For the first time, this right was recognized not only in secondary legislation, but also in the Union's primary law, through the legally binding proclamation of the Charter of Fundamental Rights of the European Union and the introduction of Article 16 of the TFEU. This development elevated data protection to the status of a constitutionalized right, on par with other fundamental rights recognized by the Union. The result was a structural reinforcement of the regulatory framework: on the one hand, data protection became a benchmark for assessing the legitimacy of actions undertaken by both the Union and the Member States when implementing EU law; on the other, Article 16 TFEU provided an autonomous legal basis for the adoption of legislative acts in the field of data protection. It explicitly recognized the Union's competence to legislate not only with regard to the processing carried out by EU institutions, but also by Member States when acting within the scope of EU law. This shift had concrete implications for the Union's legislative technique. Whereas the right to data protection had previously been implemented through minimum harmonization directives, such as Directive 95/46/EC, the post-Lisbon framework opened the path to more binding and uniform instruments capable of ensuring consistent and homogeneous application across all Member States. In the years following the adoption of Directive 95/46/EC, issues related to regulatory fragmentation and the heterogeneity of implementation practices across Member States had already begun to emerge. The Commission's reports from 2003 and 2007, published pursuant to Article 33 of the Directive, documented significant divergences among national legal frameworks, both in

terms of fundamental concepts and enforcement mechanisms, highlighting persistent shortcomings in the national implementation of the directive. The divergences among Member States, stemming from broad interpretative margins and differing political approaches, hindered the uniform application of the directive. However, these inconsistencies were not initially considered sufficient to justify an immediate legislative revision. Instead, a coordinated work programme was launched, involving national supervisory authorities and the Article 29 Working Party in efforts to enhance cooperation and promote effective implementation. Nevertheless, as early as 2007, the European Data Protection Supervisor had emphasized the inevitability of a reform and the need for it to be carefully prepared. A turning point came in 2009 with the launch of a public consultation by the Commission and the entry into force of the Treaty of Lisbon, which provided a more robust legal foundation for a comprehensive regulatory intervention. The consultation received extensive input from a wide range of stakeholders, including a notable contribution from the Article 29 Working Party entitled "*The Future of Privacy*"[146]. During the same period, the 2010 Stockholm Programme provided clear indications of the need to reform the European data protection framework. In this context, the European Council invited the Commission to assess the functioning of the existing legal instruments and, if necessary, to put forward new proposals, both legislative and non-legislative, to strengthen the protection of fundamental rights. The European Parliament, in its resolution on the Programme, welcomed the idea of a more comprehensive and coherent legal framework and also called for a revision of the Framework Decision in the field of criminal justice. In its action plan for the implementation of the Stockholm Programme, the Commission emphasized the need to ensure the effective and horizontal application of the right to personal data

[146] P Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (2014) 24-26.

protection across all Union policies. This approach was reaffirmed in the Commission's communication "*A Comprehensive Approach on Personal Data Protection in the European Union*", which highlighted the urgent need for a more coherent and effective strategy to ensure the uniform protection of this right.

The declared aim was to introduce a new legislative package by 2011, which would also include the adaptation of the legal instruments applicable to the European institutions.

In this context, in 2012 the European Commission presented a proposal for a new legal framework for personal data protection within the Union, structured around two legislative initiatives: a general regulation aimed at governing data processing in both the private and public sectors, and a specific directive addressed to competent authorities in the field of criminal justice, intended to replace the Council Framework Decision 2008/977/JHA.

The proposed legal framework was welcomed as a necessary reform and major step forward in in enhancing and harmonizing the protection of personal data across the European Union., but also triggered institutional and legal debate raising a number of concerns and required further clarification on several key points.

The chosen legislative structure consisting of both a Regulation and a Directive, revealed certain limitations in terms of comprehensiveness. While the Regulation aimed to achieve full harmonization, the accompanying Directive was perceived as offering a lower level of protection, resulting in a fragmented framework. Moreover, the possibility of extending the scope of the Regulation to include criminal justice matters was rejected by many Member States, despite the option of incorporating specific safeguards and exceptions. Nor was the alternative of a Directive mirroring the Regulation's content, yet allowing for tailored national implementation, pursued by the Commission. These disparities became especially problematic in light of the increasing exchange of data between public and private entities, where a lack of coherence would have led to

serious practical challenges[147].

The proposed regulation, in particular, sought to fundamentally reform the system established by Directive 95/46/EC, which, while recognized as the cornerstone of European data protection law, was no longer deemed adequate to address the challenges posed by technological developments and globalization. Although the principles underlying the Directive were still considered valid, the existing legal framework had failed to prevent regulatory fragmentation among Member States, nor had it eliminated legal uncertainty or the widespread perception of risk among citizens in relation to online activities. Over time, the rapid expansion of digital technologies has profoundly transformed both the economy and social relations, enabling unprecedented levels of personal data collection and use by businesses, public authorities, and even individuals. This transformation has resulted in increased exposure of personal data and, consequently, a widespread sense of insecurity and loss of control among data subjects.

Against this backdrop, the Commission stressed that personal data protection had become an essential precondition for the uptake of digital services and the success of broader European strategies[148].

On this basis, Regulation (EU) 2016/679 was adopted, repealing Directive 95/46/EC and introducing a more robust and coherent legal framework aimed at strengthening the protection of personal data while also ensuring the free flow of information within the Union. As stated in the recitals of the Regulation, the legislator acknowledged that digital transformation and globalization had rendered personal data more vulnerable and subject to large-scale processing by both public

[147] Ibid 27.

[148] Commission, 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 (General Data Protection Regulation) COM(2012) 11 final, 25 January 2012, 1-2.

and private actors. This evolution underscored the need to establish a harmonized and reinforced system, grounded in data subjects' control over their personal information and supported by effective enforcement mechanisms. While recognizing the continuing relevance of the principles underlying Directive 95/46/EC, the Regulation acknowledges the Directive's shortcomings in preventing legal fragmentation across Member States and in reassuring the public regarding data protection, particularly in the digital environment. Hence the decision to adopt a directly applicable regulation, capable of ensuring a uniform level of protection throughout the Member States and removing legal obstacles to the free movement of data[149].

2.3 The General Data Protection Regulation (GDPR)

With the adoption of the 2016/679 Regulation (EU) General Data Protection Regulation (GDPR), the European Union aimed to provide a systemic response to the technological and legal developments that had rendered the framework established by Directive 95/46/EC inadequate. The new Regulation, which entered into force on 24 May 2016 and became applicable on 25 May 2018, constitutes a legal act of general application, binding in its entirety and directly applicable in all Member States without the need for national transposition. The GDPR pursues a dual objective: on the one hand, to strengthen and harmonize the level of protection of personal data of natural persons within the Union; on the other, to ensure the free movement of such data within the internal market. The European legislator thus sought to reconcile the protection of fundamental rights with the requirements of the digital single market.

The Regulation is structured into eleven Chapters divided across ten Titles, comprising 99 Articles

[149] Regulation (EU) 2016/679 (n 75) recitals 6–10, 2.

accompanied by 173 Recitals, which serve a key interpretative function for the correct application of the legal text.

Chapter I sets out the *general provisions* of the Regulation.

Article 1 clarifies the dual purpose of the Regulation, while Article 2 defines its material scope, specifying that the Regulation applies to the processing of personal data carried out wholly or partly by automated means, as well as to non-automated processing of personal data that form part of a structured filing system. Activities conducted for purely personal or household purposes are excluded, as are processing operations related to national security or criminal justice, which are governed by specific legal instruments. One of the most significant innovations is introduced in Article 3, which substantially expands the territorial scope of the Regulation: the GDPR applies not only to controllers and processors established within the EU, but also to those established outside the EU who offer goods or services to individuals in the Union or monitor their behavior. This affirms a principle of global responsibility, bringing within the scope of the Regulation even major international digital platforms.

Article 4 sets out a terminological framework regulating key definitions such as "*personal data*", "*processing*", "*consent*", "*personal data breach*", "*pseudonymisation*", "*controller*"[150].

Chapter II of the GDPR sets out the *principles* governing the processing of personal data within the European Union, laying the foundation for a harmonized and coherent system of privacy protection.

At the heart of the entire regulatory framework are the core data processing principles outlined in Article 5, which form the normative backbone of the GDPR: *lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and*

[150] Ibid 32-35.

confidentiality; and the principle of accountability. Under the latter, the controller must be able to demonstrate compliance with all the principles listed.

The lawfulness of processing, under article 6, must be based on specific legal grounds: consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest, or the legitimate interest of the controller—provided that such interest does not override the rights and freedoms of the data subject. Where consent is required, it must be explicit, freely given, specific, and informed (Article 7). Enhanced protection is provided for children at article 8: in the context of information society services, the processing of personal data of a child under the age of 16 (or a lower age specified by the Member State, not below 13) is lawful only if consent is given or authorized by the holder of parental responsibility. The GDPR generally prohibits *the processing of special categories of personal data* (Article 9) such as data revealing health status, sexual orientation, or religious or political beliefs, unless specific exceptions apply. *The processing of personal data relating to criminal convictions and offences* is allowed only under the control of official authority or when authorized by law with appropriate safeguards (Article 10)[151].

Chapter III is dedicated to *the rights of the data subject*.

The right to information and transparency, governed by Articles 12, 13, and 14, requires the controller to provide the data subject with clear, intelligible, and easily accessible information about the processing of personal data, both when data are collected directly from the data subject and when obtained from third parties. The data subject also has *the right of access to their personal data*, as provided under Article 15, including the right to obtain a copy of the data and to be informed about the purposes of processing, the recipients, the retention periods, and other essential

[151] Ibid 35-39.

elements. The Regulation also enshrines *the right to rectification* at article 16, allowing data subjects to have inaccurate or incomplete data corrected, and the right to erasure, commonly known as the "*right to be forgotten*" (Article 17), which may be exercised in various circumstances, such as when the data are no longer necessary, have been unlawfully processed, or when consent has been withdrawn. Furthermore, the data subject may request *the restriction of processing* (Article 18), for example when contesting the accuracy of the data or objecting to the processing. In such cases, the data may be stored but not otherwise processed, except under specific exceptions.

Another important provision is set out in Article 20, which establishes *the right to data portability*: individuals who have provided their personal data in a structured, commonly used, machine-readable format have the right to receive those data and transmit them to another controller, provided that the processing is based on consent or a contract and is carried out by automated means. In line with the broader objective of empowering data subjects, Article 21 grants *the right to object to the processing of personal data*, particularly where the processing is based on the controller's legitimate interests or the performance of a task carried out in the public interest. Objections are always effective in the context of direct marketing. Finally, Article 22 safeguards the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects them. Any exceptions to this rule are subject to strict safeguards[152].

The responsibilities of the *data controller and processor* are set out in Chapter IV.

Article 24 provides that the controller must implement appropriate technical and organizational measures to ensure, and be able to demonstrate, that processing is carried out in compliance with the GDPR. These measures must be proportionate to the nature, context, and purposes of the

[152] Ibid 39-47.

processing, as well as to the risks posed to the rights and freedoms of data subjects. Article 25 introduces the principles of *data protection by design and by default*, requiring the controller to integrate technical and organizational safeguards for the protection of personal data already at the design stage of products or services. Controllers and processors not established in the European Union but subject to the GDPR by virtue of Article 3 must designate a representative within the EU (Article 27), who acts as a point of contact for data subjects and supervisory authorities. The controller–processor relationship is governed by Article 28, which requires the conclusion of a binding contract containing specific clauses that must be met when a controller engages a processor to carry out data processing activities on its behalf.

Article 30 establishes the obligation to maintain a *record of processing activities*, which must include detailed information such as the purposes of the processing, categories of data and data subjects, recipients, international transfers, and security measures adopted.

A key provision is Article 32, which imposes an obligation on both controllers and processors to ensure a level of *security of processing* appropriate to the risk, taking into account available technologies, implementation costs, and the nature, scope, context, and purposes of the processing. Appropriate measures may include encryption, pseudonymization, and systems resilience. In the event of a data breach, Article 33 requires notification to the supervisory authority within 72 hours, while Article 34 requires communication to the data subjects where necessary. A data protection impact assessment (DPIA) is mandatory for high-risk processing operations under article 35, and in certain cases, prior consultation with the supervisory authority is required according to article 36. The Data Protection Officer (DPO), mandatory under specific conditions (Articles 37–39), must operate independently and serves as the designated point of contact for both the organization

and the authorities[153].

Chapter V governs *the transfer of personal data to third countries or international organizations*. Article 44 sets out *the general principle of transfer*, according to which any international data transfer must comply with the conditions laid down by the GDPR so as not to undermine the level of protection afforded to natural persons. Transfers are permitted without restrictions only where the third country, a specific territory or sector, or an international organization is the subject of an adequacy decision adopted by the European Commission (Article 45), or where appropriate safeguards are in place (Article 46), such as standard contractual clauses or binding corporate rules (Article 47). In the absence of such safeguards, specific derogations may apply (Article 49), including explicit consent from the data subject or the necessity of the transfer for contractual purposes.

Article 50 encourages *international cooperation for the protection of personal data* between data protection authorities and relevant bodies[154].

Chapter VI sets out the rules governing the structure and functioning of *independent supervisory authorities*, which must act with full *independence* (Article 52) and possess the necessary competence and resources. These authorities are entrusted with tasks including monitoring compliance, providing guidance, raising awareness, and engaging in cooperation (Article 57), and they are empowered to exercise investigative, corrective, and authorization powers (Article 58)[155].

Chapter VII introduces the *cooperation and consistency mechanism*, designed to ensure the uniform application of the GDPR across the Union. In cases of cross-border processing, the lead supervisory authority must cooperate with the other concerned authorities. According to article 65

[153] Ibid 47-60.
[154] Ibid 60-65.
[155] Ibid 65-70.

when disagreement arises, the European Data Protection Board (EDPB) may intervene and adopt binding decisions[156].

Chapter VIII regulates the *remedies, liability and penalties* available to data subjects, *including the right to lodge a complaint with a supervisory authority* under article 77, *the right to an effective judicial remedy against a supervisory authority or against a controller or processor* (Articles 78–79), and the possibility of being represented by non-profit organizations according to article 80. *The right to compensation and liability* for damages suffered because of infringements is also recognized with article 82[157].

Chapter IX allows Member States to adopt *provisions relating to specific processing situations,* such as *freedom of expression and information, public access to official documents, the national identification number, employment, archiving, scientific or historical research purposes or statistical purposes* (Arts. 85-91)[158].

Chapters X and XI conclude the Regulation, recognizing *the exercise of delegation* conferring on the Commission the power to adopt delegated and implementing acts (Article 92), and formally repealing Directive 95/46/EC. The GDPR became fully applicable as of 25 May 2018 (Article 99)[159].

2.3.1 The GDPR and its Complementary Instruments

The adoption of the General Data Protection Regulation marked a decisive step in strengthening the fundamental right to data protection under Article 8 of the Charter of Fundamental Rights of the European Union. By establishing a single, directly applicable legal framework, the GDPR

[156] Ibid 71-79.
[157] Ibid 80-83.
[158] Ibid 83-85.
[159] Ibid 86-88.

reduced fragmentation across Member States, enhanced legal certainty, and clarified obligations for both private and public actors in the digital single market.

Yet, the EU data protection system is not founded upon the GDPR alone. It is complemented by two additional instruments. The Law Enforcement Directive (LED), Directive (EU) 2016/680, lays down specific safeguards for the processing of personal data by criminal law enforcement authorities, ensuring a balance between effective cross-border cooperation against crime and terrorism and the protection of the rights of victims, witnesses and suspects. In parallel, the Data Protection Regulation for EU institutions, bodies, offices and agencies (EUDPR), Regulation (EU) 2018/1725, ensures that the Union's own institutions are governed by rules equivalent to those imposed on Member States and private operators.

Together with the GDPR, these measures constitute a layered and coherent EU framework for personal data protection, encompassing both the general regime and the sectoral or institutional contexts, and applied consistently through a network of independent supervisory authorities at national and EU level, including the national Data Protection Authorities (DPAs), the European Data Protection Board (EDPB), and the European Data Protection Supervisor (EDPS)[160].

2.4 Recent developments and future perspectives

The General Data Protection Regulation has rapidly become the poster child of the so-called *Brussels Effect*, a concept elaborated by Anu Bradford. This framework describes the mechanism through which European standards are adopted beyond the Union's jurisdiction, either directly by private companies (*de facto Brussels Effect*) or subsequently by foreign governments under

[160] European Commission, 'Legal framework for EU data protection' (2024).

pressure from those same companies (*de jure Brussels Effect*)[161]. By leveraging the size and attractiveness of the internal market, the EU has been able to project its regulatory standards far beyond its borders. Since its entry into force in May 2018, the GDPR has inspired legislative reforms in countries as diverse as Brazil, India, and Japan, as well as in key U.S. states such as California. This capacity to set de facto global standards confirms the EU's aspiration to act as a digital rule-maker, a strategy explicitly pursued by the Commission under the broader objective of digital sovereignty[162].

Yet, while the GDPR has projected its influence far beyond the Union through the Brussels Effect, its internal application has been characterized by structural and procedural shortcomings.

Years after the full application of the GDPR, the need has emerged to enhance the effectiveness and consistency of the cooperation system between data protection authorities, particularly in cross-border cases. Although the General Data Protection Regulation was designed to provide a harmonized and simplified legal framework for personal data protection across the European Union, its implementation has revealed several structural and procedural shortcomings, especially in cross-border contexts. While the Regulation introduced robust rights for data subjects and binding obligations for controllers and processors, these guarantees have not always translated into effective or consistent enforcement.

One significant issue lies in the lack of harmonization regarding applicable law. The GDPR allows Member States to adopt sector-specific rules without establishing clear criteria on jurisdiction. This has led to legal fragmentation, particularly in cross-border data processing scenarios where multiple jurisdictions or individuals in different Member States are affected. The so-called *one-*

[161] J Tamim, The Brussels Effect and the GDPR: EU Institutions as Catalysts for Global Data Protection Norms (*European Digital Policy Initiative*, 2024).

[162] A Renda, Beyond the Brussels Effect: Leveraging Digital Regulation for Strategic Autonomy (*Foundation for European Progressive Studies*, 2022).

stop-shop mechanism, designed to streamline enforcement, frequently struggled in practice due to difficulties in determining the main establishment of data controllers, sometimes exploited through *forum shopping* failing to guarantee timely and consistent enforcement. Moreover, non-lead supervisory authorities hold limited decision-making power, creating imbalances and delays. Although the European Data Protection Board plays a binding role in disputes, it does not always succeed in bridging national divergences[163].

The European Commission's Second Report on the application of the GDPR explicitly acknowledged these systemic inefficiencies, highlighting procedural divergences between national supervisory authorities and the absence of a unified framework for cross-border cooperation, which have contributed to resolution delays exceeding twelve months in complex cases, with limited use of joint investigations despite their clear benefits. Furthermore, the report noted the underuse of joint investigations[164] and persistent disagreements in the interpretation of core GDPR provisions and the persistent discrepancies in the application of core concepts such as the legal basis for processing or the roles of data controllers and processors, which further hamper coherent enforcement and promote fragmentation among member states[165].

Complaints against Big Tech companies, including those filed by the NGO Noyb in 2018, have remained unresolved for years, especially before the Irish Data Protection Commission, which oversees many of these actors. As many large platforms have strategically chosen to establish their main EU headquarters in countries like Ireland or Luxembourg, responsibility for enforcement has

[163] L Scaffidi Runchella, 'The GDPR and the protection of the data subject between public and private enforcement in the case of cross-border processing' (2023) *Cuadernos de Derecho Transnacional* 12-15.
[164] Commission, Second Report on the Application of the General Data Protection Regulation COM(2024) 357 final 3-6.
[165] Ibid 9.

become concentrated in a small number of national authorities. This has led to backlogs, delays, and uneven enforcement across the EU. Several regulators and civil society actors have voiced concerns about the lack of resources, procedural clarity, and institutional coordination, which continue to hinder timely and effective action. While some national authorities have achieved notable enforcement results, others have struggled to respond promptly to complex complaints, reinforcing perceptions of an "*enforcement gap*" and calling into question the current system's capacity to ensure uniform protection[166]. The Commission acknowledged that some national authorities lack adequate resources and that there is insufficient institutional coordination among supervisory bodies[167].

On the judicial side, coordination among national courts in cross-border litigation remains problematic. Article 81 of the GDPR and other instruments like the Brussels I bis Regulation offer only minimal guidance on coordinating cross-border litigation, resulting in procedural fragmentation and legal uncertainty. The GDPR also adopts a dual-track enforcement model, allowing parallel administrative and judicial actions without a defined relationship between the two. This may lead to conflicting outcomes and further weaken the consistency of the system.

In response, several authorities and observers have called for a complementary procedural instrument to address issues such as timelines, access to investigative files, and inter-authority cooperation[168].

To answer these challenges, the European Commission presented on 4 July 2023 a proposal for a Regulation aimed at addressing the procedural limitations of the GDPR, particularly in cross-

[166] Compet-e, 'Il GDPR non sta funzionando come dovrebbe' (2022) https://www.compet-e.com/il-gdpr-non-sta-funzionando-come-dovrebbe/.
[167] European Commission, Second Report (n 64) 6.
[168] L Scaffidi Runchella (n 163) 15-19.

border complaints, the protection of procedural rights of parties under investigation, and in the cooperation and dispute resolution between supervisory authorities, without altering its substantive provisions.

Fully consistent with the GDPR's regulatory architecture, the proposal aimed to strengthen legal certainty, procedural transparency, and the effectiveness of cross-border enforcement.

Structured into seven chapters, the draft Regulation complements the GDPR by introducing common procedural rules applicable to cross-border cases[169].

First, it harmonizes the submission and handling of complaints in cross-border contexts (Articles 3–6). It introduces a standardized European complaint form and clarifies the criteria for admissibility, while enhancing the procedural rights of complainants, including the right to submit observations and to receive formal responses[170]. Simultaneously, it reinforces the safeguards available to data controllers and processors (Articles 15–17), ensuring the right to be heard during key stages of the procedure and access to the case file, thereby strengthening their rights of defence[171].

Second, the proposal enhances cooperation among national supervisory authorities under the framework of Article 60 GDPR. It clarifies the obligation to exchange relevant information (Article 8) and introduces tools to encourage convergence in the early stages of investigations, such as a summary of key issues (Article 9). Where disagreements arise, the European Data Protection Board may intervene through an urgency procedure to adopt a binding decision more swiftly (Article 10)[172].

---

[169] Commission, '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 2-6.
[170] Ibid 20-21.
[171] Ibid 26-27.
[172] Ibid 22-25.

Third, it clarifies and harmonizes the procedural framework for resolving disputes under Article 65 GDPR (Articles 22–26). The proposal establishes the documentation obligations of the lead supervisory authority and specific deadlines for raising and replying to objections, defines the format of reasoned objections, and ensures that both parties, and, where applicable, complainants, have the opportunity to be heard before the EDPB issues a binding decision[173].

Following a public consultation and the opinions of the EDPB and the EDPS, the European Parliament adopted its position in April 2024, followed by the Council's general approach in June 2024, introducing several amendments aimed at increasing procedural flexibility and administrative efficiency.

One of the key innovations concerns the introduction of clearer procedural deadlines to expedite cooperation among supervisory authorities. The Council also proposed a "*fast-track resolution mechanism*", allowing cases to be resolved without initiating the full cross-border procedure when, for example, the complaint has been amicably settled or the data controller has already remedied the violation. This aims to reduce administrative burdens and accelerate responses in non-controversial cases. Additionally, the Council emphasized the importance of early-stage consensus building, encouraging authorities to use the cooperation tools of the GDPR to align positions from the outset of an investigation. Both complainants and investigated parties will benefit from harmonized procedural safeguards, including the right to be heard during crucial phases of the procedure, particularly when the European Data Protection Board is called to issue a binding decision[174].

The legislative process culminated in a political agreement reached on 16 June 2025, paving the

[173] Ibid 31-14.

[174] Council of the European Union, 'Data protection: Council agrees position on GDPR enforcement rules' (Press release 2024).

way for the formal adoption of the new procedural Regulation aimed at strengthening the enforcement of the GDPR in cross-border cases. The agreement marks a significant step towards improving coordination among national data protection authorities and enhancing the effectiveness of rights protection for EU citizens.

The new rules aim to simplify and accelerate cross-border complaint handling by harmonizing the criteria for admissibility: regardless of the Member State in which a complaint is lodged, it will be assessed based on a common set of information, ensuring consistency across jurisdictions. Procedural safeguards are reinforced on both sides of the investigation. Data subjects will have the right to be heard, including in cases where their complaint is rejected, and will receive preliminary findings prior to final decisions. Likewise, data controllers or processors will be entitled to respond at key procedural stages and to comment on findings before decisions are finalized. To further increase procedural efficiency, the co-legislators introduced clear time limits: standard investigations must be concluded within 15 months, with the possibility of a 12-month extension for complex cases. Simplified cooperation procedures should be completed within 12 months.

The agreement also provides for a fast-track resolution mechanism, enabling supervisory authorities to resolve a case without initiating full cross-border cooperation, provided that the violation has been addressed and the complainant does not object to the outcome.

Finally, the regulation introduces measures to facilitate early consensus-building, including a requirement for the lead supervisory authority to submit a summary of key issues to concerned authorities. This mechanism is expected to reduce procedural friction and promote faster, coordinated decisions.

The political agreement retains the Council's proposal for a simplified cooperation procedure in straightforward cases, allowing authorities to bypass more burdensome rules and concentrate procedural resources on complex investigations. Once formally adopted by both the Council and

the Parliament, the new framework will mark a crucial step in transforming the GDPR's enforcement from a fragmented model into a more cohesive and citizen-centered system[175].

Moreover, these reforms aim not only to strengthen enforcement consistency within the Union, but also to reinforce the EU's normative influence globally, exemplifying the Brussels Effect, setting de facto standards beyond its borders.

[175] Council of the European Union, 'Data protection: Council and European Parliament reach deal to make cross-border GDPR enforcement work better for citizens' (press release 2025).

Chapter 3

The United States' Fragmented Approach to Data Protection

3.1 The Legal landscape in the United States

Unlike the European Union, the United States does not have a single, unified data protection law. It's approach is fragmented, with protection varying by sector, jurisdiction, and type of data, relying on a combination of federal and state laws, judicial interpretations, and self-regulation. U.S. data protection laws are characterized by decentralization and lack of uniformity, with regulatory authority dispersed across federal and state legislatures, courts, administrative agencies, industry groups, and private enterprises. In this patchwork model, the extent and scope of protection often vary significantly by jurisdiction and data type.

3.1.1 The Federal Approach: From Constitutional roots to sectoral model

The notion of privacy as a legal right emerged in the late 19th century, most notably through the seminal 1890 article by jurists Warren and Brandeis, *The Right to Privacy.* They argued for the protection of individual personality and dignity, framing privacy as the "*right to be let alone*". At that stage, there was no concept of "*personally identifiable information*" (PII) as a distinct legal category; rather, privacy was understood in moral and philosophical terms, with the assumption that protections naturally applied to identifiable personal information. The idea of linking data to

individuals was taken for granted, not systematically defined[176]. While U.S. courts gradually incorporated the Warren and Brandeis view into tort law[177], there remained no overarching statutory definition of PII, and no unified framework for addressing emerging privacy risks[178].

On the other hand, at the constitutional level, the U.S. Constitution does not explicitly recognize a general right to privacy, nor does it contain any provision specifically addressing data protection. The most significant constitutional reference to privacy is the Fourth Amendment, which protects individuals from unreasonable searches and seizures by the government. However, this safeguard applies only to state action, not to data collection or processing by private actors[179].

In its early judicial interpretation, the scope of the Fourth Amendment was construed narrowly, applying only to physical intrusions by the state. This limitation was illustrated in *Olmstead v United States* (1928), where the Supreme Court held that warrantless wiretapping did not constitute a violation of the Fourth Amendment, as it involved no physical trespass. In that same case, however, Justice Louis Brandeis, co-author of the seminal 1890 article The Right to Privacy, delivered a powerful dissenting opinion, arguing for an interpretation of the Fourth Amendment that would evolve over time and reflect the societal and technological changes that had occurred since its drafting. The restrictive understanding adopted in Olmstead was decisively overturned in *Katz v United States* (1967). As in the earlier case, the government had conducted surveillance without any physical intrusion. Relying on Olmstead, the lower courts had upheld the use of the recordings, reasoning that no tangible property had been invaded. However, the Supreme Court reversed this view, holding that the Fourth Amendment "*protects people, not places*," and

[176] PM Schwartz and DJ Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 *New York University Law Review* 1814 6-7.
[177] WG Voss and KA Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for US Companies' (2019) *American Business Law Journal* 7.
[178] PM Schwartz and DJ Solove (n 176).
[179] WG Voss and KA Houser (n 177).

recognizing that Katz had a legitimate expectation of privacy even in a public setting. This marked a shift from a property-based to a privacy-based interpretation of constitutional protections, one more appropriate to the upcoming realities of electronic surveillance[180].

It was not until the arrival of computerized databases in the 1960s and 1970s that U.S. policymakers began confronting the challenge of linking data to individuals beyond obvious identifiers[181]. This shift in data processing logic led to early federal privacy statutes, which calibrated protections based on how data systems were structured rather than the inherent sensitivity. These laws triggered protections only when databases were searchable via names or personal identifiers. As a result, significant categories of data remained unprotected unless they were directly linked to an identifiable individual. The Fair Credit Reporting Act of 1970 (FCRA) was the first federal privacy law to respond to computerization and digital records. It applies to any consumer reporting agency that furnishes consumer reports, communications about a person's creditworthiness, reputation, or personal characteristics, used to determine eligibility for credit, insurance, or employment. However, protections are only triggered when the data originates from a defined consumer report. Enacted four years later, The Family Educational Rights and Privacy Act of 1974 (FERPA) governs all educational institutions receiving federal funds. It protects education records, defined as information directly related to a student and maintained by the institution, and was the first federal statute to refer explicitly to personally identifiable information. Nevertheless, its safeguards apply only when such information is part of an official education record[182].

As early as 1973, in response to the increasing use of computerized databases and the resulting

[180] M Surace (n 3).

[181] A 1977 report by the Privacy Protection Study Commission observed that computer systems enabled search across database attributes, such as diagnosis or age, without using traditional identifiers like names, fundamentally changing the nature of indentifiability and exposing limitations of privacy protections.

[182] PM Schwartz and DJ Solove (n 176) 7-10.

privacy concerns, the U.S. Department of Health, Education and Welfare (HEW) issued the landmark report *Records, Computers, and the Rights of Citizens*. This document introduced the *Fair Information Practice Principles* (FIPPs) as a foundational set of privacy guidelines centered on transparency, individual access, data quality, use limitation, and accountability. These principles provided the conceptual backbone for subsequent privacy legislation, including the Privacy Act of 1974, and have since influenced numerous international data protection frameworks[183].

The Privacy Act of 1974, the only federal omnibus privacy law, applies exclusively to federal executive agencies and covers information stored in a system of records, meaning records retrieved by name, number, or other identifier assigned to an individual. The Act requires federal agencies to collect data directly from individuals whenever possible, to limit data retention to relevant and necessary information, and to maintain safeguards and procedures for access, correction, and oversight. However, the Statute does not apply to state governments or the private sector, and the vast majority of U.S. states lack comprehensive data protection legislation[184]. Consequently, the Privacy Act only covers computer searches that identify an individual when retrieval of data is done through reference to a specific personal identifier, such as a name or Social Security Number, and fails to protect data retrieved through attributes rather than identifiers. As a result, significant categories of data remained unprotected unless they were directly linked to an identifiable individual. Within three years of the statute's enactment, the Privacy Protection Study Commission had already drawn attention to and condemned this profound flaw. Nonetheless, over thirty years after enactment of the Privacy Act, Congress still has not corrected this central failing of the statute.

[183] U.S. Department of Veterans Affairs, Fair Information Practice Principles (FIPPs) Factsheet (2023).

[184] G Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards' (2000) 25 *Yale Journal of International Law* 1 23-24.

A landmark transformation came with the Cable Communications Policy Act of 1984, which, for the first time, made the mere collection of PII by cable operators a trigger for privacy obligations requiring prior written or electronic consent, notice, access rights, and adherence to Fair Information Practices. By shifting the trigger from system design to the presence of PII itself, the Cable Act underlined how the U.S. approach to data privacy evolved in response to new technologies[185].

However, this shift did not lead to the establishment of a comprehensive federal privacy regime. Instead, U.S. data protection law consolidated around a sectoral model, in which privacy statutes apply only to specific industries or categories of personal data.

This fragmented framework developed to include the *Health Insurance Portability and Accountability Act* (HIPAA) in 1996, which regulates the use and disclosure of health-related information; the *Children's Online Privacy Protection Act* (COPPA) in 1998 designed to protect the personal information of minors under 13; and the *Gramm-Leach-Bliley Act* (GLBA) in 1999 aimed at safeguarding financial information[186].

3.1.1.1 The Role of the Federal Trade Commission

During the 1990s, as the Internet began to transform the commercial and informational landscape, concerns about data privacy and security escalated significantly. Despite the existence of some sector-specific statutes, large segments of online commerce and digital data practices remained governed primarily by industry self-regulation. It was in this regulatory vacuum that the Federal Trade Commission (FTC) emerged as the de facto data protection authority in the United States. Traditionally tasked with enforcing consumer protection laws, over time the FTC leveraged its

[185] PM Schwartz and DJ Solove (n 176) 11-12.
[186] D Harrington, U.S. Privacy Laws: The Complete Guide (*Varonis*, 2025).

authority under Section 5 of the Federal Trade Commission Act, which prohibits "*unfair or deceptive acts or practices in or affecting commerce*", to begin policing corporate privacy behavior. The agency expanded its interpretation of deception and began pursuing cases involving broader unfair data practices, even in the absence of explicit commitments. Through this evolution[187], the FTC progressively constructed a regulatory framework for privacy and data security rooted in general consumer protection principles[188].

Historically, the FTC focused its enforcement on deceptive practices, targeting companies that failed to comply with their own publicly stated privacy policies. In complaints prior to 2014, companies found in violation were typically required to implement a comprehensive privacy program and to obtain users' explicit consent before applying new privacy policies to previously collected data. However, from 2014 onward, the FTC began emphasizing "*unfairness*" as a basis for enforcement, particularly in cases where companies failed to notify consumers about data collection practices or did not obtain informed consent[189]. Unlike other federal regulators whose mandates are confined to specific sectors, the FTC's jurisdiction extends across nearly all industries engaged in commercial activity. With only limited exceptions, the FTC can regulate virtually any for-profit entity that collects or processes personal data, including actors in finance, healthcare, retail, technology, manufacturing, and transportation. This expansive reach has positioned the Commission as the most influential and comprehensive privacy enforcer in the U.S. federal system[190].

---

[187] However, the breadth of its powers has also drawn criticism, particularly concerning the absence of clear statutory limits and the potential for regulatory overreach.

[188] W Hartzog and DJ Solove, 'The Scope and Potential of FTC Data Protection' (2015) 83 *George Washington Law Review* 2230 7-8.

[189] T Miller, *How Privacy Policies Shape the Future of the Online Economy: A US–EU Comparison (*Mercatus Center, George Mason University 2025) 5-6.

[190] W Hartzog and DJ Solove (n 188).

The legal provision under Section 5 allows the FTC to intervene when companies misrepresent their data practices or fail to safeguard consumer information adequately, even in the absence of sector-specific laws. In particular, because of the sectoral approach to privacy adopted by the U.S., regulating personal data through fragmented, industry-specific statutes, many sectors, particularly online commerce, remain outside the scope of the federal acts. In response to these regulatory gaps, the FTC has gradually asserted a de facto data protection mandate, enforcing commercial privacy and data security standards in areas lacking specific legislation.

A distinctive feature of the FTC's enforcement model lies in its reliance on an *ex post* redress approach, whereby the agency intervenes after a privacy violation has occurred, rather than pre-emptively regulating all possible data uses through a prescriptive ex ante framework. This strategy avoids stifling innovation or limiting the development of new technologies, since it does not impose rigid compliance pathways before harm materializes. Instead, it allows firms flexibility in data practices while still enabling the FTC to act decisively in cases of consumer harm.

Compared to the European Union's highly structured GDPR regime and *ex ante* framework, which has reportedly led to the withdrawal of certain digital services from the EU due to compliance burdens, the FTC's more flexible system enables a broader array of technological experimentation within the U.S. market.

Despite critics arguing that this model may lack sufficient deterrence, the FTC has taken substantial enforcement actions. The agency has recorded over 100 general privacy cases and more than 130 spam-related actions, demonstrating its active role in shaping U.S. data protection norms. Nevertheless, several limitations persist. The widespread use of consent decrees to resolve cases, often lasting up to 20 years, creates long-term compliance obligations without contributing to a

formal and stable body of case law[191].

Nonetheless, the FTC's case by case enforcement has gradually shaped what scholars describe as a "*common law of privacy*" in the United States, a body of regulatory expectations around notice, consent, and data security, even in the absence of federal statutory mandates[192].

In parallel to formal enforcement actions, the FTC has also embraced a model of responsive regulation, characterized by graduated intervention. At the base of the enforcement pyramid, the agency employs dialogue, guidance, and persuasion to encourage adoption of best practices. If voluntary compliance fails, the FTC may escalate to formal warnings, investigations, or public rebukes. At the top of the pyramid lie civil penalties, criminal sanctions, or the revocation of business licenses[193].

Furthermore, the FTC plays a significant role in facilitating international data flows. Through its involvement in frameworks such as the, now-invalidated, U.S.–EU Safe Harbor and its successor, the Privacy Shield, the FTC has sought to align U.S. practices with global data protection standards. Its ability to enforce cross-border privacy promises lends legitimacy to U.S. commitments on data adequacy in the eyes of foreign regulators[194].

Moreover, concerns exist about the FTC's limited resources and rulemaking powers, which may hinder its ability to enforce a future comprehensive federal privacy regime. To enhance its effectiveness, policymakers have proposed targeted reforms. These include granting the FTC limited rulemaking authority accompanied by clear standards and scope, clarifying the definition of privacy violations, and allocating additional enforcement resources. Greater coordination with

---

[191] J Huddleston, A Primer on Data Privacy Enforcement Options (*American Action Forum*, 2020) 3-5.

[192] S M Boyne, Data Protection in the United States (2018) 66 (suppl 1) *American Journal of Comparative Law* 300-306.

[193] T Miller (n 189) 6-9.

[194] W Hartzog and DJ Solove (n 188) 42.

state attorneys general and other agencies like the Department of Justice has also been recommended to improve federal oversight. A more defined and well-resourced FTC could better balance innovation with data protection and fill critical gaps left by the United States' fragmented privacy framework[195].

In recent years, the FTC has signaled its intent to pursue more robust regulatory action. The 2022 Advanced Notice of Proposed Rulemaking (ANPR) floated the possibility of comprehensive privacy rules, although critics have questioned whether such measures exceed the agency's statutory authority. Indeed, the Supreme Court's 2024 reversal of the Chevron doctrine[196], and the broader application of the major questions doctrine, have raised constitutional constraints on agency overreach. Moreover, limited congressional funding and political resistance continue to undermine the FTC's capacity to assume a role comparable to European data protection authorities[197].

3.1.2 State-Level Data Protection Laws

In the absence of a unified federal privacy law, individual states have taken increasingly proactive steps to regulate personal information. Over the past decade, a growing number of state legislatures have enacted privacy statutes that, although fragmented, collectively form an evolving patchwork of protections. These laws vary widely in scope, enforcement mechanisms, and definitions of personal data. From the pioneering California's Consumer Privacy Act (CCPA), state-level initiatives reflect divergent approaches to privacy, posing both opportunities and challenges for regulatory coherence across the United States.

[195] J Huddleston (n 191).
[196] It is a principle that requires judges to defer to the interpretation of federal agencies when laws are ambiguous, as long as such interpretation is reasonable.
[197] T Miller (n 193).

Between 2018 and 2025, twenty U.S. states passed comprehensive privacy laws which can generally be categorized into three major groups, depending on their scope and regulatory architecture.

The first group consists of states with comprehensive consumer data privacy laws[198]. These statutes, establish broad rights for individuals, such as access, correction, deletion, and opt-out mechanisms, as well as clear obligations for data controllers.

The second group includes states that have enacted narrower or sector-specific privacy laws[199]. These laws typically target specific types of data, such as biometric, health, or online advertising data, or apply only in particular contexts. While these statutes provide a degree of protection, they fall short of offering a comprehensive data governance regime.

Finally, a third category comprises states currently considering privacy legislation[200]. In these jurisdictions, comprehensive privacy bills have been introduced or are under discussion but have not yet been enacted. This ongoing legislative activity signals growing awareness and momentum for data protection at the state level, though it also underscores the lack of regulatory coherence[201]. Overall, the absence of a harmonized federal framework has prompted a surge in state-level action, but it has also deepened the inconsistencies across jurisdictions, resulting in varying degrees of data protection depending on the state.

---

[198] Bloomberg Law, 'State Privacy Legislation Tracker' (*Bloomberg Law*, 2025) https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#map-of-state-privacy-laws.

[199] Maine, Michigan, Nevada, New York, Vermont, and Washington.

[200] Namely Alabama, Arkansas, Georgia, Illinois, Maine, Massachusetts, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina, Vermont, West Virginia, and Wisconsin.

[201] Bloomberg Law (n 198).

3.1.2.1 The Fragmented Enforcement Frameworks

Despite the emergence of broadly similar privacy statutes across various U.S. states, significant divergences persist, particularly regarding data protection impact assessments (DPIAs), the definition of sensitive data, and compliance thresholds.

For instance, while most state laws require a DPIA when data processing presents a "*heightened risk of harm to consumers*," California adopts a distinct standard centered on a "*significant risk to consumer privacy*," thereby narrowing the scope of required assessments. In contrast, Utah and Iowa do not explicitly mandate DPIAs, but instead require organizations to "*establish, implement, and maintain reasonable administrative, technical, and physical data security practices*" against foreseeable risks of harm to consumers arising from data processing.

Differences also emerge in the definition of "*sensitive personal information*". California and New Jersey adopt an expansive interpretation encompassing credentials such as account logins, communication content, and government-issued identifiers. By contrast, Colorado omits certain elements, including geolocation data, from its sensitivity scope.

The requirements for the *content and structure* of assessments also diverge. Most states call for a general risk-benefit analysis and the identification of safeguards, whereas California and Colorado mandate a more detailed documentation including processing activities, internal audit trails, and the involvement of internal stakeholders. California further distinguishes itself by requiring businesses to submit annual summaries of their risk assessments to its dedicated enforcement agency, the California Privacy Protection Agency (CPPA), a unique obligation among state-level frameworks. In contrast, all other states rely exclusively on their respective state attorneys general for supervision and enforcement, often limiting the practical scope of consumer protection. California also remains unique in granting a private right of action in cases involving certain data

breaches, empowering individuals to seek redress directly in court[202].

Another critical area of divergence lies in the *review and mutual recognition of DPIAs*. While the majority of state laws remain silent, both California and Colorado mandate updates when material changes in processing occur, bringing their approach closer to that of the EU GDPR. Connecticut imposes review requirements only for data processing activities involving minors, and Colorado adds specific annual review duties for profiling practices. California's draft regulations also propose fixed review, such as annual or biannual reviews, for processing involving automated decision-making (ADM).

Finally, *recognition of DPIAs* conducted under other legal regimes also varies. Most states accept mutual recognition of existing assessments, provided they are comparable in scope and safeguards. California, however, imposes stricter criteria, requiring a supplemental addendum demonstrating compliance with its stricter standards.

This patchwork approach exemplifies a broader tension in U.S. privacy governance: the challenge of balancing interoperability with decentralized, state-specific regulatory standards[203].

3.2 The Fundamental Rights Gap: A Comparative Perspective

A key factor in understanding the transatlantic divergence in data protection lies in the contrasting legal foundations of privacy. While the European Union enshrines personal data protection as a fundamental right, the United States approaches it primarily as a matter of consumer protection and contractual governance. This distinction has far-reaching implications for the scope, enforcement, and legitimacy of privacy laws on both sides of the Atlantic.

[202] C Kibby, 'US Litigation Series: Security Breaches' (*IAPP,* 2025).
[203] Centre for Information Policy Leadership, *Comparison of U.S. State Privacy Laws: Data Protection Assessments* (2024).

As Chapter 2 has shown, the EU legal framework, culminating in the General Data Protection Regulation (GDPR), builds on a rights-based tradition, where the protection of personal data is directly linked to human dignity, autonomy, and democratic legitimacy. It is enshrined in primary law through Article 8 of the Charter of Fundamental Rights of the European Union, supported by Article 16 of the TFEU, and operationalized through a uniform legal regime applicable across Member States. The regulatory architecture is preventive (*ex ante*), risk-based, and enforced by independent supervisory authorities endowed with binding powers.

Conversely, the outlined U.S. model is fragmented and sector-specific. It lacks a comprehensive federal statute or constitutional recognition of privacy as a fundamental right. The dominant legal mechanisms rely on consumer protection, contractual consent, and agency enforcement, most notably through the Federal Trade Commission. This framework emphasizes notice-and-choice and regulates *ex post*, often based on deception or unfairness, rather than on objective principles of lawfulness, necessity, or proportionality.

3.3 The Impact of Schrems I and Schrems II on U.S. Data Protection

This fundamental rights gap has become a central point of friction in the context of transatlantic data flows, particularly in light of the landmark rulings Schrems I and Schrems II.

Thousands of companies and millions of users rely on the uninterrupted exchange of personal data between the EU and the US to support services such as cloud computing, digital advertising, financial transactions, and cross-border employment. Legal uncertainty or restrictions on such transfers pose serious risks to business continuity, elevate compliance costs, and may hinder investment and technological innovation on both sides of the Atlantic.

Despite these economic imperatives, the legal instruments designed to facilitate EU–U.S. data transfers, namely the Safe Harbor and Privacy Shield frameworks, have been invalidated by the

Court of Justice of the European Union due to their incompatibility with the EU's fundamental rights standards, as clarified in the Schrems cases[204].

Under the European Union's legal framework, adequacy decisions, first governed by Article 25 of Directive 95/46/EC and now by Article 45 of the GDPR, require that third countries ensure a level of protection that is adequate to that guaranteed within the Union. In both Schrems I and Schrems II, the CJEU Union assessed whether U.S. law provided an adequate level of protection for personal data transferred from the EU[205].

3.3.1 The US-EU Safe Harbor Agreement and Schrems I ruling

Following the adoption of Directive 95/46/EC, which prohibited the transfer of personal data to third countries not ensuring an *adequate level of protection*, the European Commission initiated negotiations with the U.S. Department of Commerce. The interruption of data flows was seen as a significant threat to transatlantic trade and business operations. To resolve this, the two parties developed a framework to enable U.S. companies to receive personal data from the EU while complying with European data protection standards[206]. The result was the International Safe Harbor Privacy Principles, formalized by the European Commission through an adequacy decision 2000/530/CE pursuant to Article 25(6) of the Directive. The system was based on voluntary self-certification: U.S. companies wishing to transfer EU personal data to the United States had to declare annual adherence to seven fundamental principles:

[204] B Duli, *Data Transfers between the EU and US: The impact of Schrems I and Schrems II for cross-border data flows, privacy, and national security* (Master of Transnational Law thesis, Católica Global School of Law 2021) 13.
[205] C Gentile, 'La saga Schrems e la tutela dei diritti fondamentali' (2021) *federalismi.it.*
[206] B Duli (n 204).

- *Notice* – Informing individuals about the purposes for which their personal data is collected and used, the types of third parties to whom the data may be disclosed, and how individuals can raise complaints.
- *Choice* – Offering individuals the opportunity to opt out of having their personal data disclosed to third parties or used for purposes different from those initially specified.
- *Onward Transfer* – Ensuring that third parties receiving personal data also subscribe to the Safe Harbor Principles or provide the same level of protection through contractual means.
- *Security* – Taking reasonable precautions to protect personal data from loss, misuse, unauthorized access, disclosure, alteration, and destruction.
- *Data Integrity* – Ensuring that the personal data collected is relevant for the intended purpose, and that it is accurate, complete, and up to date.
- *Access* – Allowing individuals to access personal data held about them and to correct, amend, or delete it where it is inaccurate or processed unlawfully.
- *Enforcement* – Implementing effective enforcement mechanisms, including recourse for individuals, verification of compliance, and sanctions for non-compliance[207].

Despite being initially praised as a necessary step to maintain data flows between the EU and the U.S., the framework was heavily criticized. The Article 29 Working Party acknowledged the symbolic importance of the agreement but expressed concerns about the high number of exceptions and the lack of enforceability. Activists and legal scholars on both sides of the Atlantic argued that Safe Harbor did not offer substantive protections equivalent to those guaranteed under Directive 95/46. Although over 2,000 U.S. companies adopted the Safe Harbor Principles within the first two years, serious structural weaknesses emerged over time, including the absence of a centralized

[207] S Crespi, 'La tutela dei dati personali UE a seguito della sentenza Schrems' (2015) *Eurojus* 2-3.

enforcement authority in the U.S. and a lack of transparency in corporate compliance practices.

These weaknesses became more pressing after the 2013 Snowden revelations, which exposed extensive surveillance programs conducted by the U.S. National Security Agency (NSA). The leaked documents revealed that intelligence services had access to personal data transferred from the EU to the U.S. under the Safe Harbor scheme, casting serious doubt on the ability of the framework to uphold the level of protection required under EU law[208].

This situation laid the groundwork for the legal challenge in Schrems I, which ultimately led to the annulment of the Safe Harbor adequacy decision by the Court of Justice of the European Union in 2015.

In particular, in 2013, Max Schrems, an Austrian citizen, filed a complaint with the Irish Data Protection Authority (DPA), requesting that it prohibit Facebook Ireland from transferring his personal data to Facebook Inc. in the United States. Schrems argued that U.S. law and practices, particularly in light of the mass surveillance programs revealed by Edward Snowden and conducted by agencies such as the National Security Agency (NSA), did not provide an adequate level of protection for the personal data of EU citizens, as required under EU law.

He further asked the DPA to interpret the Commission's Safe Harbor Decision in light of Directive 95/46/EC and the Charter of Fundamental Rights of the European Union, emphasizing the need to assess whether the legal regime of the third country (the U.S.) met the standard of data protection required by Union law. Schrems also raised the possibility that the Safe Harbor Decision could be invalidated if it failed to guarantee such a standard.

The Irish DPA dismissed the complaint, asserting that it was bound by the European Commission's adequacy determination under the Safe Harbor framework, which deemed the U.S. data protection

[208] B Duli (n 204).

regime sufficient for the purposes of Directive 95/46/EC. According to the DPA, Facebook's adherence to the Safe Harbor Principles rendered further investigation unnecessary[209].

Following this rejection, Schrems brought an appeal before the Irish High Court, which identified potential conflicts with EU law and decided to refer a preliminary question to the CJEU. The Irish court asked whether, and to what extent, Article 25(6) of Directive 95/46/EC, when interpreted in light of Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union, allowed a national supervisory authority to examine a complaint lodged by an individual concerning the protection of their fundamental rights and freedoms in relation to the transfer of personal data to a third country based on a Commission adequacy decision, particularly when the authority doubts that the third country ensures an adequate level of protection[210].

The Schrems I ruling was delivered in October 2015 by the CJEU.

First, the Court confirmed that national supervisory authorities, pursuant to Article 28 of Directive 95/46/EC, retain the power to examine complaints concerning the adequacy of personal data protection in third countries[211], also including the authority to assess whether a third country ensures a level of protection consistent with EU standards. Nevertheless, as long as a Commission adequacy decision remains valid and has not been declared invalid by the CJEU, Member States and national authorities may not adopt measures that contradict it.

The Court further clarified that when the European Commission has adopted an adequacy decision under Article 25(6) of the same Directive, thus formally authorizing data transfers to a specific third country, such a decision takes precedence over unilateral evaluations by Member States. Accordingly, national authorities may not independently suspend or invalidate data transfers based

[209] B Duli (n 204) 15.
[210] C Gentile (n 205) 4.
[211] Ibid.

on their own assessment of inadequacy, as long as the Commission's decision remains legally valid. This framework leads to two important consequences. On one hand, the right of EU citizens to request a review of third-country adequacy remains unaffected: under Article 28(4) of Directive 95/46/EC, any individual has the right to lodge a complaint with a supervisory authority concerning the protection of their rights[212]. On the other hand, the adoption of an adequacy decision by the Commission does not prevent national DPAs from assessing, upon such complaints, whether the legal system of a third country genuinely ensures an adequate level of protection. If the national court, reviewing the DPA's findings, agrees with the citizien and finds the complaint well-founded, it is then obliged to submit a preliminary reference to the Court of Justice, even when its decisions may be subject to further appeal[213].

Second, although the preliminary reference submitted by the Irish High Court concerned solely the interpretation of certain provisions of Directive 95/46/EC, the CJEU considered it appropriate to extend its examination to the validity of the Safe Harbor Decision[214]. In doing so, the Court clarified the standard of protection required of third countries under Article 25(6) of the Directive. In the absence of a clear and universally agreed definition of "*adequacy*," the Court specified that a third country is not required to replicate EU law identically, but it must ensure a level of protection that is "*essentially equivalent*" to that guaranteed within the European Union, particularly as interpreted in light of the Charter of Fundamental Rights of the EU, notably Article 7 (*respect for private and family life*), Article 8 (*protection of personal data*), and Article 47 (*right to an effective remedy and to a fair trial*) [215]. Adopting this approach, the Court concluded that the Safe Harbor Decision was invalid, as the U.S. legal system did not provide a sufficiently high level of protection, largely due

[212] S Crespi (n 207) 8-10.
[213] Ibid 14.
[214] Ibid 18.
[215] C Gentile (n 210) 5.

to the unrestricted access to personal data by U.S. public authorities and the absence of effective judicial safeguards for EU citizens.

One of the primary reasons for the Court's invalidation of the Safe Harbor framework was the possibility for U.S. authorities to derogate from data protection principles on the grounds of national security. According to the Court, such derogations were formulated in overly broad terms and lacked substantive limitations, thereby resulting in disproportionate and unjustified interference with the fundamental right to data protection. Moreover, the lack of adequate legal remedies for EU citizens was a decisive factor. Neither U.S. law nor the Safe Harbor Decision provided effective redress mechanisms against possible abusive access by public authorities. This concern was reinforced by the European Commission itself, that in 2013 acknowledged certain deficiencies in the U.S. legal framework with respect to oversight and judicial protection, further highlighting the inadequacy of the Safe Harbor regime.

The Court not only declared the framework invalid but also established guiding principles for future adequacy decisions. It emphasized that any access to personal data by public authorities must respect the principles of clarity, necessity, and proportionality. A system that permits indiscriminate surveillance of electronic communications, such as that enabled by Safe Harbor, was deemed incompatible with the very essence of the right to data protection.

A significant aspect of the Schrems I ruling lies in the Court's decision to annul the Safe Harbor Decision with ex tunc effect, in light of the seriousness of the violation. The Court found that the breach of a fundamental right of the Union could not be mitigated or postponed due to economic or systemic considerations. In doing so, the Court reaffirmed a principle already established in Digital Rights Ireland: that the effective protection of fundamental rights must not be subordinated

to concerns of legal certainty or the stability of commercial relations[216].

Therefore, the Schrems I ruling marked a paradigm shift, in which the free flow of personal data is subordinated to the protection of fundamental rights enshrined in the Charter. Notably, the judgment redefines the adequacy test as a comparative assessment between the legal protections afforded by the recipient country and those guaranteed under EU law. The objective is to ensure that the high level of protection established by the Union extends beyond its borders, following the data wherever it goes.

In light of the fundamental rights concerns raised by the ruling, the Article 29 Working Party published an opinion on 13 April 2016, in which it identified four essential European guarantees that must be respected in any legal regime governing data processing, particularly in the context of international data transfers. According to this opinion, (a) rules on data processing that are clear, precise, and accessible; (c) demonstrable necessity and proportionality of any interference with fundamental rights; (3) independent oversight mechanisms; and (d) effective legal remedies for individuals. These guarantees serve as fundamental benchmarks for assessing the legitimacy of any limitation on fundamental rights, particularly when personal data is transferred beyond the borders of the European Union[217].

3.3.2 The Privacy Shield Agreement and Schrems II

In an effort to ensure the continuity of transatlantic personal data transfers following the invalidation of the Safe Harbor mechanism in 2015 by the *Schrems I* judgment, the European Union and the United States negotiated a new agreement known as the Privacy Shield. Adopted in 2016 by the European Commission through Implementing Decision (EU) 2016/1250, the framework

[216] S Crespi (n 207) 18-23.
[217] C Gentile (n 215).

aimed to guarantee the lawfulness of such transfers under Article 25(6) of Directive 95/46/EC[218], recognizing that the new arrangement introduced a coherent set of binding obligations and redress mechanisms designed to ensure an adequate level of protection for personal data transferred from the Union to certified U.S. organizations[219].

The mechanism was based on a system of voluntary self-certification by U.S. companies with the Department of Commerce, requiring adherence to a series of data protection principles incorporated into U.S. domestic law. Certified organizations became subject to oversight and enforcement by U.S. public authorities, notably the Federal Trade Commission and the Department of Transportation[220]. To strengthen the system's effectiveness, the Privacy Shield introduced specific principles:

- *Notice* – requiring organizations to clearly inform individuals about all relevant aspects of data processing.
- *Choice* – guaranteeing individuals the right to opt out of data sharing with third parties or of its use for purposes beyond the original scope, while explicit consent (opt-in) is required for sensitive data.
- *Accountability for Onward Transfer* – obliging organizations to ensure that any transfer to third parties is governed by equivalent contractual safeguards, with continued liability in the event of violations.
- *Security* – mandating appropriate technical and organizational measures to protect personal data against loss or unauthorized access.

[218] Commission, Commission Implementing Decision (EU) 2016/1250 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1, para 1.
[219] Ibid paras 13-14.
[220] Ibid paras 15-18.

- *Data Integrity and Purpose Limitation* – requiring data to be relevant, accurate, and retained only for as long as necessary.
- *Access* – ensuring that individuals may access, correct, or delete their personal data held by an organization.
- *Recourse, Enforcement and Liability* – providing effective remedies, independent oversight, compliance mechanisms, sanctions, and binding arbitration, with liability extending to third-party processors acting on behalf of the organization[221].

Oversight of the Privacy Shield was primarily entrusted to the U.S. Department of Commerce, responsible for receiving and verifying companies' self-certifications, maintaining the official list of participants, monitoring the publication of privacy policies, and intervening in cases of non-compliance, including removal from the regime[222]. In parallel, the Federal Trade Commission was competent for legal enforcement, empowered to sanction organizations violating the Shield's principles by treating such conduct as unfair or deceptive business practices under U.S. law[223]. As for redress, European data subjects could access a multilayered system that allowed them to file complaints directly with the U.S. organization, seek resolution through independent dispute resolution bodies (ADR), or activate cooperation between European and U.S. authorities, including the FTC, in cases of persistent violations[224].

One of the most sensitive aspects of the adequacy decision concerned access to personal data by U.S. public authorities, particularly for national security purposes. The Commission acknowledged that such access was permitted, but considered it subject to sufficient limitations, safeguards, and

[221] Ibid Annex II, Section II.
[222] Ibid paras 30-37.
[223] Ibid para 54.
[224] Ibid paras 38-50.

oversight. In this regard, it referred to the Presidential Policy Directive 28 (PPD-28), which established that data collection by U.S. intelligence agencies must comply with U.S. law and the Constitution, including the Fourth Amendment. It also mandated respect for the dignity, privacy, and civil liberties of all individuals, regardless of nationality or residence, thereby extending a minimum level of protection to non-U.S. persons, including EU citizens[225]. Additionally, PPD-28 introduced substantive limits on surveillance, requiring that data collection be targeted, justified by legitimate national security objectives, and subject to oversight, even when involving non-U.S. individuals[226].

Finally, the Commission emphasized the establishment of an independent Ombudsperson within the U.S. Department of State, tasked with handling complaints from EU individuals concerning access to personal data by U.S. intelligence services. Although not a judicial body, the Ombudsperson is responsible for verifying whether surveillance activities comply with U.S. law and ensuring that appropriate remedies are applied when necessary[227]. The Privacy Shield framework was met with mixed reactions within the European Union, though the prevailing sentiment was largely critical. Privacy advocates argued that the agreement closely resembled the invalidated Safe Harbor framework and failed to address the core issue: the continued surveillance practices of U.S. intelligence agencies. As such, they contended that fundamental rights violations would inevitably persist. Critics also noted that the principles set forth in the Privacy Shield lacked binding legal effect and provided overly lenient obligations for participating companies.

Conversely, both EU and U.S. officials defended the new framework, maintaining that it introduced stronger privacy protections, enhanced oversight mechanisms, and new safeguards aimed at

[225] Ibid para 69.
[226] Ibid para 76.
[227] Ibid paras 120-122.

limiting access to personal data by U.S. intelligence services[228].

In addition to this development, in 2016 the European legislator introduced the GDPR, which established a comprehensive legal framework for the protection of personal data, whose Chapter V of the GDPR governs the transfer of personal data to third countries, allowing such transfers only under specific conditions.

Pursuant to Article 45, personal data may be transferred to a third country if the European Commission has adopted an adequacy decision, certifying that the country in question ensures a level of protection essentially equivalent to that guaranteed by the GDPR. In the absence of an adequacy decision, Article 46 allows data transfers to proceed provided that the data controller has implemented appropriate safeguards to protect the transferred data. In practice, such safeguards are typically ensured through the adoption of Standard Contractual Clauses (SCCs), issued by the European Commission and incorporated into contractual agreements between the data exporter and the data importer.

Following the invalidation of the Safe Harbor agreement by the Schrems I judgment, many companies, including Facebook Ireland, began transferring data to the United States based on these SCCs. Specifically, Facebook continued its data transfers relying on the SCCs annexed to the Commission's Privacy Shield Decision, which at the time constituted the new legal framework for transatlantic data flows[229].

While the Privacy Shield was being negotiated and implemented, Max Schrems reformulated his original complaint following the Schrems I judgment and Facebook Ireland's clarification that it was relying on SCCs to transfer personal data to Facebook Inc. in the United States.

[228] B Duli (n 204) 20.
[229] R Á Costello, 'Schrems II: Everything Is Illuminated?' (2020) 5(1) *European Papers-European Forum* 3.

Schrems argued before the Irish Data Protection Commissioner (DPC) that the SCCs could not legitimize data transfers to the U.S., given that U.S. surveillance programs did not provide an adequate level of protection for EU citizens' data. He further contended that the Privacy Shield also failed to ensure a level of protection equivalent to that required under EU law.

The legal background of the renewed claim focused specifically on data transfers under Commission Decision 2010/87/EU, which authorized the use of SCCs for international data transfers.

In response, the Irish DPC referred the matter to the High Court, which subsequently sought a preliminary ruling from the Court of Justice of the European Union[230]. The High Court argued that the U.S. legal system did not guarantee an adequate level of protection for the personal data of EU citizens, primarily due to the absence of clear limitations on the powers of U.S. intelligence services. The court's concerns focused on three key instruments of U.S. law.

First, Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorizes U.S. intelligence agencies, with prior approval from the FISA Court, to conduct surveillance on non-U.S. persons located outside U.S. territory. This provision underpins programs such as PRISM and UPSTREAM, which require telecommunications providers and internet service companies to transmit to the NSA all communications sent or received by a specific selector. Second, Executive Order 12333 allows the NSA to intercept data while in transit to the United States and to collect and retain such data before it falls under the scope of FISA protections. Lastly, the Presidential Policy Directive 28 (PPD-28), although it purports to extend certain privacy safeguards to non-U.S. individuals, was viewed by the High Court as insufficient, as it merely requires that intelligence activities be "as tailored as feasible," without imposing binding or enforceable legal

[230] B Duli (n 228).

limitations.

According to the Irish court, these legal instruments did not ensure a level of protection equivalent to that required by EU law. In particular, EU citizens lacked access to effective legal remedies comparable to those available to U.S. citizens. Moreover, the activities carried out under Executive Order 12333 were not subject to judicial oversight or enforceable redress mechanisms, in breach of Article 47 of the Charter of Fundamental Rights of the European Union[231].

The preliminary ruling request submitted by the Irish High Court focused on three key elements: the interpretation of Articles 25 and 26 of Directive 95/46/EC in light of Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union; the validity of the European Commission's decision 2010/87/EU on Standard Contractual Clauses; and the validity of Decision 2016/1250 establishing the EU-U.S. Privacy Shield. The referring court asked whether these instruments ensured a level of data protection equivalent to that guaranteed under EU fundamental rights[232].

The response of the CJEU was structured in five sections and was delivered on October 2020.

In its judgment, the Court of Justice first addressed whether the GDPR applied to transfers of personal data from the European Union to a third country when, during or after such transfer, the data may be subject to processing by the authorities of that third country for purposes such as national security, public security, or defense[233].

The Court, however, firmly rejected this interpretation. It clarified that Article 4(2) TEU refers specifically to the internal division of competences within the Union and applies only to EU Member States, not to third countries such as the United States. As such, this provision cannot be

[231] C Gentile (n 210) 8.
[232] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* [2020] ECLI:EU:C:2020:559, para 1.
[233] R Á Costello (n 229) 4.

used to exclude a data transfer to a third country from the scope of the GDPR simply because the transferred data might be accessed by foreign intelligence or security agencies[234]. The Court held that where private entities, such as companies, are involved in the transfer of personal data, the GDPR remains applicable, even if the data may ultimately be accessed for national security purposes[235].

Subsequently, the Court was asked to clarify the level of protection required under Article 46(1) and Article 46(2)(c) of the GDPR for transfers of personal data to third countries based on Standard Contractual Clauses, to determine whether an adequate level of protection is ensured in such transfers and which criteria must be considered in that assessment. Although the GDPR does not define in detail what constitutes "*appropriate safeguards*," the Court emphasized that Article 46 must be interpreted in light of Article 44 GDPR. Article 44 states that all provisions in Chapter V of the GDPR must be applied in such a way as to ensure that the level of protection afforded to individuals in the EU is not undermined by the transfer, in order to maintain a high and consistent level of protection for personal data throughout the Union, even when data leaves EU territory.

Here, the Court reaffirmed the standard established in *Schrems I*: a third country is not required to provide identical protection, but the level must be "*essentially equivalent*" to that guaranteed within the EU, in accordance with the GDPR and interpreted in light of the Charter of Fundamental Rights. The Court explicitly rejected the idea that this equivalence could be assessed with reference to national constitutional systems or the European Convention on Human Rights. It confirmed that only the GDPR and the Charter constitute the binding normative framework for evaluating the level of data protection under Union law. National law, even of constitutional rank, cannot serve as the

[234] *Schrems II*, Case C-311/18 (n 232), paras 80-89.
[235] R Á Costello (n 229) 5.

benchmark for interpreting the requirements of Articles 45 and 46[236].

Importantly, the Court clarified the responsibilities of both data exporters and supervisory authorities. Data controllers and data recipients must assess, under Article 8(3) of the Charter and Articles 51 and 57 GDPR, prior to any transfer, whether the legal system of the destination country allows for effective implementation of the SCCs. If it does not, under Article 58, the transfer must be suspended or terminated: national Data Protection Authorities have the duty to intervene and suspend transfers when adequate protection cannot be guaranteed, regardless of whether the SCCs have been formally approved by the Commission[237].

Regarding the validity of the Standard Contractual Clauses, formalized in the Decision 2010/87/EU, under Articles 7, 8, and 47 of the Charter, the referring Court had expressed doubts over their effectiveness in protecting personal data, since they do not bind authorities in third countries. The CJEU acknowledged this limitation but clarified that SCCs are not equivalent to an adequacy decision under Article 45 GDPR, noting that they are not meant to assess a country's legal system, but to offer contractual safeguards that can be applied regardless of the destination country. Their validity depends not on their ability to constrain foreign governments, but on whether they include mechanisms to ensure that data transfers are suspended or terminated when the required level of protection cannot be maintained[238].

Lastly, in its assessment of the Privacy Shield framework, the Court of Justice examined whether the United States ensures an adequate level of protection for personal data transferred from the European Union, as required by Article 45(1) of the GDPR and interpreted in light of Articles 7, 8, and 47 of the Charter of Fundamental Rights of the European Union. While the European

[236] *Schrems II*, Case C-311/18 (n 232), paras 90-105.
[237] R Á Costello (n 229) 5-6.
[238] *Schrems II*, Case C-311/18 (n 232), paras 122-149.

Commission had concluded that the Privacy Shield offered sufficient safeguards, the Court found that the framework allowed for unrestricted access to EU personal data by U.S. public authorities, particularly for purposes of national security and law enforcement. Programs such as PRISM and UPSTREAM, authorized under Section 702 of the FISA and Executive Order 12333, permitted extensive and indiscriminate surveillance without adequate limitations, and without effective judicial oversight. The Court held that these practices did not satisfy the principle of proportionality and failed to offer guarantees equivalent to those required under EU law. In particular, the surveillance mechanisms lacked clear legal limits and safeguards, especially when data subjects were non-U.S. persons.

Moreover, the redress mechanism established under the Privacy Shield, the Ombudsperson, was found to be insufficient. The Court emphasized that the Ombudsperson did not meet the standards of independence, impartiality, or judicial authority required by Article 47 of the Charter. It could not issue binding decisions, and its appointment and removal procedures did not ensure institutional independence.

As a result, the Court concluded that the Privacy Shield framework did not provide an essentially equivalent level of protection and therefore declared the adequacy decision invalid. This ruling confirmed that transfers of personal data to the U.S. based on the Privacy Shield were no longer lawful[239].

This judgment had significant implications for future EU–US data transfer frameworks, leading to the subsequent development of the EU–US Data Privacy Framework.

[239] Ibid paras 163-202.

3.4 The EU-US Data Privacy Framework

Following the invalidation of previous data transfer mechanisms between the European Union and the United States, such as the Safe Harbor and the Privacy Shield, the European Commission adopted in 2023 a new legal framework known as the EU-US Data Privacy Framework (DPF). This new instrument aims to ensure an adequate level of protection for personal data transferred to the United States, addressing the concerns raised by the judgments of the Court of Justice of the European Union.

The new Framework introduces a series of legal and organizational mechanisms designed to guarantee the protection of EU citizens' data once transferred to the United States, following the model, though with significant updates, of the earlier Safe Harbor and Privacy Shield frameworks. The Data Privacy Framework is based on a voluntary self-certification mechanism by U.S. companies. Data controllers or processors established in the United States may adhere to it by formally committing to comply with the EU-US Data Privacy Framework Principles:

- According to *the Purpose Limitation and Choice Principle*, personal data must be processed lawfully and fairly, collected for specified purposes, and subsequently used only insofar as such use is compatible with those original purposes[240].
- Regarding *the Processing of Special Categories of Personal Data*, the Framework requires explicit prior consent (opt-in), with exceptions permitted only in specific circumstances such as medical emergencies or legal obligations, in alignment with EU standards[241].

[240] Commission, Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU–US Data Privacy Framework [2023] OJ L231/1, para 13.
[241] Ibid paras 16-19.

- *The Principles of Data Accuracy, Minimization, and Security* ensure that personal data are accurate, kept up to date, and processed in a manner that is adequate, relevant, and not excessive. Data must be retained only for as long as necessary to achieve the purposes, and appropriate technical and organizational safeguards must be adopted to prevent unauthorized access, loss, or misuse[242].
- *The Transparency Principle* obliges organizations to clearly inform individuals about how their data are processed, including the purposes of processing, possible third-party disclosures, available rights, and redress mechanisms. This information must be provided at the time of collection and made publicly accessible through privacy policies and links to official DPF resources[243].
- Under *the Individual Rights Principle*, data subjects are granted key rights such as access to their personal data, the right to rectification or erasure of inaccurate or unlawfully processed information, and the right to object to processing for purposes that are materially different from those initially stated or for direct marketing. These rights may be restricted only in exceptional circumstances, such as the protection of national security or the rights of others[244].
- *The Accountability for Onward Transfer Principle* requires that any further transfer of data to third parties, whether within the United States or to other third countries, be limited to specific purposes and governed by contractual obligations that ensure a level of protection equivalent to that of the Framework. If a third party can no longer comply with these

[242] Ibid paras 20-24.
[243] Ibid paras 25-28.
[244] Ibid paras 29-36.

obligations, it must cease processing the data, while the original organization remains accountable for ensuring effective safeguards throughout the transfer chain[245].

- Finally, *the Accountability Principle* obliges certified organizations to implement and document internal compliance systems, including employee training, regular internal reviews, and cooperation with independent dispute resolution bodies and regulatory authorities. Compliance is subject to oversight and enforcement under the Recourse, Enforcement, and Liability Principle[246].

The administration and oversight of the new DPF are entrusted to the United States Department of Commerce (DoC), which coordinates its implementation and monitors the compliance of participating organizations with the Principles established by the Framework[247]. The DoC's responsibilities include:

- Managing *the certification and annual re-certification* process, which involves verifying the organization's public commitment to the Principles, ensuring the publication of compliant privacy policies, and identifying both an independent redress mechanism and the competent enforcement authority. Organizations are authorized to receive personal data only after formal approval of their certification and inclusion in the official DPF List[248].
- Reviewing the *compliance of documentation* and *monitoring*, particularly privacy policies, by checking their completeness, online accessibility, and the accuracy of links to complaint mechanisms. It may also verify affiliated entities and cross-check information with enforcement bodies. Ongoing compliance is monitored through regular and targeted

[245] Ibid paras 37-43.
[246] Ibid paras 44-46.
[247] Ibid para 47.
[248] Ibid paras 48-52.

checks; organizations must respond to any issues within 45 days, or risk referral to the FTC or DoT. Persistent non-compliance may lead to removal from the DPF List and the obligation to return or delete previously received data[249].

- *Identifying and addressing false claims of DPF participation*, including misuse of the certification mark and unauthorized references in privacy policies by conducting proactive and complaint-based investigations. In cases of non-cooperation, the matter is referred to the FTC or DoT for appropriate enforcement action[250].

Moreover, to ensure an effective level of data protection, organizations must be subject to the jurisdiction of the revelant U.S. authorities, namely the Federal Trade Commission and the Department of Transportation, which hold the necessary investigatory and enforcement powers. The FTC, may investigate and take action against violations or false claims of DPF adherence through administrative or judicial orders, monetary penalties, and the publication of enforcement outcomes. The DoT, in turn, has exclusive jurisdiction over airlines and shares jurisdiction with the FTC regarding ticket agents and it may initiate enforcement proceedings before independent administrative law judges[251].

To guarantee adequate protection, the EU-U.S. DPF provides a redress mechanism under the *Recourse, Enforcement and Liability Principle*, requiring organizations to provide accessible means of redress for individuals affected by non-compliance. As part of their certification, organizations must ensure effective and readily available independent dispute resolution mechanisms through which individual complaints and disputes can be investigated and resolved promptly, and at no cost to the individual. These mechanisms may be based either in the European

[249] Ibid paras 53-55.
[250] Ibid paras 56-57.
[251] Ibid paras 58-64.

Union or in the United States, with the option for organizations to voluntarily commit to cooperate with EU Data Protection Authorities[252].

Consequently, the DPF offers individuals a range of avenues to enforce their rights. They may file complaints directly with the organization, with the designated independent dispute resolution body, with national DPAs, with the DoC, or with the FTC. Individuals are free to pursue any or all of these mechanisms, and are not required to follow a specific order. Specifically, they may first submit a complaint to the U.S. organization, which is obligated to respond within 45 days[253]. Alternatively, complaints may be brought before the independent dispute resolution body, which must offer free and appropriate remedies, such as correction or deletion of data, or public disclosure of violations. If the organization fails to comply with the decision of the dispute resolution body, the DoC or the FTC may intervene, possibly leading to the organization's removal from the DPF List.

An additional redress avenue is available through the Data Protection Authorities of EU Member States, especially in cases involving employment-related data or where the organization has voluntarily accepted DPA oversight[254]. Finally, as a last resort, individuals may initiate binding arbitration before the EU-U.S. Data Privacy Framework Panel, composed of experts jointly appointed by the European Commission and the DoC[255].

The conditions under which U.S. public authorities may access personal data transferred from the European Union for purposes of criminal law enforcement and national security are governed by Article 45 of the GDPR, which requires that such access complies with the principle of "*essential*

[252] Ibid paras 66-68.
[253] Ibid paras 69-70.
[254] Ibid paras 71-75.
[255] Ibid paras 82-84.

equivalence" to the level of protection guaranteed under the European legal order[256].

With regard to access for criminal law enforcement purposes, U.S. authorities may obtain access to personal data transferred from the EU only through strict legal procedures such as judicial warrants or grand jury subpoenas, provided that legitimate and specific grounds are established with the principles of proportionality and procedural safeguards[257].

Regarding national security, access is regulated by the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333, both and strengthened by the recent Executive Order 14086[258] which introduces binding legal obligations for all intelligence activities to ensure legality, necessity, and proportionality[259]. Data access must be targeted when conducted within the United States, .while bulk collection is permitted only for data in transit or collected abroad, and only in exceptional circumstances, subject to strict limitations and limited use for six clearly defined security objectives[260].

The activities of U.S. intelligence services are subject to to a comprehensive oversight system, involving both internal and independent authorities[261].

A two level redress mechanism accessible to EU citizens has been established to safeguard

[256] Ibid paras 88-89.
[257] Ibid paras 90-98.
[258] Ibid paras 121-124.
[259] Ibid paras 128-132.
[260] Ibid paras 140-142.
[261] The main oversight bodies include: senior legal and compliance officers within each agency (para 162); Privacy and Civil Liberties Officers (paras 163–164); the Intelligence Oversight Board (IOB), which reports directly to the President (para 166); the Privacy and Civil Liberties Oversight Board (PCLOB), an independent entity assessing the implementation of intelligence policies, including EO 14086 (para 167); and the Foreign Intelligence Surveillance Court (FISC), a federal court with powers to authorize surveillance and impose corrective measures (paras 173–174).

individual rights[262], ensuring independence, transparency, and confidentiality for national security purposes[263]:

1. First the Civil Liberties Protection Officer (CLPO) of the Office of the Director of National Intelligence (ODNI), investigates alleged violations of U.S. surveillance law[264], conducts an impartial assessment, and may impose binding remedies on intelligence agencies.
2. Second, decisions may be appealed before Data Protection Review Court (DPRC), an independent tribunal to confirm, modify, or overturn the CLPO's decision[265].

In addition to this new instrument, further legal remedies remain available to all individuals, regardless of nationality or residence, before ordinary U.S. courts[266].

3.4.1 Towards Schrems III?

The adoption of the EU-US Data Privacy Framework in July 2023 marked the most recent attempt by the European Union and the United States to establish a stable regime for transatlantic transfers of personal data. This legal instruments follows the frame of its predecessors, Safe Harbor and Privacy Shield, both of which were invalidated by the the Court of Justice of the European Union in the landmark Schrems I and Schrems II rulings, due to the lack of adequate safeguards against U.S. government surveillance and the insufficiency of judicial remedies available to European data subjects.

[262] Commission (n 240) para 175.
[263] Ibid para 192.
[264] As an example EO 14086, FISA, EO 12333.
[265] Commission (n 240) paras 179-191.
[266] These avenues are based on laws such as the Freedom of Information Act, the Electronic Communications Privacy Act, and the Administrative Procedure Act, and allow individuals to access data held by federal agencies, challenge unlawful surveillance activities, and seek compensation for violations (paras. 195–199).

A particularly critical aspect of the new regulatory framework established by Executive Order 14086 concerns compliance with the principle of proportionality, as outlined in Article 52 of the Charter of Fundamental Rights of the European Union. Although the EO 14086 introduces some improvements compared to the former Privacy Shield, such as the identification of specific legitimate objectives for intelligence activities and a list of prohibited purposes, serious doubts remain about its compatibility with the requirements of Union law. According to Article 52 of the Charter, limitations to the exercise of fundamental rights must be provided for by law, respect the essence of the right, and meet criteria of necessity and proportionality in relation to a legitimate objective of general interest. However, several aspects of the Executive Order raise concerns about the fulfilment of these requirements. First, the wording of the legitimate objectives justifying data collection by U.S. authorities is excessively broad and vague, undermining the clarity and foreseeability of the legal basis. In addition, the Executive Order allows the President of the United States to unilaterally modify such objectives in the presence of national security threats, without formal constraints or parliamentary oversight. This regulatory flexibility undermines the requirement that restrictions to fundamental rights must be based on clear, precise, and accessible rules.

A further critical aspect of the Data Privacy Framework relates to Article 47 of the Charter, which guarantees everyone the right to an effective remedy before an independent and impartial tribunal. Executive Order 14086 introduces, in this respect, a two-level redress mechanism: complaints from EU citizens are first examined by the Civil Liberties Protection Officer, an official within the Office of the Director of National Intelligence, responsible for initiating a preliminary investigation and issuing corrective measures, which can be reviewed by the Data Protection Review Court. However, complainants are not informed whether they have been subject to surveillance, which reduces transparency and hinders meaningful challenge. Moreover, the DPRC does not directly

assess the lawfulness of the intelligence activity, but only reviews the procedural correctness of the CLPO's decision, without granting the complainant substantive rights, such as access, rectification, deletion of personal data, or compensation for damages. These rights, by contrast, are expressly recognized under Article 82 GDPR, which defines fair redress as a structural component of effective judicial protection.

From the perspective of institutional independence, further concerns arise. While representing an improvement over the Ombudsperson mechanism of the Privacy Shield, the DPRC remains a body embedded in the executive branch, whose members are appointed by the Attorney General, and not part of the federal judiciary. The Court of Justice has made clear that judicial independence depends not only on appointment procedures but also on the institutional position of the body and its immunity from external influence. In this sense, the fact that the DPRC is located within the executive and lacks a constitutional foundation comparable to Article III of the U.S. Constitution means that it does not meet the independence requirements set by Union law. As Max Schrems stated, the new structure resembles an "Ombudsperson Plus", highlighting its administrative rather than judicial nature. To further complicate matters, the State Secrets Privilege, reaffirmed by the U.S. Supreme Court in *FBI v. Fazaga*, allows the U.S. government to block access to evidence or even terminate legal proceedings if they pose a risk to national security. If applied to DPRC proceedings, this doctrine could effectively neutralize the possibility of meaningful redress for EU citizens[267].

These challenges identified in the literature are further confirmed by the first review report of the EDPB from November 2024, which expressed serious concerns regarding the DPF's ability to

[267] M Giacalone, 'Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework' (2023) 8 *European Papers – European Forum* 152-157.

ensure a level of protection essentially equivalent to that required by the Charter, particularly with regard to the access to and use of personal data by U.S. public authorities, especially for intelligence purposes.

Regarding the principles of necessity and proportionality, the EDPB pointed out that there is currently no concrete evidence of their effective implementation during the review: in particular, U.S. authorities did not provide any examples or documentation demonstrating how these principles are actually applied in the day-to-day operations of intelligence agencies. Even more problematic is the lack of an independent prior authorization mechanism for bulk surveillance, an insufficiency already censured by the ECtHR and incompatible with Articles 7, 8, and 52 of the Charter of Fundamental Rights.

Further critical elements have emerged concerning the re-authorization of Section 702 FISA. Its recent renewal through the Reform Intelligence and Securing America Act (RISAA) of 2024 failed to incorporate the core recommendations of the Privacy and Civil Liberties Oversight Board (PCLOB), such as the codification of legitimate surveillance objectives and the absence of a clear jurisdictional mandate for the FISA Court to enforce the safeguards introduced by EO 14086. Additionally, the expanded definition of "*electronic communication service provider*" (ECSP), now covering any entity with access to communication infrastructure, has been criticized for its vagueness and unpredictability, which clashes with the requirement for clear, precise and accessible law under EU Article 52 of the Charter. Similarly, the role of amici curiae, experts appointed to assist FISA Court judges in classified proceedings, has been restricted to limited interventions upon judicial invitation, thereby weakening adversarial proceedings and procedural transparency.

As for the redress mechanism, although the DPRC has been formally established and judges and special advocates have been appointed, no complaints had yet been processed at the time of the

review, making it impossible to assess whether the system effectively ensures independent and effective redress, as required under Article 47 of the Charter. The continued use of standardized responses, such as "*no covered violation*" or "*remedy issued*", together with the lack of an appeal mechanism, further determines doubt on the real effectiveness of this system.

The EDPB also pointed out a less regulated and often overlooked form of government access to data: the purchase of personal information from private entities. This practice, outside the scope of EO 14086, allows U.S. intelligence services to bypass DPF safeguards by acquiring highly sensitive data, such as geolocation, online browsing history, or biometric identifiers, via commercial markets[268].

The commercial and operational dimension of the DPF, also evaluated by the EDPB, raised further concerns. In particular, the report highlights the absence of systematic and independent oversight by U.S. authorities over certified companies. As already observed under the previous Privacy Shield, the lack of proactive enforcement and ex officio investigations makes compliance more formal than substantive. Furthermore, the handling of data by organizations that have withdrawn or let their certification expire remains opaque and poorly accountable, violating key GDPR principles. The extremely low number of complaints from EU citizens in the first year of DPF operation is not a sign of success, but rather as evidence of an ineffective redress system, due to limited accessibility and lack of awareness among data subjects.

Additional concerns relate to the lack of operational guidance for onward transfers to non-adequate third countries, and the divergence in the interpretation of "*HR Data*" between U.S. and EU

[268] European Data Protection Board, Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, Version 1.1 (2024) 12-22.

authorities. In particular, while the EDPB adopts a broad, employment-based interpretation, the U.S. Department of Commerce tends to restrict it to intra-group transfers. This regulatory divergence creates legal uncertainty and risks undermining data protection in the employment context.

Lastly, at the domestic legal level, there is still no comprehensive federal data protection law, despite privacy legislation being adopted in twenty U.S. states. Moreover, the failure to address automated decision-making protections under Article 22 GDPR, and the weakening of FTC regulatory authority by the Loper Bright ruling all contribute to the systemic fragility of the framework[269].

Taken as a whole, these factors reveal a fragile, fragmented and structurally unbalanced framework, casting doubt on the resilience of the adequacy decision in the face of future judicial scrutiny. The risk of a new intervention by the Court of Justice, a potential Schrems III, appears increasingly plausible.

[269] Ibid 7-11.

Chapter 4

Comparative Perspective beyond the West: Data Protection Models in China and Japan

4.1 The Chinese Approach to Data and Privacy Protection

In recent years, the People's Republic of China has adopted a comprehensive set of legal measures aimed at regulating the protection of personal data, marking a significant evolution within a legal context traditionally oriented towards state control of information by establishing complex regulatory framework which, although partly inspired by European models, reflects profoundly different priorities involving national security, cyber-sovereignty, and the central role of the Communist Party in the digital sphere.

The protection of personal data in China has not developed as a tool for safeguarding the individual as a holder of fundamental rights, but rather as a guarantee for the citizen-consumer.

Unlike the European Union, which bases the protection of personal data on the recognition of the right to privacy as a fundamental right, the Chinese system adopts a structurally different approach, both normatively and conceptually. In fact, in China, it is not entirely accurate to speak of a coherent regime for the protection of personal data, but rather of a set of sectoral and fragmented provisions that only began to take on a certain systemic coherence with the adoption of the Personal Information Protection Law (PIPL) in 2021.

The centrality of the economic-commercial aspect clearly emerges from the fact that the rules on personal information protection were primarily designed to regulate data processing in the context

of market activity and e-commerce, rather than to recognize an autonomous dimension of privacy as an inviolable personal right. The figure of the active and self-determined "*data subject*," which is central in the European GDPR, is absent: the individual is rather seen as a passive recipient of measures aimed at promoting governance and collective welfare. Even mass surveillance, such as the widespread presence of cameras in urban areas, is not interpreted as a threat to privacy, but as a tool of efficiency and public order. In this context, speaking of a true data protection regime is inappropriate: the existing provisions belong more to the realm of consumer law than to that of fundamental rights.

By contrast, privacy protection, although it does not carry the same weight as in the European context, where it is seen as a right to liberty and autonomy, is effectively recognized in Chinese law, both at the constitutional and civil level, however associated with concepts such as personal dignity, honor, or reputation, rather than with informational self-determination. This reflects a profoundly different legal and cultural approach, in which data protection serves collective interests, such as public order or national security, more than individual freedoms[270]. While in liberal democracies fundamental rights are conceived as instruments to limit state power, in the Chinese model, instead, rights are seen as emanating from the state itself and granted in accordance with national priorities. This explains why privacy and data protection in China are often framed not as shields against state intrusion, but as tools of social regulation in the service of national stability and governance[271].

[270] P de Hert and V Papakonstantinou, *The Data Protection Regime in China: In-depth Analysis for the LIBE Committee*, Policy Department C - Citizens' Rights and Constitutional Affairs, European Parliament (2015) 13-16.

[271] W Li and J Chen, 'From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China' (2024) *Computer Law and Security Review* 16.

4.1.1 State Surveillance and Privacy in China

The People's Republic of China has established a centralized and pervasive surveillance regime in which the protection of privacy is systematically subordinated to state power. This framework is built on a legal and technological architecture that integrates mass data collection, extensive tracking, and political control of information, maintaining national security as the guiding principle. While presenting the data protection regime as pursuing a dual goal of safeguarding national security and promoting economic growth, the regime does so at the expense of personal information protection, which is undermined by the government's near-unrestricted access to personal data.

In recent years, data have been elevated to the status of a strategic resource, described as the main engine of the country's digitalization, while privacy protection has remained subordinate to the safeguarding of broad and vague concepts such as important data and core data, which serve to justify state intervention for security reasons[272].

The Party-state does not merely collect data: it actively employs it to shape social behavior and public opinion, turning surveillance into an instrument of political and cultural control. In this perspective, data regulation serves to maintain and optimize the state's capacity to monitor, direct, and intervene in citizens' lives, rather than to limit it.

China's surveillance infrastructure combines traditional identification systems with advanced monitoring technologies. Personal identification is required for most public services, and the principle of Real Name Registration ensures that all online activity is linked to verifiable identities. The Internet is conceived not as a space for openness but as a controlled environment, where unacceptable communications are swiftly removed and where both individuals and providers bear

[272] A He, State-Centric Data Governance in China (CIGI Papers No. 282, 2023) 1-3.

direct liability. Beyond censorship, the government actively shapes public debate by employing a vast army of trained commentators, the *fifty cent party*, to steer online discussions in favor of official positions[273].

The rapid acceleration of datafication, driven by both state and private actors, has made Chinese citizens more vulnerable to privacy intrusions. A wide range of surveillance tools, such as biometric recognition, geolocation, and health-tracking applications, have been integrated into everyday governance, reshaping social control through technology.

This network is used for both legal and extralegal purposes: from monitoring and profiling Uyghurs in Xinjiang to locating fugitives in public spaces[274]. It has also been deployed during the pandemic with health codes that enabled real-time movement tracking, sometimes for purposes unrelated to public health, requiring citizens to use mobile applications that, based on personal and geolocation data, determined access to public spaces or mandated quarantine, with information shared directly with the police[275].

Furthermore, another notable initiative is the social credit system, which relies on the large-scale integration of personal data to shape behavior and enforce compliance with state rules[276]. The Party-state's economic development goals have also fueled datafication and data dependency. In particular, a permissive regulatory environment, supported by tax incentives and government-sponsored incubators, has allowed platforms to accumulate vast amounts of online data, while other operators collected information from the physical world at a faster rate than in other countries.

---

[273] A Bartow, 'Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China' (2013) 74 *Ohio State Law Journal* 868-870.
[274] M Jia, 'Authoritarian Privacy' (2024) 91(3) *University of Chicago Law Review* 767.
[275] Ibid. 775.
[276] In its pilot phase, the social credit system primarily created state-maintained blacklists to penalize unlawful behavior, such as banning individuals from high-speed train travel for failing to repay court-ordered debts. In some local experiments, individuals and businesses were rated according to numerical scores based on a wide range of behaviors.

Giants such as Alibaba, Tencent, and Baidu have come to possess deeper knowledge of their users' lives than that held by Facebook, Google, or Amazon[277].

On the regulatory side, the regime has mostly free rein to access all data including personal data in the name of national security[278]. Instruments such as the Personal Information Protection Law (PIPL) contain numerous exceptions to consent (art. 13), including a catch-all provision allowing the collection and processing of personal data in "*other circumstances provided in laws and administrative regulations*," thereby giving the state wide latitude to intervene[279]. Digital platforms, previously allowed to expand freely, are now subject to stringent control, as shown by the Didi Chuxing case[280]. The result is a system in which the collection and analysis of data are inseparable from political control, and in which data protection serves to regulate private and foreign actors, not to limit the state itself, but rather to reinforce the characteristics of China's surveillance state[281].

The concept of data security in China differs from that prevailing in democratic countries: it is aimed primarily at protecting data from external threats or abuses by private actors, but not at limiting government access. In this context, privacy protection becomes part of a broader strategy of social control, in which the collection and analysis of data are inseparable from the exercise of political power.

This model has resembled the characteristics of a surveillance state capable of monitoring, directing, and intervening in the daily lives of citizens, through the combination of permissive legal instruments, advanced technologies, and a centralized political management of information.

---

[277] Ibid. 768.
[278] A He (n 3).
[279] Ibid. 5-8.
[280] Ibid. 11-13.
[281] Ibid. 17.

4.1.1 Normative framework and Legislative reforms

From a normative standpoint, it is important to note that the Constitution of the People's Republic of China does not explicitly recognize either the right to privacy or the protection of personal data. The only constitutional provisions that may be indirectly linked to privacy protection are Article 40, which guarantees the freedom and confidentiality of correspondence, limiting such protection only in cases of criminal investigation or national security, and Article 35, which protects freedom of expression.

Additional protections are found in sectoral laws: for example, Article 4 of the 1987 Postal Law reiterates the inviolability of private correspondence. In civil law, Article 101 of the General Principles of Civil Law (1986) protects reputation and prohibits defamation, while the 1988 Judicial Interpretations include unauthorized disclosure of private information as a violation of the right to reputation. In criminal law, Article 246 of the Criminal Code provides sanctions for serious insult or defamation, and the Tort Liability Law (2009) allows citizens to seek damages in case of privacy violations[282].

Despite this normative background, judicial remedies for privacy protection remain limited and often ineffective. Civil or criminal actions are rare and usually limited to high-profile cases such as identity theft or serious defamation, while litigation specifically related to unlawful data processing remains marginal. This reflects a legal culture that does not conceive of individuals as autonomous data subjects. Unlike the European model, where privacy and data protection are normatively distinct, in China this distinction is more blurred: privacy is sometimes invoked as a substitute for data protection, but it is not legally equivalent to it.

[282] Privacy International and Law and Technology Centre of the University of Hong Kong, The Right to Privacy in China: Stakeholder Report, Universal Periodic Review, 17th Session – China (2013) 4.

Theoretically, the Chinese system today appears to be moving toward a dualist model, which distinguishes, albeit not absolutely, between the right to privacy and the protection of personal information. This distinction is formally established in civil law, particularly through the 2017 General Provisions and the 2020 Civil Code, which recognize privacy as a personality right (Art. 110) and personal information as a legal interest (Art. 111). The 2015 Cybersecurity Law also defines personal information broadly[283], while the 2020 Civil Code (Art. 1032) frames privacy as the private sphere of life, including spaces, activities, and information not intended for disclosure. Article 1034 further clarifies that private information within personal data must be handled according to privacy rules, otherwise general data protection rules apply. This legal architecture suggests a binary, parallel protection between privacy and personal data.

However, jurisprudential practice continues to show overlap and ambiguity. For instance, a photograph of a person changing clothes, if not anonymized, qualifies as both personal data (being identifiable) and private content. Once anonymized, it loses its qualification as personal data but remains private information deserving protection. Thus, privacy may exist without personal data, but not always the reverse. Moreover, private information which are not recordable or identifiable[284], remain outside the legal definition of "*personal information*," and therefore escape the protection provided by data processing laws.

While the civil law framework appears to be evolving toward a dualist structure, the Chinese criminal law remains monist. In this context, privacy violations are prosecuted solely through provisions on unlawful data processing, without recognizing privacy as an independent legal interest.

[283] Article 76 of the Cybersecurity Law defines personal information as any kind of data, whether recorded electronically or not, that can identify a person, either alone or in combination with other elements.

[284] A whispered conversation, an intrusive look, or a physical interference in a private space.

Several amendments to the Criminal Law of 1979 have introduced specific offences such as the *unlawful selling, provision,* or *acquisition of personal information*, especially by public authorities or operators in key sectors. However, as prosecutions are confined to cases involving exceptionally large volumes of data or demonstrable serious harm, the actual enforcement of these provisions remains rare, significantly limiting their deterrent effect and practical effectiveness[285].

Despite these developments, the Chinese criminal law system continues to use provisions on the unlawful processing of personal data to punish conduct that directly violates privacy. The absence of a distinct criminal offence for privacy violations leads to two major consequences: first, a violation of the principle of legality (*nulla poena sine lege*), as norms originally conceived for other purposes are inappropriately extended; second, a regulatory gap that leaves many intrusions into private life unpunished when they do not involve recorded or identifiable data. This internal contradiction between legal approaches weakens the overall protection of the individual and confirms the urgency of reform that recognizes privacy as an autonomous legal interest also in criminal law, as already occurs in jurisdictions such as the European one[286].

Beyond civil and criminal law, consumer protection legislation has become a major pillar in the regulation of personal information. The 2012 Decision of the Standing Committee of the National People's Congress was a turning point, introducing principles of legality, legitimacy, necessity, and consent, and extending privacy obligations to both the private and public sectors. Despite its symbolic value, it was limited to online contexts, lacked enforceable rights such as access or rectification, and did not create an independent authority[287].

[285] W Li and J Chen (n 271) 14.
[286] Z Guo, J Hao and L Kennedy, 'Protection Path of Personal Data and Privacy in China: Moving from Monism to Dualism in Civil Law and Then in Criminal Law' (2024) 52 *Computer Law & Security Review* 105928 3-12.
[287] P de Hert and V Papakonstantinou (n 270) 20.

Still, it set the stage for further reforms, such as the 2013 amendment of the Consumer Protection Law, which added provisions on personal data processing, consent, transparency, and confidentiality—though often vaguely drafted and permissive, often allowing for implied or opt-out consent[288]. Despite these shortcomings, this consumer-oriented approach laid the groundwork for more comprehensive legislation, culminating in the PIPL of 2021.

At the international level, China has signed but not ratified the ICCPR, participates in the Asia-Pacific Economic Cooperation (APEC) Privacy Subgroup[289], and cooperates with the OECD on data initiatives. However, despite receiving invitations from the Council of Europe to sign and ratify international data protection conventions, it has not adhered to binding instruments like Convention 108+, leaving it free from international obligations in the field of data protection[290].

These gaps and inconsistencies paved the way for a new phase of reform, which between 2017 and 2021 introduced a set of comprehensive laws that profoundly reshaped China's data governance, transforming a regulatory landscape that had developed incrementally since the 1990s. Early initiatives such as the Golden Projects[291] and the 2007 establishment of the Multi-Level Protection System (MLPS) had already framed data management in terms of administrative efficiency, social stability, and national security. Over time, the leadership's awareness grew regarding the challenges of digitalization and the risks of data abuse. Yet, early legislative attempts, ranging from sectoral provisions to rules on consent, criminal liability, or data localization, remained fragmented

[288] W Li and J Chen (n 285).

[289] Although a member of APEC, being the APEC Privacy Framework a non-binding instrument that operate sentirely on the basis of consensus and voluntary commitments, it does not enforce obligations, but rather reflect aspirational goals of cooperation: Privacy International and Law and Technology Centre of the University of Hong Kong (n 282) 5.

[290] P de Hert and V Papakonstantinou (n 270) 16.

[291] A series of state-led programmes to digitize government functions and build nationwide information networks.

and weakly enforced. The creation of the Cyberspace Administration of China (CAC) in 2012 centralized competences and prepared the ground for more coherent reforms[292].

Building upon these foundations, the Chinese legislature adopted the Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information Protection Law (2021), which together created, for the first time, a structured and comprehensive framework addressing network security, data governance, and personal information. This cycle was further complemented by the Regulations on Network Data Security Management (2024), which systematize existing norms and close important gaps, particularly in relation to cross-border transfers, compliance duties for large processors, and the enforcement of PIPL rights. These reforms were not only a response to technical and economic needs, but also by strategic objectives such as the promotion of "cyber-sovereignty" and the integration of data governance into the national security agenda, while formally recognizing certain rights for individuals within a framework that continues to prioritize state interests.

4.1.2.1 The Cybersecurity Law

Adopted in November 2016 and entering into force on 1 June 2017, the *Cybersecurity Law* was the first comprehensive statutory instrument to consolidate rules on network security, critical information infrastructure (CII)[293] protection, and personal information handling in China. Structured into seven chapters and seventy-nine articles, it combines general provisions with

[292] R Creemers, 'China's Emerging Data Protection Framework' (2022) *Journal of Cybersecurity* 2-4.

[293] Under the CSL, CII refers to network facilities and information systems in important sectors such as public communications, energy, transport, finance, public services, and national defense, whose destruction, loss of function, or data leakage could seriously endanger national security, the national economy, or public interest (Art. 31).

sector-specific rules on network safety, CII protection, personal information security, obligations of network operators, and emergency management[294].

Its objectives include the protection of "*cyberspace sovereignty, national security, and public interests" alongside the safeguarding of the 'lawful rights and interests' of individuals and organizations and the promotion of informatization*" (Art. 1)[295]. The CSL applies to all activities related to the construction, operation, maintenance, and use of networks within the PRC (Art. 2)[296], and defines *network operators* broadly to include *owners, administrators, and network service providers*[297], extending the scope beyond traditional telecommunications to any entity offering products or services via the Internet, including individuals and organizations operating online platforms (Art. 76).

Personal information is defined as "*information that can be used, alone or in conjunction with other information, to determine the identity of a natural person, including but not limited to a person's name, date of birth, identity card number, biometric information, address, and telephone number*" (Art. 76)[298]. Articles 40–43 require lawful, proper, and necessary collection and use of personal information, informing users of the purposes, methods, and scope of processing and obtaining their consent. Data subjects are granted the rights to access, rectify, and delete their personal information, and prohibit disclosure without consent or anonymization. In the event of a

[294] A Qi, G Shao and W Zheng, 'Assessing China's Cybersecurity Law' (2018) 34 *Computer Law & Security Review* 1344.
[295] Cybersecurity Law of the People's Republic of China (China Securities Regulatory Commission) 1.
[296] Ibid.
[297] The CSL imposes on them general obligations of security and compliance (Arts 10 and 21), user identification through real-name registration (Art 24), the protection of personal information (Arts 40–43), data localization and restrictions on cross-border data transfers (Art 37), control over network products and services (Arts 23 and 35), and the duty to provide technical cooperation to the authorities (Art 28).
[298] Ibid 22.

breach or risk thereof, operators must take remedial measures, notify affected individuals, and report to the competent authorities. While these provisions impose formalized privacy obligations on private-sector actors, the CSL grants public authorities wide-reaching access to personal data. Article 28 requires network operators *to provide technical support and assistance* to public security and state security agencies for national security and criminal investigations. This dual logic, protecting personal information while embedding it in a state-centric governance model, creates structural vulnerabilities and a heightened risk of data leakage[299].

Article 37 introduces a data localization requirement, obliging CII operators to store personal information and "*important data*" domestically, with cross-border transfers subject to a security assessment by competent authorities[300]. The CSL thus provides a legal basis for two strands of data protection: personal information and important data. While the concept of personal information is expressly defined in the law, the notion of important data remains undefined in the implementing draft measures. This ambiguity also affects the practical application of the security assessment requirement for cross-border data transfers, as the scope, procedures, and criteria for such assessments remain unclear.

Given this uncertainty, it is difficult to fully assess the potential impact of the data localization rules on both domestic and foreign businesses[301].

Beyond Article 37, further criticisms target the overly broad definitions of network operators and critical information infrastructure, which generate regulatory uncertainty and extend heavy compliance duties to a wide range of actors. Provisions on real-name registration and mandatory technical assistance to security agencies raise additional concerns over privacy erosion and the

[299] JA Lee, 'Hacking into China's Cybersecurity Law' (2018) 53 *Wake Forest Law Review* 86-89.
[300] Cybersecurity Law of the People's Republic of China (n 295) 10.
[301] A Qi, G Shao and W Zheng (n 294) 1353.

chilling effect on freedom of expression.

This combination of vague terminology, undefined key concepts, and far-reaching state powers has led some commentators to view the CSL not merely as a cybersecurity framework, but as a versatile instrument for industrial policy and political control[302]. The absence of strong democratic checks and balances creates a wide discretionary space for enforcement, raising the risk of selective application against dissenting individuals or companies perceived as adversarial to the state[303]. As a result, while the CSL formally recognizes certain rights for individuals, these remain subordinated to the overarching objectives of cyber-sovereignty and national security, reinforcing a state-centric model of data governance.

4.1.2.2 The Data Security Law

In the years following the entry into force of the Cybersecurity Law, the implementation of its data-related provisions encountered obstacles, while the importance of the central role of data in economic, social, and governmental processes grew significantly. In 2020, the Central Committee of the Chinese Communist Party formally recognized data as a factor of production on par with land, capital, and labor, consolidating its strategic value for national development. At the same time, the demand for more robust regulation increased, particularly with regard to large digital platforms, whose practices of algorithmic recommendation and profiling were considered potentially capable of influencing content distribution and encouraging undesirable consumer behaviors.

A significant development during this phase was the creation, in 2019, of the App Governance

[302] JA Lee (n 299) 71-77.
[303] Ibid. 98.

Working Group[304], alongside standardization bodies and industry associations. This group developed standards for the use of data in mobile applications and carried out enforcement campaigns, such as Clean Net 2019, which resulted in thousands of judicial proceedings. From 2020 onwards, regulatory action took on a more proactive orientation, aiming to shape the digital economy, strengthen the security of critical infrastructure, and regulate strategic sectors such as online platforms and fintech services.

It is within this context that the Data Security Law (DSL) was adopted in June 2021 and entered into force on September 1 of the same year[305].

The Data Security Law (DSL) is intended as a framework law for data regulation in China, with a dual objective: on the one hand, to regulate the processing and security practices of all data, personal and non-personal, with the exception of state secrets, to protect the rights of individuals and organizations; on the other, and above all, to preserve digital sovereignty and national security (Art. 1). Article 4 further establishes a link between data security and the broader concept of national security, thus expanding the scope of the law well beyond the mere technical protection of information.

The law has a broad scope of application extending extraterritorially: activities involving data processing carried out abroad fall under the DSL if deemed detrimental to national security, the public interest, or the rights of Chinese citizens/organizations, thereby reinforcing the principle of cyber-sovereignty (Art. 2)[306].

The governance system is centralized: a central institution for national security coordinates the

[304] Which brought together the Cyberspace Administration of China, the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS), and the State Administration for Market Regulation (SAMR).
[305] R Creemers (n 292) 5-6.
[306] China Law Translate, Data Security Law (2021).

implementation of the law, while the Cyberspace Administration of China, public security authorities, and sectoral regulators exercise specific competences, avoiding overlaps and ensuring uniform enforcement[307].

The law explicitly emphasizes the strategic role of data both in reforming governance processes and as a lever for the next phase of China's economic rise. At the same time, it recognizes that these processes increase the country's vulnerability surface, making reinforced protection necessary. The DSL's response is the creation of an integrated system covering all data held by individuals, businesses, or public entities[308]. It also provides broad definitions, aiming to widen the law's scope of application in Article 3 of the concepts of "*data*" as any record of information in electronic or other form, "*data handling*" as any activity of managing, transmitting, or disclosing information, and "*data security*" as any aspect related to the protection of information[309].

A cornerstone of the DSL is the establishment of a "*categorical and hierarchical*" data protection system, which divides data based on their importance to economic and social development and their potential impact on national security, the public interest, or the rights of citizens and organizations in the event of alteration, destruction, loss, or unlawful use. Within this framework, there are two main categories[310]: the category of *important data*, introduced in the CSL but never clearly defined, for which the DSL provides for the creation of national, regional, and sectoral catalogues[311]; and the category of *core national data*, which includes information vital to national security, strategic sectors of the economy, and fundamental public interests, and which falls within

[307] J Chen and J Sun, 'Understanding the Chinese Data Security Law' (2021) 2 *Int Cybersecurity Law Review* 210.
[308] R Creemers (n 292) 6.
[309] A Kokas, 'China's 2021 Data Security Law: Grand Data Strategy with Looming Implementation Challenges' (*China Leadership Monitor*, Winter 2021, Issue 70, 1 2021) 6-7.
[310] R Creemers (n 308).
[311] J Chen and J Sun (n 307) 211.

the broader category of important data. The DSL entrusts local governments and sectoral authorities with the task of preparing data classification catalogues, structured on two levels, one national and others regional or sectoral, and establishes three main mechanisms:

- a system for risk assessment, reporting, information sharing, monitoring, and early warning;
- an emergency response system;
- a data security review mechanism, allowing the examination of any data processing activity potentially harmful to national security, without the possibility of appeal[312].

The DSL provides strict rules for the cross-border transfer of important data, subjecting it to a security assessment by the CAC or other measures approved by the competent authorities (Art. 31)[313]. For operators of Critical Information Infrastructure (CIIO), there is an obligation to store such data within China, with transfers abroad permitted only when strictly necessary for business activities and with prior cooperation with the CAC, as provided by the Cybersecurity Law. For non-CII data, the specific rules are determined by the CAC and other bodies.

Furthermore, since the DSL includes personal data within the general definition of "*data*," cross-border transfers are also subject to the requirements of the PIPL, including impact assessments, separate consent, localization measures, or standard contracts[314].

Although it has a very broad scope that also covers non-personal data, the DSL significantly affects the protection of personal data in China, both through its extended definition of data its restrictions on cross-border transfers and stringent security requirements. Its close connection with national security, the wide interpretative discretion left to the authorities, and the absence of uniform

[312] R Creemers (n 292) 6-7.
[313] China Law Translate (n 306).
[314] J Chen and J Sun (n 307) 213-217.

technical standards, however, raise issues of legal certainty and predictability, especially for international operators.

4.1.2.3 The Personal Information Protection Law (PIPL)

The Personal Information Protection Law (PIPL), which came into effect on 1 November 2021, represents the first comprehensive regulation on personal data protection adopted by the People's Republic of China. It complements an existing legislative framework already characterized by the Cybersecurity Law of 2017 and the Data Security Law of 2021, forming part of a broader regulatory strategy that intertwines privacy protection with safeguarding national security and exercising centralized state control over information flows[315].

The PIPL constitutes an evolution of the trends already initiated with the CSL of 2017, significantly expanding its scope and the level of regulatory detail. Unlike the CSL, which limited personal data protection to "*network operators*" and introduced data localization requirements only for operators of critical infrastructure, the PIPL applies to all "*personal information handlers*", encompassing both private entities and government bodies. In doing so, the legislator has broadened the legal bases for processing, including, alongside the data subject's consent, additional grounds such as handling public health emergencies, conducting news reporting in the public interest, or other cases provided for in laws and administrative regulations[316].

The law is structured into 8 chapters and 74 articles, setting out in detail the principles, legal bases, data subject rights, obligations of handlers, and enforcement mechanisms, with an approach that combines the objectives of individual protection, economic development, and safeguarding national security.

---

[315] G Greenleaf, 'China's Completed Personal Information Protection Law: Rights Plus Cyber-security' (2021) UNSWLRS 91, (2021) 172 *Privacy Laws & Business International Report* 1.
[316] R Creemers (n 308).

The purpose of the legislation is stated at Article 1 "*to protect rights and interests in personal information, regulate the processing of personal information and to promote the reasonable use of personal information"*. It stipulates that the processing of personal information must abide by the principles of legality, legitimacy, justice, integrity, minimum necessity, openness and transparency, and the purposes of processing shall be explicit and reasonable. Moreover, the PIPL mandates that processing be limited to its stated purpose, with collection restricted to the minimum necessary and carried out in a way that minimizes any potential impact on individual rights and interests. It prohibits excessive collection, requires data accuracy to prevent harm, and forbids unlawful collection, use, disclosure, or sale of personal information, as well as activities that could endanger national security or the public interest[317].

In addition to its domestic scope, the PIPL applies extraterritorially to the processing of personal information outside the territory of the People's Republic of China when such processing involves providing products or services to individuals located in the PRC, or analyzing and assessing their behavior. It also extends to "*other situations provided for by law or administrative regulations*"[318], a provision that allows the scope of extraterritoriality to be further expanded through subsequent legal or regulatory measures. Entities engaging in such processing from abroad are required to designate a representative within the PRC and communicate the representative's identity to the relevant supervisory authorities. Additionally, similar requirements for appointing a representative apply to any organization processing personal information in volumes specified by the Cyberspace Administration of China[319], a category likely to encompass major platform operators.

Beyond its extraterritorial scope, the PIPL also establishes stringent requirements on data

[317] China Briefing Team, 'The PRC Personal Information Protection Law (Final): A Full Translation' (2021) arts 5–10.
[318] Ibid. art 3.
[319] Ibid. arts 52-53.

localization and cross-border transfers, set out in Chapter III. Under Article 40, Critical Information Infrastructure Operators and other handlers that process personal information above thresholds set by the Cyberspace Administration of China must store a copy of such data within Chinese territory. According to Article 38, cross-border transfers are permitted only if one of the following conditions is met: (i) the handler passes a CAC-organized security assessment; (ii) the handler obtains personal information protection certification from an accredited body; (iii) the handler concludes a contract with the overseas recipient using standard terms issued by the CAC; or (iv) another condition provided for by PRC laws or regulations applies.

In all cases, three further requirements must also be satisfied: the transfer must be genuinely necessary for business purposes, the explicit consent of the individuals concerned must be obtained after clear notification, and a Personal Information Protection Impact Assessment (PIPIA) must be conducted and retained on record.

Furthermore, Article 41 prohibits the provision of domestically stored personal information to foreign judicial or law enforcement authorities without prior approval from competent PRC bodies. Articles 42 and 43 empower the Chinese government to impose retaliatory measures against countries or companies that adopt discriminatory restrictions against China. Transfers may also be permitted pursuant to international treaties or agreements to which the PRC is a party[320].

Article 4 defines personal information as "*all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, excluding information after anonymization*". The notion of handling is particularly broad, encompassing collection, storage, use, processing, transmission, provision, disclosure, and deletion. A personal information handler is any public or private entity that independently determines the purposes and means of

[320] G Greenleaf (n 315) 4-5.

processing[321].

The scope of application includes very few exceptions: Article 72 excludes only processing carried out by natural persons for personal or family purposes; other exemptions, such as those for statistical or archival purposes by public authorities, are permitted only if conducted in accordance with the law. The PIPL also allows, within reasonable limits, the use of personal information that has been made public by the data subject or otherwise lawfully disclosed, unless the individual has expressly objected; where such information significantly affects individual rights and interests, consent must nonetheless be obtained. Special attention is given to *sensitive personal information*, which receives heightened protection and is defined as information which, if leaked or illegally used, may infringe upon human dignity or cause serious harm to personal or property security. This category includes *biometric data, religious beliefs, medical health information, financial accounts, location tracking, and the personal information of minors under the age of 14*. Processing such data requires separate and specific consent (Art. 29), alongside the adoption of enhanced protective measures. When processing the personal information of minors, handlers must obtain the consent of parents or other legal guardians and establish dedicated internal policies and procedures for managing such information[322].

Chapter IV of the PIPL is dedicated to the *Rights of Individuals in Activities of Processing Personal Information* and sets out a comprehensive framework of protections for data subjects. These include the rights of access, rectification, erasure, restriction, and objection to processing. The law further provides for data portability, rights in relation to automated decision-making, such as the right to refuse profiling and to request explanations, post-mortem rights enabling close relatives to exercise certain rights on behalf of the deceased, and the right to bring legal action against handlers

[321] China Briefing Team (n 317) art 75.
[322] TrustArc, 'China PIPL Whitepaper' (2021) 3.

who unlawfully deny the exercise of rights[323].

Beyond individual rights, Chapter 5 imposes specific organizational and governance obligations on personal information handlers. These include establishing internal governance structures, implementing data classification procedures, adopting technical safeguards such as encryption and de-identification, developing incident response plans, and providing regular staff training. Handlers that process personal information above thresholds set by the CAC are also required to appoint a personal information protection officer and register their details with the competent authority.

The law also mandates the performance of a Personal Information Protection Impact Assessment (PIPIA) in certain high-risk scenarios, including the processing of sensitive personal information, cross-border data transfers, the use of automated decision-making systems, and other operations likely to have a significant impact on individuals' rights and interests. These assessments must be documented and retained for at least three years for potential inspection by supervisory authorities[324].

4.1.2.4 The Regulations on Network Data Security Management

The Regulations on Network Data Security Management, adopted by the State Council on 30 September 2024 and in force since 1 January 2025, establish a detailed framework for managing the security of a broad spectrum of data, including Personal Information (PI) and important data, while strengthening the supervisory powers of the competent authorities. This legislative measure acts as an implementing and integrative development of China's three cornerstone data governance laws: the Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information

[323] G Greenleaf (n 315) 2.
[324] China Briefing Team (n 317) arts 51-56.

Protection Law (2021)[325].

While the CSL, DSL, and PIPL each regulate specific aspects of cybersecurity, data security, and PI protection, the Regulations consolidate their common requirements and extend them to the broader category of network data processing activities. This category covers all electronic data processed via networks, not only PI and important data, and explicitly addresses emerging challenges such as data scraping and generative AI training, which were previously subject only to interim measures.

The Scope and definitions of the Regulations clarify that "*network data*" is any electronic data processed through networks, excluding data stored on physical media, and that a "*network data processor*" includes all entities that determine processing purposes and methods, a wider concept than the PIPL's PI processor.

The extraterritorial scope mirrors the triggers in Article 3(2) PIPL and Article 2(2) DSL, applying not only to overseas processing of PI for Chinese individuals, but also to network data processing abroad that may harm China's national security, public interest, or citizens' lawful rights.

In the section on General Requirements, the Regulations incorporate the common obligations already established under the CSL, the DSL, and the PIPL, extending them to all network data processing activities and the continuity principle already present in the PIPL for the transfer of personal information for network data processors.

With regard to cross-border transfers of personal information, Article 35(6) allows the transfer of PI outside the PRC without undergoing a security assessment, obtaining certification, or concluding and filing a standard contract, when the transfer is necessary to fulfil statutory duties or obligations. However, its scope remains unclear to obligations under foreign law. The exemption

[325] J Gong, M Dong e J Che, 'An In-depth Analysis of China's Network Data Security Regime – Part II: Detailed Look at Data Protection Requirements' (*Bird & Bird*, 2025).

applies solely to PI and not to network data in general, unless such network data contains PI. Article 36 also provides that where the PRC is a party to an international treaty or agreement containing provisions on the conditions for providing PI abroad, those provisions may prevail[326].

On personal information protection, the Regulations extends PIPL requirements. On notice, processors must provide clear, accessible privacy notices stating purposes, methods, categories of PI, retention periods or criteria, data recipients (in list form), and procedures for exercising rights. Moreover consent rules are refined as sensitive PI requires separate consent, and parental/guardian consent is needed for minors under 14. The right to data portability, under Article 25, is allowed when identity verification, legal basis, technical feasibility, and protection of third-party rights are ensured. Foreign PI processors falling under the Regulations' extraterritorial scope must appoint a local representative or set up a body in China and file contact details with the municipal CAC.

In line with the DSL, the Regulations define "important data" through sectoral or regional catalogues issued by the competent authorities. Important data processors must conduct annual risk assessments (Art. 33) for submission to the CAC and provincial authorities, and carry out prior risk assessments (Art. 31) before any transfer, entrustment, or joint processing to ensure legality, necessity, recipient reliability, and adequate safeguards .

Moreover, large PI processors, defined as those handling PI of more than ten million individuals, are required to appoint a network data security officer, establish a dedicated internal management body, and conduct risk assessments before providing data to third parties[327].

Sector-specific rules require AI service providers to secure the management of training data, removing or anonymizing any PI contained within such datasets, and preventing data security risks.

[326] Latham & Watkins, 'China Clarifies Privacy and Data Security Requirements in Network Data Security Management Regulations' (*Client Alert Commentary*, 2025) 2-4.
[327] Ibid. 4-6.

The use of automated tools, such as web crawlers or robotic process automation, must be assessed for its potential impact and must not disrupt others' networks or services. Large network platforms, defined as those with at least fifty million registered users or ten million monthly active users, must publish an annual social responsibility report on PI protection. Finally, providers of services to government bodies, critical information infrastructure operators, or public service systems must adopt stricter protection standards and cannot use entrusted data without consent[328].

These Regulations not only systematize existing norms but also address significant gaps, particularly in cross-border data governance and in the practical enforcement of PIPL rights. They introduce new mechanisms, such as mandatory checklists in PI notices, a dual regime of annual and transaction-specific risk assessments for important data, and the partial extension of important data obligations to large PI processors, that expand state oversight and raise compliance expectations. However, several aspects remain unclear, notably the scope of the new cross-border exemption and the criteria for designating important data, creating potential compliance uncertainty. By extending certain important data duties to large PI processors, the Regulations also broaden state control over the private sector beyond the boundaries previously set by the DSL and PIPL.

Finally, their effective implementation will depend on the issuance of further instruments, in particular the sectoral catalogues for identifying important data, which are still largely missing.

4.1.3 The Chinese Model of Data Protection: A Comparative Lens

When compared to the European model embodied in the GDPR, the Chinese approach reveals both formal convergences and profound substantive divergences. At the normative level, the GDPR is firmly rooted in the recognition of data protection as a fundamental right, enshrined in Article 8 of

[328] Ibid. 7-8.

the Charter of Fundamental Rights of the European Union and Article 16 TFEU. By contrast, the Chinese framework has followed a different trajectory: privacy was never entrenched as a constitutional right, but for decades remained tied to the protection of reputation, later reinforced by the Tort Liability Law of 2009, and only explicitly acknowledged as a statutory entitlement in the 2021 Civil Code. This evolution reflects the gradual transition from a general notion of privacy to an explicit recognition of personal data protection as a legal category, embedded in a stratified body of civil, criminal, consumer protection, and cybersecurity law, culminating in the adoption of the CSL, DSL and PIPL. Unlike the GDPR's unitary and rights-based foundation, these instruments frame personal information protection primarily as a tool of governance, serving national security, economic modernization, and state control over the digital sphere[329].

This divergence manifests itself most clearly in the role of the State. Under the GDPR, public authorities are subject to strict limitations and judicial oversight whenever they interfere with personal data, and independent supervisory bodies (national DPAs and the EDPB) are empowered to enforce compliance uniformly across the Union. By contrast, in China, the State enjoys virtually unrestricted access to personal information on broad and vague grounds such as national security or public interest. At the same time, private actors and foreign companies are subjected to stringent obligations of compliance and data localization, while enforcement is entrusted to agencies such as the Cyberspace Administration of China, which are not independent but structurally subordinated to the Party-state. In this sense, Chinese data protection laws operate primarily to discipline the market and reinforce state sovereignty, rather than to impose substantive limits on state power itself.

Despite their divergences, the GDPR and the PIPL share some formal similarities, such as general

[329] W Li and J Chen (n 271) 14.

principles, basic data subject rights, and extraterritorial scope. Yet key differences persist: the PIPL relies mainly on consent and state-sanctioned exceptions, lacks clear notions like "data processor," and imposes stricter rules on cross-border transfers through data localization and security reviews[330].

Moreover, while the PIPL shows textual overlap with the GDPR, this reflects selective adaptation rather than genuine emulation. China's emphasis on cyberspace sovereignty, limited integration in EU digital markets, and minimal corporate lobbying exclude the conditions for a true Brussels Effect. In this sense, the PIPL is not a manifestation of the Brussels Effect, but rather a case of "*gravity assist*", offering technical reference points while China pursues its own state-centric trajectory [331]. Furthermore, there has been no serious debate about granting China an adequacy decision. As the CJEU has stressed in its case law, adequacy requires strict protection of fundamental rights and limitations on government access to data. Given the scale of state surveillance in China, recognition of the PIPL under the GDPR framework remains unrealistic[332]. These divergences highlight the distinctive trajectory of the Chinese framework when compared with the European model, a contrast that becomes even more evident when set against the American approach.

When compared to the United States, the Chinese framework reveals an almost opposite trajectory in the governance of personal data. The U.S. system is defined by fragmentation, sector-specific statutes, and reliance on consumer protection principles, while the Chinese model embodies a centralized and unitary approach, anchored in state sovereignty and national security.

At the normative level, the United States lacks of a comprehensive federal law on data protection

---

[330] One Trust Dataguidance, Comparing privacy laws: GDPR v. PIPL (PDF), https://www.dataguidance.com/sites/default/files/gdpr_v_pipl_.pdf.
[331] W Li and J Chen (n 271) 6-10.
[332] Ibid. 4

and instead relies on sectoral statutes, complemented by state-level initiatives. Enforcement is primarily entrusted to the FTC, which has progressively asserted jurisdiction under its consumer protection mandate. This model reflects a market-driven regulation, where personal data are understood as an economic resource and obligations arise mostly in response to market failures or consumer harm. The ultimate aim is to ensure consumer confidence and fair competition in the digital marketplace.

By contrast China's overarching legislative framework has created a unified framework applying to both private and public actors. These laws operate within a broader paradigm of cyber-sovereignty, where personal information is treated as a strategic resource under strict state oversight.

Yet a crucial asymmetry remains: in the U.S., constitutional guarantees such as the Fourth Amendment limit government surveillance but leave the private sector largely unregulated; in China, the opposite applies, with private actors strictly controlled while state authorities retain broad discretionary powers. This reflects deeper differences. U.S. privacy is treated mainly as a consumer interest, lacking federal recognition as a fundamental right, while in China privacy has only recently been codified in the 2021 Civil Code and remains subordinated to state imperatives. The PIPL confirms this governance-oriented logic by distinguishing between privacy and personal information protection.

Beyond these structural divergences, both China and the United States have faced scandals that exposed the fragility of their systems: in China, the 2017 *Hangzhou bus lending* case revealed misuse of personal information for fraudulent loans, while in the U.S. the *Cambridge Analytica* affair underscored the risks of corporate data exploitation. Despite their divergent regulatory logics, both cases show persistent difficulties in preventing abuses and a growing social awareness of the

broader implications of data protection[333].

Taken together, the two regimes illustrate how data protection can differentiate from the European paradigm: in the United States, as a fragmented and market-driven framework oriented towards consumer interests; in China, as a centralized and sovereignty-driven framework that instrumentalizes personal information for governance and national security. Their divergence from the EU's rights-based model underscores that the global landscape of data protection is shaped less by technical similarities than by fundamentally distinct normative priorities.

4.2 The Japanese Approach to Data Protection

Japan represents a distinctive case in the landscape of personal data protection, as it is one of the few non-European jurisdictions to have obtained, in 2019, an adequacy decision from the European Commission, allowing the free flow of data with the Union. This recognition reflects the progressive convergence of the Japanese system towards European standards, while preserving features that remain closely tied to it legal and cultural context. Built around the Act on the Protection of Personal Information (APPI), first enacted in 2003 and subsequently reinforced by several reforms, the Japanese framework illustrates how a non-European jurisdiction can align with the EU paradigm while retaining a normative identity of its own.

4.2.1 Historical and Normative Foundations

Western legal systems have traditionally conceived privacy as a core individual right, though with different emphases. In the United States, it has been linked primarily to liberty values and protection against governmental intrusion, whereas in Europe it has developed around the principle of human dignity and respect for the individual. The Japanese conception of privacy diverges from

[333] X Chai, 'Comparative Study on Data Protection Between China, The United States and Europe' (2023) 13 *Journal of Education Humanities and Social Sciences* 441-442.

both of these models. Historically, it was not regarded as an inherent individual entitlement but was often perceived as a form of selfishness or excessive individualism, in tension with the communitarian values underpinning Japanese society. Cultural traditions such as *messhi-hoko*, the idea of sacrificing one's private interests for the sake of the public good, and the ethos of *Bushidō*, which emphasized loyalty to the community rather than personal autonomy, illustrate this orientation[334].

In this context, privacy has been understood less as protection from external intrusion and more as the preservation of social harmony and trust. Central cultural notions such as *amae* (the expectation of benevolence from others) and *enryo* (the restraint exercised to avoid burdening others) reflect this relational understanding, where the assertion of strong individual rights may be seen as disruptive. The absence of a native term equivalent to "privacy", with the borrowed word *puraibashii* lacking deep cultural resonance, further confirms that the concept entered Japanese discourse primarily as a Western import. Social practices shaped by group-oriented traditions, from rice agriculture to workplace cooperation, reinforced compromise as a virtue and individual assertiveness as a vice. Even linguistic habits, with the prevalence of implied rather than explicit communication (*tatemae versus hon'ne*), underscore a cultural preference for subtlety and balance over confrontation[335]. Furthermore, the distinction between *uchi* (the inner circle of family and close relations) and *soto* (the outer circle of strangers) reflects a social order in which identity and protection are defined by group membership rather than by an autonomous private sphere. Related concepts such as *seken* (traditional communal values), *shakai* (modernized worldviews imported from the West), and *ikai* (the external sphere associated with danger and impurity) demonstrate

[334] H Miyashita, 'The Evolving Concept of Data Privacy in Japanese Law' (2011) 1(4) *International Data Privacy Law* 230.
[335] Y Orito and K Murata, 'Privacy Protection in Japan: Cultural Influence on the Universal Value' (2005) *Electronic Proceedings of Ethicomp 5* 3-4.

that privacy is often conceived as the management of boundaries between these domains rather than as an absolute individual right[336].

In this light, the Western conception of privacy as the right to be let alone appeared foreign, and at times even contrary to the cooperative spirit of Japanese society. Rather than an inviolable personal domain, Japanese tradition has emphasized a form of informational privacy, understood as the regulation of access and disclosure across social groups and the preservation of social harmony, rather than the assertion of individual autonomy.

On the constitutional level, although the Japanese Constitution is relatively recent, having been adopted in 1946 during the U.S. occupation, it does not explicitly recognize a general right to privacy. Nor did its predecessor, the Meiji Constitution of 1889. Both texts, however, included partial protections: the Meiji Constitution safeguarded the home from unlawful searches, while both constitutions guaranteed the secrecy of communications. The 1946 Constitution, reflecting American influence, further protected freedom of association, thereby extending to a form of associational privacy.

Japanese courts, however, did not confine themselves to these narrow provisions. Instead, they grounded the protection of privacy in the broader and more flexible language of Article 13, which declares that "*all of the people shall be respected as individuals*" and that their "*right to life, liberty, and the pursuit of happiness*" shall be the supreme consideration in governmental affairs, provided it does not interfere with the public welfare. This provision has since served as the constitutional foundation for judicial recognition of privacy, enabling courts to construct privacy as an implicit right despite its absence from the text. It was on the basis of Article 13 that Japanese courts, starting in the 1960s, began to articulate privacy as a legally enforceable right through a series of landmark

[336] M A Sayre, 'The Right to Privacy and the Japanese Constitution' (2024) 2 *Student Journal of Information Privacy Law* 25-26.

cases[337].

Privacy was first explicitly recognized by a Japanese court in 1964 in the so-called After the Banquet (*Utage no Ato*) case.

In this decision, the Tokyo District Court affirmed that privacy encompasses the right not to have one's private life arbitrarily exposed to the public, a protection that extends to both individual and family life. Although the case involved private parties and therefore bore greater resemblance to American tort law than to constitutional adjudication, its influence proved far-reaching. It provided the conceptual foundation for subsequent jurisprudence in which the Supreme Court of Japan elevated privacy protection into the constitutional domain, grounding it in Article 13 of the 1946 Constitution. The judgment thus marked the crystallization of privacy as a legally enforceable right and reflected the growing recognition of its importance within Japanese society.

In the years following After the Banquet, the Supreme Court of Japan progressively expanded the scope of privacy protection. In 1969 it acknowledged that individuals possess a right not to be photographed without their consent (*shōzōken*), recognizing the existence of a general principle of photographic privacy. Subsequent rulings further clarified the contours of this evolving right. In 1981, the Court held that the disclosure of a citizen's criminal record by a municipal government violated constitutional privacy, affirming that personal information an individual wishes to keep confidential deserves judicial protection.

A few years later, in 1984, the Court suggested that privacy also entails the right to correct erroneous official information that could seriously harm an individual's reputation, although in that particular case the record in question was not deemed inaccurate. This gradual jurisprudential expansion eventually encountered limits. In 2008, in a litigation surrounding the *Jūki-Net* national

[337] Ibid. 22-23.

resident registry, a database containing personal data of the entire population, the Supreme Court rejected claims that the system violated constitutional privacy. While acknowledging widespread concerns about centralized data collection, the Court upheld the scheme's constitutionality, a position later reaffirmed in relation to its successor, the MyNumber identification system.

Nevertheless, the public debate surrounding these cases directly influenced the adoption of Japan's first comprehensive data protection law, the Act on the Protection of Personal Information (APPI)[338].

Beyond its enactment, Japan's data protection system is best understood as a multi-layered regulatory framework, in which the APPI functions as the central pillar but is complemented by other instruments. While the general provisions of the APPI apply to both the public and private sectors, specific laws regulate the processing of personal information by public bodies: the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO) and the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies (APPIHIAA). In addition, many prefectures and municipalities have adopted local ordinances on the handling of personal information. The system is further supplemented by the Cabinet Order, the Basic Policy on the Protection of Personal Information, and binding guidelines issued by the Personal Information Protection Commission (PPC), as well as provisions scattered across other statutes, such as the Employment Security Act. Civil remedies based on tort law, continue to play an important role in privacy disputes. Finally, industry-specific guidelines and the supplementary rules adopted in the context of the EU–Japan adequacy decision add further layers of regulation[339].

[338] Ibid. 26-28.

[339] T Hoffmann, *Data Protection by Definition: Report on the Law of Data Disclosure in Japan* (University of Passau IRDG Research Paper Series No 22-03, 2022).

4.2.2 The Act on the Protection of Personal Information (APPI)

The Act on the Protection of Personal Information (APPI), originally enacted in 2003, constitutes the cornerstone of Japan's data protection framework. Its adoption marked the first comprehensive attempt to regulate personal information at the national level, following earlier local ordinances in the 1970s and the limited 1988 *Act on the Protection of Personal Information Pertaining to Computer Processing by Administrative Organs.* Since then, the APPI has undergone a series of significant reforms, reflecting the growing importance attributed to privacy in the digital age[340].

Initially, the law applied only to private entities that managed more than 5,000 records, reflecting a relatively light-touch approach designed to balance privacy with the promotion of economic activity in the digital sphere. A major reform was introduced in 2015 and entered into force in 2017. This amendment established the Personal Information Protection Commission (PPC) as an independent supervisory authority with regulatory and enforcement powers. The reform also abolished the threshold of 5,000 records, making the APPI applicable to all business operators, and introduced new protections for "*special care-required personal information*", covering sensitive categories such as health, race, or creed[341].

Further significant changes came with the 2020 amendment, which took effect in April 2022. These revisions expanded the extraterritorial scope of the law, making it applicable to foreign companies processing the personal data of individuals located in Japan. They also introduced mandatory data breach notifications to both the PPC and affected individuals, enhanced the rights of data subjects to access, correct, delete, or restrict the use of their information, and strengthened penalties for non-

[340] K Ishiwaka, *Japan's Personal Information Protection Legal Framework and Its International Initiatives* (Presentation, WTO Joint Statement Initiative on E-Commerce Workshop, 2025) https://www.wto.org/library/events/event_resources/ecom_0805202510/779_2422.pdf.

[341] A Coos, 'Data Protection in Japan: All You Need to Know about APPI' (*Endpoint Protector Blog*, 2022) https://www.endpointprotector.com/blog/data-protection-in-japan-appi.

compliance. The amendment also clarified the treatment of "*pseudonymously processed information"* and "*personally referable information*", extending the scope of regulation to cover modern forms of data, such as browsing history and cookies, when linked to identifiable individuals.

This progressive strengthening of the APPI created the conditions for the European Commission's 2019 adequacy decision, which recognized Japan as providing a level of protection essentially equivalent to that of the European Union. This was complemented by the adoption of supplementary rules by the PPC to ensure compatibility with the GDPR, thereby enabling the free flow of personal data between Japan and the EU[342].

The Act on the Protection of Personal Information is structured into seven chapters.

The *General Provisions* (Chapter I, Arts. 1-3) set out the purpose of the law and provide the key definitions. Article 1 of the APPI establishes the purpose of the Act: to protect individual rights and interests while recognizing the economic and social value of personal information. It frames personal data not only as a matter of privacy, but also as a resource for innovation, industrial development, and quality of life.

Article 2 provides the key definitions. *Personal information* is defined as any information concerning a living individual that can identify that person, either directly (e.g., name, date of birth) or indirectly through identifiers such as codes, numbers, or other descriptors. From such definition, the law further distinguishes between:

- *Personal data* (Art. 2(3)), meaning personal information that forms part of a database;

[342] N Sugihara, 'Japan Makes Amendments to Their Act on the Protection of Personal Information: Establishing an Obligation to Report Data Breaches to the PPC' (*Talking Tech*, 2020) https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2020/06/amendments-to-the-protection-of-personal-information-act-of-japa.html.

- *Retained personal data* (Art. 2(7)), which is subject to disclosure and correction rights;
- *Special care-required personal information* (Art. 2(3)), a category of sensitive data[343] requiring stricter safeguards.
- *Pseudonymously processed information* (Art. 2(9) and *anonymously processed information* (Art. 2(11)), aimed at enabling data use for innovation and research while mitigating risks to individual privacy[344].

In defining the entities that handle personal data, the APPI distinguishes between different types of business operators[345], figures that partly correspond to the European concept of the data controller, and that reflect the categories of data set out in the law. Specifically:

- *Personal Information Handling Business Operator (PIHBO)* (Art. 2(5)): an entity that processes personal information in general.
- *Pseudonymously Processed Information Handling Business Operator (PPIHBO)* (Art. 2(10)): an entity that manages pseudonymized information.
- *Anonymously Processed Information Handling Business Operator (APIHBO)* (Art. 2(12)): an entity that manages anonymized data.
- *Personally Referential Information Handling Business Operator* (Art. 26-2(1)): an entity that processes "personally referable information," meaning residual data not fully attributable to an identified person.

[343] For example race, creed, medical history, or criminal records.
[344] Government of Japan, *Act on the Protection of Personal Information* (2022) 2-5.
[345] The concept of business operator implies the use of data for commercial purposes, thereby excluding public bodies or private individuals who process data for non-commercial purposes. However, following the 2017 reform, the size-based criterion was abolished: today, all companies are required to comply with the APPI rules, regardless of the amount of data they process.

Chapter II (Arts. 4-6) of the APPI sets out the '*responsibilities of the central and local governments*'. The central government must design and implement nationwide policies for the proper handling of personal information, while local authorities adapt these measures to regional needs. The Act also requires legislative action where stricter safeguards are necessary and calls for international cooperation to ensure global compatibility. Complementing on these provisions, Chapter III (Arts. 7-14) introduces the '*measures for the protection of personal information*'. It mandates a Basic Policy on the Protection of Personal Information, approved by cabinet decision, to guide all relevant actors — central government, local authorities, administrative agencies, and private operators. The central government provides support through guidelines and complaint-handling mechanisms, while local authorities ensure proper management of data within their agencies, assist businesses and residents, and mediate disputes. Both levels are required to cooperate to ensure consistency in data protection nationwide[346].

Chapter IV (Arts. 15-58) of the APPI represents the operational core of the legislation, as it sets out in detail the obligations of entities processing personal data, structured according to the type of operator and the degree of identifiability of the information.

- Section 1 (Arts. 15–35) – *Obligations of Personal Information Handling Business Operators (PIHBO)*

  This section lays down the general obligations of data controllers. They include the principle of purpose limitation, which requires data to be processed only for specifically declared purposes and mandates consent for any further use, as well as the obligation of lawful acquisition, with particular attention to sensitive categories that demand explicit consent. The law also establishes duties of transparency towards data subjects, obligations

[346] Government of Japan (n 344) 5-8.

to ensure the accuracy and security of personal data, and a duty of supervision over employees and entrusted parties. Transfers to third parties are permitted only with consent, with stricter requirements applying to cross-border transfers or to personally referable information. Finally, the section grants data subjects fundamental rights – access, rectification, erasure, and cessation of use – and imposes additional duties on operators, such as record-keeping of transfers and the handling of complaints[347].

- Section 2 (Arts. 35-2 and 35-3) – *Obligations of Pseudonymously Processed Information Handling* Business Operators (PPIHBO)

  This section establishes obligations for entities processing pseudonymized data, including the prohibition on re-identifying individuals and the requirement to implement technical and organizational safeguards to minimize re-identification risks[348].

- Section 3 (Arts. 36–39) – *Obligations of Anonymously Processed Information Handling Business Operators (APIHBO)*

  This section sets out rules for anonymized data, requiring transparency measures (disclosure of processing methods and categories of data) and prohibiting any attempt at re-identification[349].

- Section 4 (Arts. 40–46) – *Supervision*

  This section regulates the supervisory powers of the Personal Information Protection Commission (PPC), which may request reports, conduct inspections, issue recommendations, and, in serious cases, adopt binding orders and sanctions[350].

[347] Ibid. 8-23.
[348] Ibid. 23-26.
[349] Ibid. 26-28.
[350] Ibid. 28-32.

- Section 5 (Arts. 47–58) – *Private Sector Body's Promotion for the Protection of Personal Information*

  This section recognizes the role of accredited private organizations that, while not creating new substantive obligations, provide support, guidance, and self-regulatory tools for business operators[351].

- Section 6 (Arts. 58-2 to 58-5) – *Service*

  This section contains residual and procedural provisions of a technical nature, relating to the Commission's services in enforcing the Act[352].

Chapter V (Arts. 59–74) establishes the *Personal Information Protection Commission (PPC)* as Japan's independent supervisory authority. Created within the Cabinet Office framework, the Commission formally operates under the jurisdiction of the Prime Minister but is designed to function autonomously in order to guarantee neutrality in the oversight of personal data protection (Art. 59), with its independence explicitly safeguarded by Art. 62. Pursuant to Arts. 60–61, its mandate combines the protection of individuals' rights with the promotion of the effective use of personal data, and it exercises broad powers of supervision, enforcement, and rule-making[353].

Chapter VI (Arts. 75–81), *Miscellaneous Provisions*, introduces supplementary rules to clarify the scope and application of the APPI. Article 75 extends the Act to cases in which a business operator abroad handles personal data of individuals located in Japan, thus confirming the law's extraterritorial effect. Article 76 establishes exclusions for activities such as journalism, academic research, religion, and politics, while still requiring basic safeguards. Articles 77–81 regulate administrative coordination, allowing delegation of functions to local authorities, cooperation with

[351] Ibid. 32-38.
[352] Ibid. 38-39.
[353] Ibid. 39-45.

foreign regulators and compliance with international treaties, as well as reporting duties to the Diet and implementation through Cabinet Orders[354].

Finally Chapter VII (Arts. 82–88), *Penal Provisions*, introduces the penal provisions of the APPI, establishing criminal liability for behaviors such as breach of confidentiality, non-compliance with PPC orders, or the unlawful use of personal databases. Liability extends not only to individuals but also to corporations, which may face fines of up to 100 million yen under Article 87. The penal provisions also apply to offenses committed abroad (Art. 86), while minor violations, such as failures to notify under specific provisions, may result in non-criminal fines (Art. 88). Although the PPC is entrusted with broad investigative powers, it does not itself conduct criminal prosecutions, but rather refers cases to public prosecutors or police, who act under the Code of Criminal Procedure[355].

4.2.3 The EU-Japan Adequacy Decision

Chapter V of the GDPR regulates transfers of personal data to third countries or international organizations. Such transfers are permissible only where they comply with the guarantees set out in the Regulation. The principal mechanism is the so-called "*Adequacy Decision*", by which the European Commission recognizes, through an implementing act, that a third country ensures a level of protection essentially equivalent to that guaranteed within the Union. In reaching such a finding, the Commission considers the factors listed in Article 45(2) GDPR, including the existence of comprehensive data protection legislation, the rule of law and respect for fundamental rights, the presence of an independent supervisory authority with sufficient enforcement powers, and the country's international commitments in the field of data protection. Adequacy decisions remain

[354] Ibid. 45-48.
[355] Ibid. 48-49.

relatively rare, with only a limited number of jurisdictions[356] having been recognized to date[357].

On January 23rd 2019, the European Commission adopted the Adequacy Decision recognizing that the Japanese legal framework ensures a level of personal data protection essentially equivalent to that provided under the GDPR. This was the first Mutual Adequacy decision, since Japan in turn recognized the adequacy of the European Union under its domestic legislation, thereby creating the world's largest area of free data flows based on high standards of protection[358].

The legal basis for this recognition lies in Article 45 of the GDPR, which empowers the Commission to authorize transfers to a third country once it has established, on the basis of a comprehensive assessment, that the system guarantees an "*essentially equivalent*" level of protection to that within the Union. Importantly, as clarified by the Court of Justice of the European Union, such equivalence does not require an identical replication of EU rules, but rather effective guarantees in substance, implementation, supervision, and enforcement[359].

In carrying out this assessment, the Commission reviewed the constitutional and jurisprudential underpinnings of privacy protection in Japan, including Supreme Court rulings recognizing the individual's right to prevent unnecessary disclosure of personal information to third parties. It then examined the legislative framework, focusing on the Act on the Protection of Personal Information

---

[356] As of 2023, the European Commission has recognized as adequate: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom, United States (Data Privacy Framework), and Uruguay (European Commission, Adequacy decisions https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

[357] N Blue, 'Spirited Away: The EU's Adequacy Decision for Japan as a Roadmap for U.S. Privacy Law after Schrems II' (2022) 21 *Wash U Global Stud L Rev* 448-451.

[358] F Y Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) 33(2) *Harvard Journal of Law & Technology* 671.

[359] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 on the adequate protection of personal data by Japan under Regulation (EU) 2016/679 [2019] OJ L76/1 1-2.

and its successive amendments, which progressively aligned Japan's regime with international standards. A central element was the establishment of an independent redress mechanism under the Personal Information Protection Commission (PPC), whose supervisory and enforcement powers were considered sufficient to satisfy the GDPR's requirement of an "*independent supervisory authority*". Its powers to investigate operators, issue recommendations and binding orders to business operators in order to protect individual rights were positively evaluated as effective institutional guarantees[360]. To bridge the remaining gaps with the GDPR, the adequacy decision also relied on Supplementary Rules adopted by the PPC, together with formal assurances and commitments from the Japanese government. These additional instruments addressed specific shortcomings in relation to sensitive data, individual rights, onward transfers, and safeguards against disproportionate access by public authorities. As a result, transfers of personal data from the EEA to organizations subject to the APPI and the Supplementary Rules can take place without additional authorizations, while Japanese entities remain directly subject to the GDPR whenever the conditions of Article 3 are met[361].

As stated by Recital 10, the Adequacy applies exclusively to private organizations falling within the scope of the APPI, while data processing by Japanese public authorities, particularly for law enforcement or national security purposes, is explicitly excluded[362]. Moreover, the Decision is subject to continuous monitoring and periodic review. Pursuant to Article 3 of the Decision and Recitals 180–181[363], the Commission must carry out a first review within two years of its entry into force and subsequent reviews at least every four years, with the possibility of suspending, amending, or repealing the Decision should the level of protection no longer be maintained.

[360] N Blue (n 357) 451-453.
[361] Decision 2019/419 (n 359).
[362] Ibid. 3.
[363] Ibid. 33.

The adoption of the Decision required legislative amendments and the introduction of additional measures compared to the original framework. In particular, the PPC issued draft Guidelines in April 2017, which were later revised and adopted as Supplementary Rules binding on domestic operators processing personal data transferred from the EU, which strengthened both safeguards and individual rights[364].

Firstly, Supplementary Rule (1) expanded the category of "*special care-required personal information*" under Article 2(3) of the APPI to include data transferred from the European Union concerning an individual's sex life, sexual orientation or trade-union membership. Moreover, such data cannot be collected without the prior consent of the individual concerned and is shielded from disclosure to third parties except in narrowly defined circumstances[365]. Under Supplementary Rule (2) the temporal limitation on the exercise of individual rights was removed. While the APPI excludes data scheduled for deletion within six months from the notion of "*retained personal data*", EU data transferred to Japan must now always be treated as retained personal data. This guarantees EU citizens the full range of access, rectification, and erasure rights regardless of the retention period.

Stricter conditions were also imposed on the purpose limitation principle. Business operators receiving data from the EU are required to confirm and record the exact purposes for which the data have been transferred, and they may not alter those purposes unless the data subject has provided fresh consent under Arts. 15-16 of APPI[366]. Supplementary Rule (3) ensures that this obligation also applies to onward sharing in Japan, so that data must remain tied to the original purpose unless renewed consent is given[367].

[364] H Miyashita, 'EU-Japan Mutual Adequacy Decision' (2020) *blogdroiteuropéen*.
[365] Decision 2019/419 (n 359) 11-12.
[366] H Miyashita (n 364).
[367] Decision 2019/419 (n 359) 8.

Fourth, Supplementary Rule (4) tightened restrictions on onward transfers to third countries of personal data originally received from the EU. Under the APPI, international transfers were already conditioned on the prior consent of the data subject, however, Japanese practice had previously allowed reliance on regional mechanisms such as the APEC Cross-Border Privacy Rules which does not establish a binding legal relationship between the data exporter and the importer. The Supplementary Rules now permit onward transfers only where the recipient country ensures equivalent protection, appropriate safeguards such as contracts or binding corporate rules are in place, or the explicit consent of the data subject has been obtained[368]. Finally, Supplementary Rule (5) raised the standard for anonymization. Under the APPI, "*anonymously processed personal information*" does not require technically irreversible de-identification, which means that some data considered anonymous in Japan would still qualify as personal data under the GDPR. The Rules provide that EU data can be treated as anonymous only if the de-identification is irreversible, requiring the destruction of all information or processing methods that could permit re-identification. This ensures that data transferred from the EU are regarded as anonymous in Japan only where they would also be considered anonymous under European law[369].

Beyond its regulatory implications, the Adequacy Decision was also strongly driven by economic and political considerations. As pointed out by Wang, the main motivation for the Japanese government lay not so much in expanding individual rights, but in unlocking the economic potential of cross-border data flows. Prime Minister Abe presented the agreement as a way to revitalize the Japanese economy by leveraging personal data, and stressed in his 2019 Davos speech that data had become the key driver of global development, shaping what he called "*Society 5.0*" and a global regime of "*Data Free Flow with Trust*". This framing highlighted Japan's ambition to

[368] Ibid. 13.
[369] Ibid. 6.

position itself as a leader in digital governance, using data as a strategic resource both for growth and for reducing social inequalities.

Indeed, the Decision was adopted in parallel with the EU–Japan Economic Partnership Agreement (EPA), which entered into force in February 2019, reflecting the deliberate strategy to align data governance with trade liberalization.

The two instruments were explicitly presented as complementary, combining trade liberalization with a trusted framework for digital transfers. For Europe, the arrangement promised privileged access to the Japanese market and the benefits of unrestricted data flows with a key commercial partner. For Japan, it reinforced its strategic alliance with the Union and provided legal certainty for Japanese companies operating in Europe and needing to transfer data internationally[370].

At the same time, however, the close temporal proximity between the Adequacy Decision and the EPA underlined their practical entanglement under the broader label of "digital trade". While the European Commission repeatedly stressed that the protection of personal data was non-negotiable in trade negotiations, Article 18.1(2)(h) of the EPA explicitly recognizes that each party remains free to define and regulate its own level of protection of personal data in pursuit of public policy objectives. This provision illustrates the tension between the proclaimed fundamental character of data protection and its accommodation within the logic of economic integration. Taken together, the Adequacy Decision and the EPA were thus promoted as a new model for reconciling trade law and data protection law, but they also reveal the inherent ambiguities in balancing privacy as a fundamental right with the imperatives of international commerce[371].

The Adequacy Decision is not a static recognition but a framework subject to constant monitoring and revision under Article 45(3) GDRP. At the same time, it has served as a driver for the gradual

[370] F Y Wang (n 358) 673-674.
[371] H Miyashita (n 364) 6.

strengthening of Japan's data protection framework. In line with the triennial review obligation introduced by the 2020 reform of the APPI, the PPC published an Interim Report in June 2024, released for public consultation with a view to preparing a new round of amendments in 2025. The Report anticipates a comprehensive reform of Japan's data protection regime, addressing issues such as the relaxation of incident reporting obligations in cases of minor breaches; the introduction of specific rules on biometric data, including stricter purpose specification and the right of data subjects to request suspension of processing; and the long-awaited inclusion of provisions on children's personal information, such as mandatory parental consent, reinforced security measures, and clarification that a child is defined as an individual under the age of sixteen. It further considers the extension of collective redress mechanisms to privacy violations, thereby opening the door to a potential class action system, as well as the establishment of an administrative fine regime to strengthen the enforcement powers of the PPC[372].

Finally, the Decision, while recognized as a milestone, has also attracted significant criticism, particularly regarding its limited scope, the differentiated protection it affords to European and Japanese citizens, and the issue of government access to personal data in Japan. As Miyashita observed, in practice hundreds of companies have voluntarily provided customer data to the police, often without judicial oversight, creating a "*black box*" system lacking transparency for data subjects[373]. The Commission itself acknowledged that voluntary disclosure requests under Article 197(2) of the Code of Criminal Procedure are non-compulsory and thus operate outside the ordinary system of judicial warrants[374]. More broadly, the adequacy framework has been criticized

[372] K Takase et al, 'Japan: Personal Data Protection Commission – Announces Interim Report of Triennial Review' (*Baker McKenzie InsightPlus*, 2024).
[373] H Miyashita (n 364) 11-12.
[374] Decision 2019/419 (n 359) 22-23.

as "*insular*", since the enhanced safeguards apply only to EU data, while domestic Japanese data continues to be subject to weaker protections[375].

4.2.4 The Japanese Model in Comparative Perspective

In comparative perspective, the Japanese model reveals its hybrid nature. On the one hand, the reforms of the APPI and the adoption of the Supplementary Rules reflect a clear convergence with the European Union's framework; on the other, Japan continues to follow its own path, rooted in a pragmatic and economic conception of privacy.

In the EU legal order, data protection is enshrined as a fundamental right, closely linked to human dignity and to the principle of informational self-determination. By contrast, Japan does not recognize privacy as a constitutional fundamental right. Rather, its legislative framework is conceived as a pragmatic mean to prevent concrete harms and to sustain the functioning of the digital economy emphasizing the economic value of data. European instruments, most notably the Charter of Fundamental Rights, explicitly recognize privacy and data protection as fundamental rights. By contrast, Article 13 of the Japanese Constitution only implicitly refers to privacy, while the Act on the Protection of Personal Information highlights not only individual rights but also the economic value of data, framing it as a driver of industrial and social development. The divergence also emerges in the scope of protection: the GDPR defines personal data broadly, covering any information that may directly or indirectly identify a person, including online identifiers. The APPI instead adopts a narrower definition, limited to information that can reasonably identify an individual, reflecting Japan's concern with avoiding excessive constraints on business activity. The adequacy arrangement illustrates this divergence: in order to achieve recognition by the European Commission, Japan introduced an additional set of rules applying only to data originating from the

[375] F Y Wang (n 358) 672.

EU. The result is an “insular” model of protection, in which European data benefits from enhanced safeguards, while Japanese citizens remain subject to less stringent standards.

A different set of comparisons emerges when Japan is placed alongside the United States. The American system is notoriously fragmented and sectoral, with protections scattered across multiple statutes complemented by state laws and FTC enforcement based on consumer protection. Japan, on the other hand, has established a general legal framework through the APPI and created a centralized and independent authority, the Personal Information Protection Commission. Nonetheless, similarities exist: in both systems, personal data are primarily treated as an economic resource, and obligations often arise in response to consumer harm or economic needs. The decisive difference lies in institutional architecture. Whereas the United States remains anchored to a consumer-centric, market-driven model and ex post enforcement, Japan has moved closer to the European approach through the establishment of uniform obligations and the oversight role of the PPC.

The comparison with China further accentuated Japan’s distinctiveness. The Chinese framework has developed into a comprehensive architecture combining combining the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, in which the protection of personal information is subordinated to objectives of national security, social control, and the collective interest. Japan, in contrast, has adopted a lighter approach, where the state does not seek pervasive control, but rather delegates significant responsibility to private actors under the oversight of the PPC. In China, cross-border transfers are subject to strict security reviews and localization requirements, while in Japan the adequacy decision reflects a willingness to align with European standards to facilitate trade.

Taken together, these comparisons show that Japan occupied an intermediate position within the global landscape of data protection. It stands between the European fundamental-rights approach

and the more economic or state-centric models of the U.S. and China. The Adequacy Decision of 2019 illustrates a rare convergence of two profoundly different models. It represents Japan's capacity to strategically adapt to European standards for political and economic purposes, while preserving a culture of privacy that is pragmatic, business-oriented, and different from the constitutional recognition found in Europe.

Chapter 5

Artificial Intelligence and the Protection of Personal Data

5.1 AI and Data Protection as a fundamental right

Artificial Intelligence (AI) is a profound technological transformation with global implications. As highlighted by the UN, it represents an extraordinary opportunity for innovation, inclusive growth, and progress, but also a potential source of destabilization, with implications for international security, information integrity, and the protection of fundamental rights, such as privacy and personal data[376].

In the contemporary digital age, its rapid development has initiated a new era of data collection and analysis, reshaping interactions between individuals and technology and enabling unprecedented efficiencies across multiple sectors: everything from medicine and finance to advertising and government administration is being dramatically transformed by AI-based systems, altering the ways data are gathered, processed, and used. Yet, this technological transformation raises complex ethical and legal challenges, particularly with respect to the safeguarding of privacy and the protection of personal information[377]. As more complex algorithms and machine learning

[376] United Nations System Chief Executives Board for Coordination, Summary of deliberations: United Nations system white paper on artificial intelligence governance (2024) UN Doc CEB/2024/1/Add.1 5.

[377] S Mirishli, 'Ethical Implications of AI in Data Collection: Balancing Innovation with Privacy' (2025) *arXiv preprint arXiv:2503.14539* 41.

models are integrated into organizational operations, the personal data collection and processing activities have increased exponentially, exposing a critical gap between technological innovation and existing regulatory safeguards[378].

In this context, the notion of "AI privacy" is often used to indicate the protection of personal or sensitive information that is collected, used, shared, or stored by AI systems, highlighting the new scale and pervasiveness of data processing in artificial intelligence, where individuals' control over their personal information becomes increasingly fragile[379].

As traditional privacy legislation is unable to keep pace, risks of abuse, lack of transparency, and erosion of public trust grow. Securing information in the age of AI is therefore not so much a technical issue as it is an inherent societal issue requiring the combined efforts of legislators, the private sector, and the public[380].

5.1.1 Emerging Challenges of AI for Data Protection

Artificial intelligence today finds application in a wide range of areas from *Natural Language Processing, Speech Recognition, Machine Learning, Deep Learning*, and *Biometrics.*

At its core, however, AI is fundamentally data-driven[381]: its rapid progress has been made possible by the exponential growth of available information, the so-called "*data deluge*" process, and by advances in computing power, making privacy and data protection central to any legal assessment of the technology.

The enormous amount of data on which AI relies – *Big data* – is often provided directly by users

[378] S Sirojov, *'Data Privacy Challenges in Artificial Intelligence Overview*' (2025) 2.
[379] A Gomstyn and A Jonker, 'Esplorare i problemi di privacy nell'era dell'AI' (2024) *IBM Think.*
[380] S Sirojov (n 378).
[381] G Finocchiaro, 'Intelligenza Artificiale e protezione dei dati personali' (2019) *Giurisprudenza Italiana* 1671.

themselves, consciously or not, through social networks, search engines, and connected devices. Platforms such as Facebook, Instagram, Google, but also Chinese giants like Alibaba and Baidu, have built their wealth on systematic collection and exploitation of personal information, a phenomenon described as *surveillance capitalism*: in this perspective, data have been defined as the "*new oil*" of the digital economy. The European Commission itself referred to this phenomenon in its communication of 2014 "*towards a thriving data-driven economy*" where it described big data as large volumes of heterogeneous information produced at high speed by multiple sources, whose management requires advanced tools of analysis.

The convergence of Big Data and IoT – *Internet of Things* (IoT), namely the interconnection of everyday objects such as smartphones or wearables – defines a technological environment rich in opportunities but also risks for the fundamental right to personal data protection. These devices continuously collect and transmit data regarding individuals' habits, preferences, and even health conditions, often without users' full awareness[382].

The integration of AI into such devices, the so-called Edge AI, intensifies concerns of constant surveillance, accountability and security, and the erosion of the principle of consent as the legal basis for processing.

Recent advances, from large language models to biometrics and quantum machine learning, also amplify these challenges.

Large Language Models (LLMs) demonstrate remarkable capacity to absorb and generate human-like text. Yet, they can deduce sensitive personal information from seemingly harmless inputs, recalling *the mosaic theory*, where fragments of information put together, may reveal information

[382] M Bera*, Il GDPR e la disciplina dei soggetti del trattamento alla prova dell'evoluzione tecnologica* (Tesi di laurea, Università degli Studi di Pavia 2025) 59-65.

that is highly personal. Biometric technologies such as face scanning and emotion analysis also widen the scope of personal data collection, often without obtaining meaningful consent. Furthermore, the potential of Quantum Machine Learning (QML) raises concerns for sensitive data by threatening encryption systems and increasing opacity[383].

In practice, the privacy risks of AI often materialize through recurring patterns: the large-scale collection of sensitive data (including biometric and health information), the use of data without genuine consent or for purposes other than those initially agreed, and the increasing risks of data leakage or model inversion that can expose information contained in training datasets. These dynamics demonstrate how AI does not create entirely new problems, but rather amplifies existing vulnerabilities of data protection, making traditional guarantees such as consent, purpose limitation, and security more fragile[384].

In the absence of specific regulation, traditional principles such as minimization and purpose limitation risk becoming ineffective. Faced with these challenges, the protection of personal data must be reaffirmed as a fundamental right of the digital era[385].

5.2 International Initiatives and Global Governance

Although the development of AI is currently dominated by United States, China, and the European Union, the consequences of its use are inherently international. Artificial Intelligence applications create cross-border externalities – everything from the disruption of markets to privacy and security risks – that cannot be addressed by domestic law alone. Moreover, the global scope of AI research and development, largely driven by multinational companies, highlights the necessity of common

[383] S Mirishli (n 378) 41-44.
[384] A Gomstyn and A Jonker (n 379).
[385] S Mirishli (n 383).

international standards to avoid regulatory fragmentation.

During recent years, AI regulation has therefore become an imperative for national governments but also for international bodies and multistakeholder initiatives. States, intergovernmental organizations, and private actors have all embraced the need for global cooperation in order to maximize the full potential of AI while reducing its negative effects. This acknowledgement has led to the development of several historic initiatives, which illustrate the gradual shift from soft law principles and ethical guidelines towards the development of binding international regulation in the field of AI[386].

One of the earliest multilateral measures was initiated by OECD, which in May 2019 adopted the Recommendation on Artificial Intelligence, the first intergovernmental standard on AI. Although a soft law tool, the Recommendation has become a widely used document and even inspired the G20 AI Principles, while also influencing AI strategies across OECD members. The Recommendation is structured around two pillars:

1. Five values-based principles applicable to all stakeholders:
    - *inclusive and sustainable growth and well-being*;
    - *respect for the rule of law, human rights and democratic values*, explicitly including privacy and the protection of personal data;
    - *transparency and explainability*;
    - *robustness, security and safety*;
    - *accountability*.
2. Five policy recommendations addressed to adherents:

[386] J Tallberg et al, 'The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research' (2023) 25 *International Studies Review* 1-6.

- *investing in AI research and development*;
- *fostering an inclusive and interoperable AI ecosystem*;
- *shaping agile and coherent governance and policy frameworks*;
- *building human capacity and preparing for labor-market transformation*;
- *strengthening international co-operation for trustworthy AI*.

Notably, the OECD highlights that data utilized for training and operating AI should be representative and respectful of privacy and data protection, directly linking AI governance to informational rights protection.

In addition, the Recommendation was updated in 2023 and 2024 to address new challenges related to generative AI[387], but also reiterated privacy and data protection as fundamental components of the human-centric approach to AI governance[388].

More recently, in 2024, the United Nations published the White Paper on Artificial Intelligence Governance, outlining the UN System's role in shaping a global approach to AI based on international law and human rights. The Document emerged in response to the urgent necessity to bring coherence and leadership to the multiple international efforts already underway in AI, in a context marked by the rapid expansion of generative systems and LLM, as well as growing concern for the risks posed by such technologies[389].

The approach recommended for the regulation of AI is based on key pillars represented by the UN Charter, international human rights law and obligations such as the 2030 Agenda for Sustainable Development: the objective is to deliver a system that provides appropriate incentives and

[387] Such as disinformation, transparency, risk management, and sustainability.
[388] OECD, Recommendation of the Council on Artificial Intelligence (adopted 22 May 2019, amended 3 May 2024) OECD/LEGAL/0449.
[389] United Nations, Summary of deliberations (n 376) 5.

safeguards to advance ethical and human-rights based governance while maximizing the positive impact of technology and mitigating the risks[390].

Particular emphasis is devoted to the interaction between AI and data governance. Since artificial intelligence is highly dependent on the availability and quality of data, the protection of personal data and privacy is identified as an essential requirement for creating reliable systems that are aware of fundamental rights. The White Paper also calls for specific attention to the potential human rights impacts of data retention, collection, processing and transfer, especially when AI tools are employed in security contexts[391].

Within this framework, several UN bodies have developed initiatives on AI and Data Governance. In November 2021, UNESCO adopted the Recommendation on Ethics of Artificial Intelligence, the first global soft-law instrument to incorporate ethics into AI regulation, providing a universal framework to support States and private operators in addressing the social and environmental impacts of AI, aimed at safeguarding human rights and dignity, environment and cultural diversity, as well as equitable access to the perks of AI[392].

The Recommendation is grounded in shared values of *human rights and dignity, environmental sustainability, diversity and inclusiveness, and the pursuit of peaceful and just societies*. Moreover, it articulates core principles such *as proportionality, fairness, safety, sustainability, privacy and data protection, human oversight, transparency, accountability, digital literacy and multi-stakeholder governance*[393].

Privacy and data protection are explicitly recognized as central to human dignity, autonomy and

[390] Ibid. 45.
[391] Ibid. 19.
[392] UNESCO, Recommendation on the Ethics of Artificial Intelligence (SHS/BIO/PI/2021/1, 2022) 1-15.
[393] Ibid. 17-25.

agency: personal data must be collected and processed pursuant to international law, subject to adequate frameworks that ensure a legitimate purpose, legal basis and informed consent.

Among its areas of policy action[394], the Recommendation emphasizes *data policy*, urging States to guarantee data quality and security, respect of privacy with particular attention to the risk of surveillance, and ensure individuals' control over their data through transparency, access and erasure. Furthermore, stricter protection is required for sensitive data[395].

The unanimous approval by 193 Member States in November 2021 represents an attempt by the United Nations system to respond to the need to establish globally shared values and principles for ethical and responsible artificial intelligence, grounded in the protection of human rights and human dignity, and oriented towards fairness and sustainability[396].

Beyond soft law instruments, the first decisive step towards binding regulation was taken in September 2024, when the Council of Europe adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, the first international treaty specifically devoted to artificial intelligence. The Convention, signed by 15 States and the EU, seeks to ensure that all AI system are consistent with human rights, democracy and the rule of law[397].

The Instrument lays down a set of general obligations, requiring States to ensure that the development and implementation of AI systems respect fundamental rights and do not undermine

[394] Namely: ethical impact assessment; ethical governance and stewardship; data policy; development and international cooperation; environment and ecosystem; gender; culture; education and research; communication and information; economy and labour; health and social well-being.

[395] For example biometric, health and genetic data, and data revealing racial or political views, Ibid. 29-30.

[396] United Nations, Summary of deliberations (n 376) 17.

[397] Council of Europe, Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (opened for signature 5 September 2024, not yet in force) CETS No 225 2.

democratic processes and rule of law. It introduces key principles such as respect for *human dignity and autonomy, transparency and oversight, accountability, equality and non-discrimination.* A central provision is dedicated *to privacy and personal data protection*: at all stages of the development and use of artificial intelligence, states must ensure the protection of people's privacy and personal data, respecting existing laws and standards and implementing effective measures that ensure real guarantees and protection for citizens.

The Convention also establishes remedies and procedural safeguards, including the right to contest decisions substantially relying on AI, the obligation to inform individuals when interacting with AI systems, and the possibility to impose moratoria or bans on AI applications that are deemed incompatible with human rights and democratic values[398].

Although not yet in force, by introducing binding standards, the Convention marks a significant step forward in the transition from ethical guidelines and soft-law instruments towards a coherent legal framework, expressly recognizing the protection of privacy and personal data as fundamental pillars of global AI governance.

5.3 The European Union: the Artificial Intelligence Act

The increasing use of technology supported by artificial intelligence systems has significantly shifted human relations, learning methods, and public decision-making processes, raising unprecedented regulatory challenges. Within the European Union, these dynamics are framed in the broader context of the European Data Strategy 2030, launched by the European Commission in 2020 with the aim of creating a single data market across the Union that will ensure global competitiveness and data sovereignty while protecting European values and rights in the digital

[398] Ibid. 4-5.

world.

The Strategy, as a cornerstone of European digital policy, established objectives such as enhancing the availability and interoperability of data, clarifying rights of access and use, ensuring effective governance of data flows, and establishing common European data spaces: it reflects the idea that data has become a key resource for innovation, economic growth, sustainability and societal progress[399].

This ambitious programme materialized in a comprehensive package of legislative measures: the Data Governance Act (2022), designed to facilitate data sharing and reuse through the European Data Spaces; the Data Act (2023), clarifying the conditions under which data can generate value; and the Digital Services Act and Digital Markets Act (2022), respectively focused on protecting users' fundamental rights in the digital environment and preventing unfair market practices by dominant platforms. This regulatory path culminated in the Artificial Intelligence Act, aimed at ensuring the trustworthy development and deployment of AI systems[400].

As discussed in Chapter 2, the European Union has established itself as a central global actor in the protection of personal data, recognized as a fundamental right and safeguarded by the General Data Protection Regulation, which today constitutes the foundation of the European approach to regulating new technologies, including AI.

Since 2017, EU institutions began shaping an AI governance strategy inspired by an ethical and human-centric approach, aimed at reconciling technological development with the protection of fundamental rights. Following the first policy documents on robotics and ethics[401], in 2018 the

[399] European Commission, 'A European strategy for data' (2020).
[400] P Falletta and A Marsano, 'Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR' (2024) 1 *Rivista Italiana di Informatica e Diritto* 1.
[401] The European Parliament's Civil Law Rules on Robotics (2017) and the European Economic and Social Committee's Opinion on AI (2017).

Commission presented the *Digital Day Declaration*, *Artificial Intelligence for Europe* and *the Coordinated Plan on AI,* which consolidated the concept of reliable and human-centric AI. This vision was further elaborated in the *Ethics Guidelines for Trustworthy AI* (2019) and in the *Assessment List* (2020), which codified the concept of trustworthy AI, based on legality, ethics and technical robustness, and articulated in seven key requirements such as safety, transparency, fairness, and accountability.

The European Strategy for AI is grounded in the dual principle of excellence and trust, with the aim of reinforcing Europe's industrial and scientific competitiveness and consolidating its potential to compete globally, while ensuring respect for democratic values and fundamental rights[402].

The White Paper on AI of 2020 was a turning point, translating ethical issues into concrete regulatory recommendations: mandatory obligation for high-risk systems, with compliance verification before hitting the market, and a voluntary labeling system for low-risk AI[403].

Here, the Commission placed solid emphasis on the protection of personal data, identifying it as one of the most sensitive points in shaping artificial intelligence systems. First, it highlighted the crucial role of the quality of training data, since incomplete or biased datasets may generate discrimination and privacy violations[404]. Furthermore, the document reaffirmed the importance of compliance with the GDPR and the Law Enforcement Directive, requiring personal data protection to be guaranteed throughout the entire cycle of AI systems with transparency, traceability and documentation to ensure proper and proportionate use of data. Particular attention was dedicated to the processing of biometric data and to remote facial recognition in public spaces, since such

[402] European Commission, 'European Approach to Artificial Intelligence' (2025).
[403] C Stix, 'The ghost of AI governance past, present and future: AI governance in the European Union' (Eindhoven University of Technology, pre-print, 2021) 3-16.
[404] European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust COM(2020) 65 final, Brussels, 19 February 2020. 11-12.

practices are in principle a form of processing prohibited by the GDPR, permitted only in exceptional need cases and under the conditions of necessity, proportionality and adequate protection[405].

Following the White Paper on AI, the Commission presented in 2021 the Proposal for the Regulation on a European approach for Artificial Intelligence, which, after the legislative process, led to the adoption in 2024 of Regulation (EU) 2024/1689 on Artificial Intelligence (the "*AI Act*"). With this initiative, the EU was the first legislator in the world to propose a comprehensive legal text on AI, aiming to establish harmonized rules across the Union and reconciling technological innovation with the protection of fundamental rights.

The AI Act pursues a dual objective: on the one hand, *to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter*, and, on the other, *to support innovation*[406].

In developing the regulatory framework, the EU legislator chose to pursue a horizontal and general approach, with a deliberately broad definition of AI to ensure long-term applicability and avoid rapid obsolescence in a fast-evolving technological context[407]. It also has an extraterritorial scope, applying not only to entities established in the Union but also to non-European providers offering goods or services within the EU. The main addressees are providers and deployers of AI systems, along with importers, distributors, and producers who integrate AI into their products[408].

The AI Act adopts a pyramid-shaped risk-based structure that distinguishes four categories[409].

---

[405] Ibid. 21-22.
[406] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence [2024] OJ L1689/1, art. 1, 44.
[407] P Falletta and A Marsano (n 400) 4.
[408] Regulation (EU) 2024/1689 (n 406) 45-46.
[409] P Falletta and A Marsano (n 400) 4-5.

At the top, unacceptable-risk systems[410] are prohibited as they are deemed incompatible with fundamental rights with only very limited exceptions for law enforcement. High-risk systems, namely those applications likely to have a significant impact on fundamental rights or on the safety of individuals, are not prohibited, but subject to requirements and obligations on providers, importers, distributors and deployers[411]. In particular, Article 27 imposes the obligation of carrying out a *Fundamental Rights Impact Assessment (FRIA)* with the aim of examining the categories of individuals likely to be affected, the compliance of the system with European and national fundamental rights law, and the foreseeable effects of its use[412].

Limited-risk systems are mainly subject to transparency obligations, ensuring that users are informed when interacting with AI or exposed to synthetic content such as deep fakes. The objective is to ensure informed-choices and to prevent deceptive or manipulative practices[413].

Finally, minimal-risk systems, which make up the majority of applications, remain free from binding obligations, relying only on voluntary codes of conduct[414]. A novel feature concerns general-purpose AI models, for which the Regulation introduces specific duties, especially in cases of systemic risk.

Another key feature of the AI Act is its multi-level governance system, which combines EU and national oversight. At Union level, the European Commission created the AI Office[415] to supervise

[410] These include: social scoring systems, predictive policing, facial recognition technologies based on scraped data, cognitive and behavioral manipulation systems, emotion recognition in the workplace and educational settings, as well as most forms of remote biometric identification in public spaces.
[411] Regulation (EU) 2024/1689 (n 406) arts 8-15 and 16-27, 55-70.
[412] Ibid. art 27, 69.
[413] Regulation (EU) 2024/1689 (n 406) 82-83.
[414] D Krause, The EU AI Act and the Future of AI Governance: Implications for U.S. Firms and Policymakers (*SSRN*, 2025) 6.
[415] Regulation (EU) 2024/1689 (n 406) art 64, 95.

implementation and cooperate with national authorities in monitoring high-risk systems[416], while the AI Board[417] promotes coordination and best practices among Member States[418]. Nationally, each country designates one *notifying authority* and one *market surveillance authority*, both of which must operate independently, impartially and objectively to ensure the uniform application of the Regulation.

Particular attention is devoted to the protection of personal data. Data Protection Authorities, already central under the GDPR, play a crucial role in supervising high-risk AI applications, especially those involving biometric data and law enforcement. The ongoing debate on whether to entrust oversight to new technical agencies or to existing DPAs highlights once again that data protection remains at the heart of the European approach to AI governance[419].

5.3.1 The relationship between the GDPR and the AI ACT

The European Regulation on Artificial Intelligence is not an autonomous legislative tool, but part of a broad and articulated regulatory framework, characterized by a plurality of instruments on data and digital transformation. In this context, coordination with the GDPR appears inevitable, taking into account the convergence between the two regimes. AI systems, in order to be effective and predictive, must process an enormous amount of data: this makes the collection and processing phase particularly sensitive, which nonetheless remains governed by the GDPR, as the primary safeguard of the fundamental right of data protection enshrined in Articles 8 of the Charter of Fundamental Rights of the EU and 16 TFEU[420].

[416] Ibid. arts. 88-92, 110-112.
[417] Composed of one representative from each Member State and, as non-voting observers, the AI Office and the European Data Protection Supervisor.
[418] Ibid. arts 65-66, 96.
[419] M Cappai, Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale? (2024) *Federalismi.it* 190-195.
[420] P Falletta and A Marsano (n 400) 8.

Indeed, as recalled in Recital 10, the AI Act operates within the Union's comprehensive legal framework for the protection of personal data, without altering its application. Providers and deployers of AI systems remain subject to their respective obligations as controllers or processors and Union and national data protection law and, data subjects, in turn, continue to enjoy the full range of rights established under EU law. The harmonized rules introduced by the AI Act are thus intended to complement this framework, by facilitating the effective exercise of data protection rights and other human rights. Consequently, the two regulations must be interpreted and applied in a complementary manner, to balance innovation with the safeguarding of fundamental rights and to avoid interpretative tensions and overlaps[421].

The relationship between the AI Act and the GDPR can be exemplified from various perspectives. Both frameworks share a common regulatory philosophy grounded in *the risk-strategy approach* and the principle of accountability. Their extraterritorial scope projects European standards beyond the Union's borders[422], and they converge on principles such as *fairness, minimization, transparency, accuracy,* and *privacy by design* and *by default*[423].

Aside from these convergences, the two systems also try to rationalize compliance and avoid duplication.

One prominent example is the relationship between the *Fundamental Rights Impact Assessment* under the AI Act and the *Data Protection Impact Assessment* under the GDPR: the two instruments can be considered as parts of one single process, capable of connecting the risks associated with personal data to the broader impact on fundamental rights. In this way, the risk-based logic and the principle of accountability are translated into a unified operational model. However, national

[421] Regulation (EU) 2024/1689 (n 406) 3-4.
[422] As regulated by article 2 AI Act and article 3 GDPR.
[423] P Falletta and A Marsano (n 400) 8-10.

divergences in DPIA practice risk duplication and legal uncertainty, underscoring the need for greater harmonization by the EDPB[424]: recent studies have shown that DPIA requirements vary significantly across Member States[425], creating disparities in protection and legal certainty within the single market.

Alongside areas of convergence and integration, the interaction between the GDPR and the AI Act also reveals significant frictions.

A first example concerns *automated decision-making*. The GDPR adopts a flexible model for automated decision-making (Article 22), allowing exceptions under safeguards, while the AI Act takes a stricter stance and prohibits certain practices outright, such as social scoring seeking to prevent structural abuses by imposing absolute and non-derogable bans on practices deemed incompatible with EU values[426]. The AI Act also expands the legal basis for processing sensitive data under Article 10(5) [427], creating tensions with the stricter GDPR framework under Article 9(2)[428].

Transparency, while being recognized as a shared principle, is also challenged in practice. GDPR requires that individuals receive meaningful information, in clear and intelligible language, about the logic of automated decision-making and its consequences. Yet, most AI systems are *black boxes*, and it's difficult to provide accurate and understandable explanations to non-experts. Similar

[424] Tytti R et al, '*Impact Assessment Requirements in the GDPR Vs the AI Act: Overlaps, Divergence, and Implications*' (2025) 21-23.

[425] As etablished by Article 35 (4) "*The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment*".

[426] P Falletta and A Marsano (n 400) 10-11.

[427] Art. 10(5) AI Act allows the use of sensitive data for bias detection and correction in high-risk AI systems only under strict safeguards, including the impossibility of using alternative data, robust technical and organizational measures, strict access controls, prohibition of transfers, timely deletion, and justification in records of processing.

[428] M Cappai (n 419) 190.

challenges arise with large-scale data collection techniques such as *web scraping*, where individual notice is impossible for all data subjects.

A further difficulty concerns the compatibility of AI systems with some of the GDPR's most fundamental guarantees. Rights such as access, rectification, erasure and data portability are particularly challenging to guarantee in complex or generative AI models, where personal data are often transformed into numerical representations that are difficult to trace, update or delete. Outputs may themselves constitute personal data, including inferences about individuals, which raises additional questions about rectification and erasure[429].

At the same time, the principles of data minimization, purpose limitation and storage limitation are undermined by the reliance on vast and continuously updated datasets blurring the boundaries of purpose, and extending retention periods indefinitely[430].

Therefore, the interaction between the AI Act and the GDPR cannot be reduced to a single dynamic: at times complementary, in others overlapping or conflicting. The absence of a proper coordinating mechanism risks imposing unnecessary burdens on operators, who must adapt the GDPR to the wider AI frameworks and may reduce the effective scope of protection of individuals. In this perspective, over-regulation can both reinforce rights and erode them[431].

To address these critical challenges, a definitive step would be the harmonization of the impact assessments of the two regimes, consolidating data protection and fundamental rights into a single coherent procedure. In parallel, formal cooperation between data authorities and AI regulatory bodies would promote consistent interpretations of key principles such as data minimization and

[429] Mammì Borruto F e Mantovani A, 'AI Act e GDPR: come si integrano le norme sulla protezione dei dati' (2024) *Agenda Digitale*.
[430] M Moretti, "Intelligenza artificiale e protezione dati: sinergie tra GDPR e AI Act" (2024) *Agenda Digitale.*
[431] P Falletta and A Marsano (n 400) 11.

purpose limitation, which are particularly challenging in dynamic AI systems, thereby strengthening the overall coherence between the AI Act and the GDPR[432].

The Meta Case further exposed these challenges. Meta attempted to use the public data of European Facebook and Instagram users to train its artificial intelligence models, on the basis of legitimate interest under Article 6(1)(f) GDPR.

The controversy engaged reactions from several national supervisory authorities and activated cooperation under the GDPR's one-stop-shop mechanism with the involvement of the EDPB, which on 18 December 2024 adopted Opinion 28/2024.

The case highlighted systemic tensions between the protection of fundamental rights and the promotion of technological innovation, opening new questions on the governance of AI within the European Union.

The Opinion clarified three crucial issues[433]: (i) the conditions under which AI models can be considered anonymous; (ii) the circumstances in which legitimate interest may serve as a lawful basis for training; and (iii) the implications of unlawfully processed data in the deployment phase[434].

In particular, the EDPB affirmed that a model is anonymous only when re-identification is highly improbable; that legitimate interest requires a strict test of necessity, proportionality and fairness; and that unlawful training data may compromise the lawfulness of subsequent deployment[435]. At

---

[432] E Drouard, 'Interactions and overlaps between the GDPR and AI Act' (2024) *Renaissance Numérique*.

[433] These directly relate to data protection legislation: the qualification of an AI model as anonymous defines whether the GDPR applies (Art. 4(1)); the reliance on legitimate interest concerns the lawfulness of processing (Art. 6(1)(f)); and the implications of unlawfully processed data in the deployment phase reflect the principle of lawfulness and accountability extending throughout the lifecycle of processing (Art. 5(1)(a)).

[434] I Menne, 'Training AI in Europa: tra protezione dei dati e competitività digitale' (2025) *Altalex*.

[435] M Moretti (n 430).

the same time, the case revealed practical limits of the European framework. The divergent reactions of national authorities showed that the one-stop-shop mechanism ensures procedural uniformity but not substantive consistency. Moreover, some GDPR rights remain difficult to apply to AI: the right to erasure collides with the technical impossibility of "machine unlearning", transparency duties are hard to fulfil given the opacity of training processes, and the use of public content risks undermining the protection of vulnerable groups such as minors [436].

In addition, although limited in scope, the Opinion represents a first attempt to adapt data protection principles to the technical complexity of AI, reaffirming that accountability, transparency and proportionality remain the guiding principles. The EDPB Opinion ultimately confirms the EU's commitment to fostering a responsible development of AI while safeguarding individuals' fundamental rights under the GDPR, which remains fully applicable to AI systems. Yet it leaves aside other critical aspects, such as the processing of sensitive data, automated decision-making, and privacy by design, and suggests that compliance must be assessed on a case-by-case basis. In this sense, the Opinion should not be read as a definitive reconciliation between the GDPR and the AI Act, but rather as an initial, still incomplete attempt to align two regulatory logics that remain only partially convergent[437].

Ultimately, the Meta case demonstrates both the adaptability and the fragility of the current framework: while GDPR concepts such as legitimate interest and accountability remain applicable, their interaction with the AI Act is still incomplete, generating interpretative uncertainties and enforcement challenges, questioning the system's ability to ensure an effective balance between technological innovation and the protection of personal data as a fundamental right.

[436] I Menne (n 434).
[437] M Moretti (n 430).

5.4 Comparative perspectives: the United States, China, and Japan

The global landscape on the regulation of artificial intelligence reveals deeper divergences in governance models and normative values. Beyond the European Union, which has opted for a comprehensive rights-based approach through the AI Act, the other leading jurisdictions are defining their own pathways. Specifically, the United States and China have become the principal global competitors in shaping the technological and regulatory race, while Japan represents an interesting case of convergence with the European vision.

5.4.1 The U.S. Approach

The regulatory framework of the United States regarding artificial intelligence is highly fragmented, characterized by the coexistence of multiple sources of law[438] and by a strong orientation towards technological innovation and economic competitiveness. Contrary to the EU AI Act aimed at generating a comprehensive and harmonized regime, the U.S. approach remains sectoral, based on a multi-layered framework rather than binding federal legislation, reflecting the tradition of limited federal intervention and reliance on private self-regulation[439].

Hard law provisions are more commonly introduced at the state level, whereas federal intervention often takes the form of sector action, congressional initiatives, or agency guidelines.

Although Congress has debated several bills – such as the *Algorithmic Accountability Act* (2019), the *AI in Government Act* (2020), and the *National AI Initiative Act* (2020) – few have become law, reflecting a modest growing concern about algorithmic threats[440]. Lacking a generic federal law,

[438] E Stradella, 'Le fonti nel diritto comparato: analisi di scenari extraeuropei (Stati Uniti e Cina)' (2022) 51(1) *DPCE Online* 71.
[439] 'Un confronto comparato tra la regolamentazione dell'IA negli Stati Uniti ed in Europa' (2025) *Rivista Diritto di Internet* 1.
[440] E Stradella (n 438) 74-75.

the agencies operate in distinct areas of technology: the Food and Drug Administration (FDA) controls AI-based medical devices under HIPAA regulations, the National Highway Traffic Safety Administration (NHTSA) regulates driverless cars with a focus on highway safety, and finance regulators such as the Securities and Exchange Commission (SEC) and the Federal Reserve monitor trading algorithmic practices with an eye towards transparency and consumer protection[441].

At the same time, State legislatures have also taken the lead: Maine has prohibited most governmental uses of facial recognition, while Virginia, Massachusetts, and Washington have adopted more limited or permissive rules[442].

The U.S. strategy is also reliant on voluntary standards and soft law. The FTC has issued guidance on transparency, accountability, data quality, and explainability, while the 2020 Office of Science and Technology Policy *Memorandum* explicitly rejected a precautionary approach, encouraging agencies to foster trust in AI through fairness and innovation-friendly policies[443]. Similarly, the National Institute of Standards and Technology *AI Risk Management Framework* provides voluntary guidelines constructed around transparency, traceability, fairness, and privacy, leaving corporations broad discretion in implementation[444].

Private industry also plays a central role, reinforcing the central role of private self-regulation. Major technology companies such as Microsoft, Google have adopted internal ethical guidelines, emphasizing fairness, transparency, and non-discrimination, illustrating the expectation that businesses should regulate themselves responsibly.

---

[441] 'Un confronto comparato tra la regolamentazione dell'IA negli Stati Uniti ed in Europa' (n 439) 1-2.
[442] E Stradella (n 438) 77-78.
[443] E Stradella (n 440).
[444] 'Un confronto comparato tra la regolamentazione dell'IA negli Stati Uniti ed in Europa' (n 439) 1.

Executive orders have also been significantly influential, enabling the President to establish priorities and dedicated infrastructures. In 2019, President Donald Trump signed the *Executive Order on Maintaining American Leadership in Artificial Intelligence* in 2019, which declared AI a national priority, favoring investment in AI research and development to ensure U.S. technological dominance at the global level[445].

The subsequent change of administration highlighted a sharp contrast. While former President Biden pursued a cautious strategy of responsible innovation – through the 2023 *Executive Order on AI* which imposed binding mandates on safety, privacy, and non-discrimination, and the *AI Bill of Rights* and its *Blueprint* setting up principles on reliability, anti-discrimination, and data protection safeguards – Trump's reelection reversed this course, redefining U.S. supremacy in AI as a strategic goal to assure dominance, promoting deregulation within the America First agenda[446].

One turning point was the debate on the *One Big Beautiful Bill Act (OBBBA)* of 2025, which initially included a clause known as "AI Enforcement Pause" to suspend federal regulation for five years while pre-empting more than 149 state laws on transparency and consumer protection. Though removed from the final text, the proposal revealed the divide between technology companies, supportive of deregulation as a means to simplify compliance and strengthen U.S. competitiveness and civil society, concerned about threats to civil rights and privacy[447].

In this context, the federal strategy of deregulation culminated in the *AI Action Plan* of July 2025 under the title *Winning the Race: America's AI Action Plan* emphasized innovation by removing regulatory obstacles, promoting infrastructure investment, and U.S. leadership abroad through AI

[445] Ibid. 2.

[446] M Foti, 'AI, cambio di rotta: dalle richieste di regolamentazione alla deregolamentazione trumpiana' (2025) *Altalex.*

[447] L Favarotto, 'Stati Uniti: chi detta le regole dell'IA?' (2025) *ISPI – Istituto per gli Studi di Politica Internazionale.*

diplomacy[448]. This agenda was reinforced by additional policies favorable to the technology industry, such as federal preemption of state-level AI laws, the legitimization of copyrighted material for algorithmic training, and privileged access to federal datasets. While justified as necessary to guarantee U.S. leadership in AI, this approach has deepened tensions between rapid technological innovation and the protection of fundamental rights[449].

By emphasizing industrial competitiveness and the geopolitical projection of technology, this approach represents a distinctly deregulatory model, designed to differentiate the U.S. approach from the more risk-oriented European framework (AI Act)[450]. In the absence of a uniform federal law, and with a heavy reliance on corporate self-regulation, concerns over privacy, transparency, and algorithmic discrimination have intensified, fueling calls for a comprehensive federal framework capable of ensuring minimum safeguards[451].

5.4.2 The Chinese Approach

China's governance of Artificial Intelligence reflects a state-led strategy aimed at consolidating international competitiveness, fostering economic growth, and reinforcing social stability. From the launch of the *New Generation Artificial Intelligence Development Plan* in 2017, Beijing has pursued a world leadership goal in AI by 2030, both industrially and commercially, as well as through technological and moral standards development. The Plan establishes three milestones: by 2020, the elaboration of initial ethical guidelines and regulatory norms; by 2025, the establishment of a preliminary system of laws, regulations, and security assessment mechanisms; and by 2030,

[448] H Anderson, HY Huang and J Oltean, 'White House Unveils Comprehensive AI Strategy: "Winning the Race: America's AI Action Plan"' (*White & Case*, 2025).
[449] M Foti (n 446).
[450] H Anderson et al (n 448).
[451] 'Un confronto comparato tra la regolamentazione dell'IA negli Stati Uniti ed in Europa' (n 439) 2.

the construction of a comprehensive legal and ethical framework for AI governance.

Unlike the United States' market-driven model or the European Union's rights-based, horizontal approach, China has primarily adopted a vertical regulation approach, targeting specific technologies and applications deemed risky[452].

This governance model is defined by strong central oversight, enabling the government to implement and enforce regulations with remarkable speed, particularly in sensitive areas such as surveillance and public services, with agencies such as the Cyberspace Administration of China and the Ministry of Industry and Information Technology setting policy directives and enforcement. Tech companies collaborate closely with government bodies, aligning their operations with national strategies for AI development and social governance, while civil society participation remains limited, with state-sanctioned organizations playing a more prominent role than independent NGO[453].

To implement the 2017 Plan, China first enacted a series of ethical and policy guidelines. In 2021, the *Ethical Code for the New Generation of Artificial Intelligence* (2021), which set out core principles to promote fairness, security, and transparency, while addressing risks such as bias, discrimination, and privacy violations, and in 2022, high-level guidelines to further strengthen the ethical governance of science and technology, further consolidating the normative foundations for China's AI regulation[454].

A second phase followed, marked by a sequence of targeted administrative regulations, each

[452] M Zou and L Zhang, 'Navigating China's regulatory approach to generative artificial intelligence and large language models' (2025) 1 *Cambridge Forum on AI: Law and Governance e8,* 1-4.

[453] A l-Maamari, 'Between Innovation and Oversight: A Cross-Regional Study of AI Risk Management Frameworks in the EU, U.S., UK, and China' (2025) *Cornell University arXiv* 12.

[454] S Migliorini, 'China's Interim Measures on generative AI: Origin, content and significance' (2024) *53 Computer L & Secur Rev* 105985 3.

addressing emerging risks in specific technological domains.

The *Provisions on Algorithmic Recommendations in Internet Information Services* (2021) required transparency in recommendation systems and granted users specific rights, such as the ability to turn off algorithmic recommendations, delete profiling tags, and obtain explanations when algorithms significantly affected their interests. The Provisions highlighted concerns about misinformation, manipulation, and discriminatory profiling in the digital information environment. Building on this framework, the *Regulations on Deep Synthesis* (2022) addressed the growing threats of AI-driven content generation, particularly deep fakes. Avoiding politically charged terminology, the regulations used the broader category of *deep synthesis technology* to cover text, images, audio, video, and virtual content created through deep learning and related methods. These rules mandated labelling, transparency, and security measures to mitigate threats to privacy, national security, and public trust.

The most significant development was in 2023 with the *Interim Measures of Generative AI*, also advanced by CAC and multiple Ministries. They require providers to conduct security assessments, ensure transparency, and prevent harmful content, with the dual aim of promoting innovation and safeguarding security. Though Articles 1 and 3 stress the need to balance innovation with lawful governance and public protection, the final text places stronger emphasis on technological development, framed within China's broader modernization strategy[455]. Crucially, they reaffirm that generative AI services remain subject to the broader legal framework, including the Personal Information Protection Law (PIPL): even frontier technologies must comply with data protection requirements, with penalties for violations. Providers are treated as content producers and held legally responsible for the outputs of their systems, highlighting China's emphasis on control and

[455] M Zou and L Zhang (n 452) 4-5.

accountability[456].

In parallel, China has relied on technical standards to operationalize its regulations such as the *Implementation Guidelines on Content Labelling in Generative AI Services* in 2023, and, in 2024 the mandatory *Basic Security Requirements for Generative AI Services*, which defined obligations on datasets, models, and security assessments. This focus on information and content security was further reinforced by the *AI Safety Governance Framework*, which identified risks such as misinformation, bias, privacy leakage, and threats to national and ideological security[457].

More recently, Shanghai hosted the World Artificial Intelligence Conference, where the People's Republic of China firmly presented its national AI strategy through a thirteen-point action plan, accompanied by a proposal to establish international bodies dedicated to AI regulation, with the declared objective of positioning China as a responsible actor in the global governance of the technology, particularly in relation to countries of the Global South. Unlike the United States, which emphasizes the development of cutting-edge technological models, China's strategy is distinguished by its focus on the widespread diffusion of practical AI applications across strategic sectors of society and the economy[458].

Overall, China's AI governance reflects a state-led, security-oriented model that combines rapid regulatory interventions with technical standards, prioritizing national security and social stability over individual rights: a sharp contrast to the EU's rights-based framework and the U.S.'s fragmented, market-driven approach.

[456] S Migliorini (n 454) 4-6.
[457] M Zou and L Zhang (n 452) 4.
[458] K Northrop, 'China is betting on a real-world use of AI to challenge U.S. control' (2025) *The Washington Post* https://www.washingtonpost.com/world/2025/07/31/china-ai-united-states-control/?utm.

5.4.3 The Japanese Approach

Japan's approach to the regulation of AI has evolved progressively, moving from early ethical principles to operational guidelines and, more recently, to the adoption of an initial legislative framework. The first government initiatives date back to 2015 with the establishment of a dedicated R&D system, research on the impact of AI on the country's industrial structure, and the promotion of *Society 5.0*, a future vision in which new technologies drive social and economic transformation[459].

This trajectory has been guided by a human-centric vision of AI, emphasizing human dignity and values, social welfare, diversity, trust, and cooperation. In this context, the government published the *Social Principles of Human-Centric AI* in 2019, which set out key aspects[460], with the aim of using AI to attain them rather than limit its use[461]. Since then, Japan's strategy has followed two complementary directions: regulation on AI, aimed at managing the risks associated with the use of these technologies, and regulation for AI, namely regulatory reforms intended to promote their adoption.

In accordance with the *AI Governance in Japan report* published in 2021 by the Ministry of Economy, Trade and Industry (METI), the Country adopted an agile governance model based on voluntary corporate efforts and non-binding guidelines, complemented by sectoral rules on transparency obligations for digital platforms and competition safeguards. This framework is reinforced by other relevant instruments such as the Act on the Protection of Personal Information

[459] T Ichikawa, 'Norms in New Technological Domains: Japan's AI Governance Strategy' (2025) *CSIS - Center for Strategic & International Studies*.

[460] Including transparency, accountability, fairness, security, privacy, education, research, governance, and international cooperation.

[461] K Gardhouse, 'A Comparison of the Approaches to Generative AI in Japan and China' (*Private AI*, 2024) https://www.private-ai.com/en/blog/generative-ai-japan-china-comparison?utm.

(APPI), amended in 2022, introduced the concept of pseudonymized data to enable the safer use of personal data for algorithmic training, as well as governmental guidelines, such as the *Governance Guidelines for Implementation of AI Principles*, and by private and academic initiatives.

On the other hand, regulation for AI aims to advance artificial intelligence as a driver of economic and social modernization. In this perspective, the legislator has introduced targeted sectoral reforms, to clarify the lawfulness of using data for machine learning and strengthened the protection of shared datasets against misuse[462].

One of the most important features of Japan's AI policy regime is international interoperability. Rather than focusing on reducing domestic risks, Japan's policy seeks to ensure compatibility between different governance systems. In the context of superpowers such as the EU or U.S., Japan positions itself as a neutral mediator as a G7 member and the only Asian country in the group[463]. This approach was consolidated in 2023, when Japan, holding the G7 presidency, led the Hiroshima AI Process, the first attempt to build an international framework for the governance of advanced artificial intelligence. The stated goal was to maximize the innovative opportunities of AI, particularly generative AI, while at the same time mitigating risks[464].

Building on this, in April 2024, the Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications (MIC) published the *AI Guidelines for Business,* later updated in 2025. Although non-binding, they set foundational values and cross-sector principles[465] embedding AI ethics into corporate governance structures and influence judicial interpretation,

[462] H Habuka, 'Japan's Approach to AI Regulation and Its Impact on the 2023 G7 Presidency' Strategy' (*CSIS - Center for Strategic & International Studies,* 2023).
[463] T Ichikawa (n 459).
[464] 'The Hiroshima AI Process: Leading the Global Challenge to Shape Inclusive Governance for Generative AI' (2024) *JapanGov – The Government of Japan.*
[465] Including dignity, inclusion, sustainability, fairness, safety, and privacy.

procurement standards, and assessments, while fostering voluntary industry self-regulation. In parallel, the Personal Information Protection Commission (PPC) warned about risks of inserting personal data into generative AI systems, requiring compliance with the APPI and even issuing a formal warning to OpenAI[466].

Although Japan has traditionally relied on a soft-law approach to AI regulation, discussions on introducing binding legislation gained momentum in early 2024, largely in response to developments in the European Union and the United States.

In February 2024, a draft bill requiring businesses working with advanced AI systems to provide notification and reporting was delivered, reflecting Japan's broader strategy of promoting international interoperability. Moreover, Prime Minister Ishiba announced the ambition to build an AI legal system that could serve as a model for the world. The proposal culminated in the *AI Act* – officially *the Bill on Promotion of R&D and Utilization of AI-related Technologies* –enacted in May 2025[467]. The Act does not impose new binding obligations, but establishes an AI Strategic Headquarters, defines the responsibilities of public and private actors, and provides direction through a national Basic Plan for AI. It defines AI broadly as technologies simulating human cognition and rests on four guiding principles: treating AI as a strategic asset, promoting industrial use, mitigating risks through transparency, and contributing to international norms. While non-binding, the Act sets Japan's political vision for AI and may signal more concrete regulation in high-risk sectors such as healthcare or critical infrastructure[468].

Overall, Japan's approach to AI regulation remains marked by flexibility, reliance on soft law, and a strong emphasis on international interoperability. The AI Act provides a strategic vision rather

[466] K Inoue and C Kamata, 'Japan's emerging framework for responsible AI: legislation, guidelines and guidance' (2025) *International Bar Association*.
[467] T Ichikawa (n 459).
[468] K Inoue and C Kamata (n 466).

than binding obligations, while instruments such as the APPI and the AI Guidelines for Business complement this framework. Japan thus seeks to balance innovation with safeguards, positioning itself as a mediator in global AI governance.

5.5 Concluding Remarks: Challenges and Future Perspectives

The comparative analysis conducted shows how Artificial Intelligence regulation has become a central testing ground for the protection of personal data as a fundamental right. On the international stage, initiatives such as the OECD Recommendation, UNESCO's Ethics of AI, and the UN White Paper have progressively converged on the idea that privacy and data protection are indispensable conditions for trustworthy AI. The Council of Europe's Framework Convention further demonstrates the transition from ethical principles to binding safeguards.

Against this background, regional and national frameworks differ significantly.

The European Union stands out for its rights-based approach, firmly anchored in the GDPR and now extended through the AI Act, which explicitly integrates fundamental rights impact assessments and reinforces the centrality of data protection. The United States, by contrast, maintains a fragmented, market-driven regime, where federal inertia and reliance on self-regulation leave privacy and algorithmic accountability exposed to sectoral inconsistencies. China has pursued a state-centric, security-oriented strategy, where rapid regulatory interventions and technical standards prioritize social stability and national competitiveness over individual guarantees. Japan, instead, suggests an intermediate model, combining soft-law flexibility with a strong emphasis on international interoperability and human-centric

principles.

Across these models, common challenges persist.

The technical opacity of AI systems complicates the enforcement of principles such as

transparency, accountability, and data minimization. The tension between the demands for vast datasets and the guarantees of privacy and consent undermines the effectiveness of traditional safeguards. In addition, cross-border data flows and global corporate actors expose the limits of purely domestic regulation, reinforcing the urgency of harmonized international standards.

Therefore, reconciling technological innovation with safeguards for personal data will remain one of the central challenges of AI regulation. The models examined in this chapter show different paths towards this balance, but also highlight persistent gaps and tensions that future governance frameworks will need to address.

CONCLUSION

The analysis conducted in this thesis has shown how, in recent decades, the protection of personal data has been progressively recognized as a fundamental right and an essential safeguard in the digital era. Through a comparative approach, the study has traced the historical and normative evolution of this right across different contexts: from the international framework to the European Union, from the United States to the extra-Western experiences of China and Japan, and finally to the most current and forward-looking perspectives, with particular focus on the impact of artificial intelligence. What emerges is a complex framework in which data protection has become a central component of the corpus of fundamental rights, though it assumes different forms depending on the legal systems and technological challenges they face.

From an original conception of privacy as the protection of private life against external intrusions, the right to personal data protection has progressively emerged as an autonomous and fundamental right. This process, initiated with the concept of the right to be let alone and consolidated through international instruments, from the Universal Declaration of Human Rights to the International Covenant on Civil and Political Rights, up to the Council of Europe's Convention 108+ and the OECD Guidelines of 1980, has marked the transition from a negative safeguard against interference to a positive system of rules designed to guarantee dignity, autonomy, and freedom in the digital age.

The legal systems selected in this research – the European Union, the United States, China, and Japan – exemplify markedly different approaches to personal data protection, each reflecting distinct legal traditions, institutional frameworks, and political cultures.

The European Union has established itself as the most advanced model, enshrining data protection as a fundamental right at the constitutional level through Article 8 of the Charter of Fundamental

Rights and Article 16 of the Treaty on the Functioning of the European Union, and articulating, first through Directive 95/46/EC and later through the General Data Protection Regulation, a legal framework of safeguards that combines substantive rights, accountability obligations, and effective sanctioning mechanisms. The extraterritorial effect of the Regulation has also contributed to the global diffusion of European standards, giving rise to the so-called Brussels Effect. Yet, significant limitations remain: the uneven application of the GDPR by national authorities, the fragmentation of enforcement procedures, and the limited scope of the Charter in areas such as national security. By contrast, the United States lacks constitutional recognition of the right to data protection and relies on a fragmented, sectoral framework, based on statutes such as HIPAA and COPPA, alongside the ex post enforcement role of the Federal Trade Commission. This model, functional to market and consumer protection, nonetheless reveals a significant *fundamental rights gap* compared to Europe, as evidenced by the Schrems I and Schrems II judgments that invalidated transatlantic data transfer mechanisms. The newly adopted EU–US Data Privacy Framework represents the latest attempt to reconcile the two systems, but doubts remain as to whether it can ensure a level of protection truly equivalent to that guaranteed within the European Union. A very different picture emerges in China, which between 2017 and 2021 developed an articulated legal system culminating in the Personal Information Protection Law: a regime that recalls universal principles of lawfulness and transparency, but is embedded in a logic of digital sovereignty and state control, where data protection functions does not limit public power but serves as an instrument of political and economic governance. Japan stands in sharp contrast: starting from a conception of privacy primarily linked to social honor and reputation, diverging from the Western idea of individual autonomy, it has undertaken a trajectory of convergence with European standards. The reforms of the Act on the Protection of Personal Information, together with the establishment of an independent supervisory authority, led to the EU's 2019 adequacy decision: an

emblematic case of the Brussels Effect where European legal standards are received within a distinct cultural and legal context.

On the global level, emerging technologies have amplified risks for fundamental rights. The most advanced and delicate frontier is today represented by the regulation of artificial intelligence and its implications for data protection. Artificial intelligence, raises problems of mass data collection, profiling, algorithmic opacity, and erosion of consent, placing traditional principles of data protection under strain. Cross-border data flows and mass surveillance practices also reshape the boundaries of protection, questioning the effectiveness of national responses. In this context, the need for global AI governance appears increasingly urgent, given the lack of binding international provisions: just recently the Council of Europe adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, the first binding treaty in this area, which represents an important but not yet sufficient step towards global governance. Again, national differences are particularly evident. The European Union has positioned itself at the forefront, complementing the GDPR with the AI Act, which prohibits practices incompatible with human dignity and introduces obligations proportionate to the level of risk. The United States maintains a fragmented framework, combining soft law, executive initiatives, and voluntary practices, privileging innovation and competitiveness over uniform guarantees. China follows a state-centric model, where the PIPL and the 2023 Interim Measures subject AI systems, including generative AI, to state priorities of surveillance and security. Japan has progressively strengthened its framework, from the APPI to the adoption of a national AI Act with strategic purposes, aimed at fostering interoperability and democratic values.

Overall, the comparison reveals a fragmented but dynamic landscape. The European Union emerges as the promoter of an organic, rights-based model; the United States privileges market logics; China emphasizes sovereignty and state control; while Japan represents a trajectory of

convergence towards Europe. This demonstrates that no single model prevails, but rather a plurality of approaches reflecting different conceptions of the relationship between the individual, the State, and technology. It nevertheless remains clear that data protection is not merely a set of technical rules, but a genuine safeguard of freedom in the digital society, a guarantee of autonomy and dignity, and a condition for the exercise of many other fundamental rights. Emerging challenges, from mass surveillance to regulatory fragmentation, to the disruptive impact of AI, require continuous legal and institutional adaptation and call for the definition of common standards of protection.

In conclusion, this thesis has highlighted how data protection, while shaped differently across legal systems, remains a cornerstone of the democratic order in the digital era and a key field where the balance between technological progress and fundamental rights is constantly tested. It is not merely a set of technical rules, but a safeguard of freedom and a guarantee of autonomy and dignity in the digital society. Emerging challenges, from mass surveillance to regulatory fragmentation, to the disruptive impact of AI, require constant legal and institutional adaptation and call for the definition of international standards of protection. With the continuous advance of technology, data protection has become as a central safeguard to ensure that innovation develops in harmony with human rights, fostering a more just, transparent, and human-centered society.

BIBLIOGRAPHY

Anderson H, Huang HY e Oltean J, 'White House Unveils Comprehensive AI Strategy: "Winning the Race: America's AI Action Plan"' (*White & Case*, 2025) https://www.whitecase.com/insight-alert/white-house-unveils-comprehensive-ai-strategy-winning-race-americas-ai-action-plan

Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices*, 881/11/EN WP 185 (European Commission, 2011). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, WP 136, (European Commission, 2007). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Bartow A, 'Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China' (2013) 74 *Ohio State Law Journal*.

Bera M, *Il GDPR e la disciplina dei soggetti del trattamento alla prova dell'evoluzione tecnologica* (Tesi di laurea, Università degli Studi di Pavia 2025). https://unitesi.unipv.it/retrieve/b9c83ba1-c426-44bc-b4dc-56514d6de086/Tesi-Magistrale-Mattia-Bera.pdf

Bing, J. 'The Council of Europe Convention and OECD Guidelines on Data Protection' (1984) 5 *Michigan Yearbook of International Legal Studies, HeinOnline.*

Birnhack MD, 'The EU Data Protection Directive: An Engine of a Global Regime' (2008) 24(6) *Computer Law & Security Report*.

https://e-revistas.uc3m.es/index.php/CDT/article/view/8083/6236

Bloomberg Law, 'State Privacy Legislation Tracker' (*Bloomberg Law*, 2025).

https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#map-of-state-privacy-laws.

Blue N, 'Spirited Away: The EU's Adequacy Decision for Japan as a Roadmap for U.S. Privacy Law after Schrems II' (2022) 21 *Washington University Global Studies Law Rev*.

https://journals.library.wustl.edu/globalstudies/article/8756/galley/25550/view

Boyne SM, Data Protection in the United States (2018) 66 (suppl 1) *American Journal of Comparative Law*.

https://d1wqtxts1xzle7.cloudfront.net/63775948/DataProtection_20200629-71006-17jtabm-libre.pdf?1593441027=&response-content-disposition=inline%3B+filename%3DData_Protection_in_the_United_States.pdf&Expires=1751563157&Signature=JeogF2TsN94qo6ca~Mz2-D11745lFQixsm9-wVk0sl6EcPrGe2TdKAZvcRmORuInl1gTUzUvXksAa4fHFe9~6A6~kHoNUZESeK4nnjGh6yd4dphPhSXZCX-tfv2Jt28fZHfxkKC7Nx~kMrNFd9MnsV4-MtutY80WjiZd01zfC1OtIgwzWFyPqHeXOWnX5kcq~Ti1Gwsdj5FMRYy0cLSQspmyvgT3h5~2WQaiMeXZBp8EmxjJjqyFD2Dz3utTJ00OtMB2UbyckP32rJp3wHkAihdTQJlh7LASiP40SPTIoE7IzJ0298RIxDhW6sbaTZaypro3LS91GAiVL5d2AQQZPg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Bruno G, 'Diritto alla riservatezza: nascita ed evoluzione giurisprudenziale in Italia' (2025) *Filodiritto*.

https://www.filodiritto.com/diritto-alla-riservatezza-nascita-ed-evoluzione-giurisprudenziale-italia

Bruno Saetta, 'Dato personale e categorie di dati' (*Garante per la protezione dei dati personali*, 2018).

https://protezionedatipersonali.it/dato-personale

Califano L, Fiorillo V, and Galli F, *La protezione dei dati personali: natura, garanzie e bilanciamento di un diritto fondamentale* (Giappichelli 2023).

https://www.giappichelli.it/media/catalog/product/excerpt/9791221104578.pdf?srsltid=AfmBOoq6rlZ9PxqlE3HHZHYmn8C4td8QE59QBhHbkrIrv7EdGSZsHuVD

Cappai M, Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale? (2024) *Federalismi.it.*

https://eusl.it/wp-content/uploads/2025/03/IA-e-protezione-dei-dati-personali-nel-ddl-n.-1146-Marco-Cappai.pdf?utm

Carpanelli, E., et al. *La protezione dei dati nel diritto internazionale ed europeo: Il ruolo delle corti nazionali nell'applicazione della Carta dei Diritti Fondamentali* (Università di Parma, Centro Studi in Affari Europei e Internazionali (CSEIA), Progetto E-NACT, n.d).

https://cjc.eui.eu/wp-content/uploads/2020/05/eNACT_Handbook_Italian-version_data-protection-compresso.pdf

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* [2020] ECLI:EU:C:2020:559.
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62018CJ0311

Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790.
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62017CJ0623

Centre for Information Policy Leadership, *Comparison of U.S. State Privacy Laws: Data Protection Assessments* (2024).
https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comparison_us_state_privacy_laws_dpa_feb14.pdf

Centre for Intellectual Property and Information Law, *Complete Travaux Préparatoires of the Data Protection Directive (95/46/EC)* (Cambridge University 2001)
https://resources.law.cam.ac.uk/cipil/travaux/data_protection/COMPLETETRAVEAU(ENGLISH)DPDIRECTIVE.pdf

Chai X, 'Comparative Study on Data Protection Between China, The United States and Europe' (2023) 13 *Journal of Education Humanities and Social Sciences*.
10.54097/ehss.v13i.8217

Charter of Fundamental Rights of the European Union [2000] OJ C364/1
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000X1218

Chen J and Sun J, 'Understanding the Chinese Data Security Law' (2021) 2 *International Cybersecurity Law Review*.
https://doi.org/10.1365/s43439-021-00038-3

China Briefing Team, 'The PRC Personal Information Protection Law (Final): A Full Translation' (2021). https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

China Law Translate, *Data Security Law* (20 June 2021). https://www.chinalawtranslate.com/en/datasecuritylaw/

Colapietro, C., 'I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale' (2018) *Federalismi.it* n. 22. https://www.astrid-online.it/static/upload/cola/colapietro_federalismi-21_11_18.pdf.

Commission Implementing Decision (EU) 2019/419 of 23 January 2019 on the adequate protection of personal data by Japan under Regulation (EU) 2016/679 [2019] OJ L76/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419 ù

Commission of the European Communities, Communication from the Commission to the Council and the European Parliament: Protection of individuals in relation to the processing of personal data COM (90) 314 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990DC0314

Commission, '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. https://eur-lex.europa.eu/resource.html?uri=cellar:d02eb625-1a4d-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF

Commission, ‘Second report on the application of the General Data Protection Regulation’ (Communication COM(2024) 357 final, 25 July 2024).
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52024DC0357&utm_source

Commission, Commission Implementing Decision (EU) 2016/1250 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207/1.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250

Commission, Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU–US Data Privacy Framework [2023] OJ L231/1.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D1795

Commission, 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 (General Data Protection Regulation) COM (2012) 11 final.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:en:PDF

Compet-e, ‘Il GDPR non sta funzionando come dovrebbe’ (2022).
https://www.compet-e.com/il-gdpr-non-sta-funzionando-come-dovrebbe/

Coos A, ‘Data Protection in Japan: All You Need to Know about APPI’ (*Endpoint Protector Blog*, 2022). https://www.endpointprotector.com/blog/data-protection-in-japan-appi

Costello RÁ, 'Schrems II: Everything Is Illuminated?' (2020) 5(2) *European Papers-European Forum* 1045.

https://www.europeanpapers.eu/europeanforum/schrems-II-everything-is-illuminated

Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No. 181, 2001)

Council of Europe, Ameding protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223, 2018).

https://rm.coe.int/16808ac918

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (1950).

https://www.echr.coe.int/documents/d/echr/convention_ENG

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (1981).

https://rm.coe.int/1680078b37.

Council of Europe, Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No 225, 2024).

https://rm.coe.int/1680afae3c

Council of the European Union, 'Data protection: Council agrees position on GDPR enforcement rules' (Press release, 13 June 2024).

https://www.consilium.europa.eu/it/press/press-releases/2024/06/13/data-protection-council-agrees-position-on-gdpr-enforcement-rules/

Council of the European Union, ‘Data protection: Council and European Parliament reach deal to make cross-border GDPR enforcement work better for citizens’ (press release, 16 June 2025). https://www.consilium.europa.eu/it/press/press-releases/2025/06/16/data-protection-council-and-european-parliament-reach-deal-to-make-cross-border-gdpr-enforcement-work-better-for-citizens/#:~:text=25%20maggio%202018.-,Ricevibilit%C3%A0,sulla%20base%20delle%20stesse%20informazioni.

Court of Justice of the European Union, 'Field of Application of the Charter of Fundamental Rights of the European Union' (Fact Sheet, 2018). https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_en.pdf?utm_source

Creemers R, ‘China’s Emerging Data Protection Framework’ (2022) *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyac011

Crespi S, 'La tutela dei dati personali UE a seguito della sentenza Schrems' (2015) *Eurojus.* https://rivista.eurojus.it/la-tutela-dei-dati-personali-ue-a-seguito-della-sentenza-schrems/?generate_pdf=2444

Cybersecurity Law of the People’s Republic of China. http://www.csrc.gov.cn

de Hert P and Papakonstantinou V, *The Data Protection Regime in China: In-depth Analysis for the LIBE Committee*, Policy Department C - Citizens’ Rights and Constitutional Affairs, European Parliament (2015).

https://cris.vub.be/ws/portalfiles/portal/17639565/pdh15_vpThe_data_protection_regime_in_ChinaIPOL_IDA_2015_536472_EN.pdf

Digital Policy Alert, 'EU regulation laying down additional procedural rules relating to the enforcement of GDPR in cross-border cases'.
https://digitalpolicyalert.org/change/6283-eu-regulation-laying-down-additional-procedural-rules-relating-to-the-enforcement-of-gdpr-in-cross-border-cases

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) [2002] OJ L201/37.
https://www.edps.europa.eu/sites/default/files/publication/dir_2002_58_it.pdf

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136

Drouard E, 'Interactions and overlaps between the GDPR and AI Act' (*Renaissance Numérique*, 2024).
https://www.renaissancenumerique.org/en/publications/interactions-and-overlaps-between-the-gdpr-and-ai-act-with-etienne-drouard/?utm

Duli B, *Data Transfers between the EU and US: The impact of Schrems I and Schrems II for cross-border data flows, privacy, and national security* (Master of Transnational Law thesis, Católica Global School of Law 2021).

https://core.ac.uk/download/491648449.pdf

Esposito L, *'La protezione dei dati personali: l'impatto del GDPR sugli Stati membri dell'Unione europea'* (Tesi di Laurea Magistrale, Luiss Guido Carli 2018).

https://tesi.luiss.it/23704/1/115033_ESPOSITO_LUCA.pdf

EUR-lex Access to European Union law, DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046

EUR-Lex Access to European Union law, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

European Commission, 'A European strategy for data' (2020).

https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission, 'European Approach to Artificial Intelligence' (2025).

https://digital-strategy.ec.europa.eu/it/policies/european-approach-artificial-intelligence

European Commission, ‘Legal framework for EU data protection’ (2024). https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en

European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust COM(2020) 65 final, Brussels, 19 February 2020. https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

European Data Protection Board, Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, Version 1.1 (2024). https://www.edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf

Falletta P and Marsano A, Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull’intelligenza artificiale e GDPR (2024) 1 *Rivista Italiana di Informatica e Diritto.* https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/238/183

Favarotto L, ‘Stati Uniti: chi detta le regole dell’IA?’ (2025) *ISPI – Istituto per gli Studi di Politica Internazionale.* https://www.ispionline.it/it/pubblicazione/stati-uniti-chi-detta-le-regole-dellia-214850

Finocchiaro G, ‘Intelligenza Artificiale e protezione dei dati personali’ (2019) *Giurisprudenza Italiana*. http://www.blogstudiolegalefinocchiaro.it/wp-content/uploads/2019/09/G.-Finocchiaro_GiurisprudenzaItaliana_2019.pdf

Foti M, ‘AI, cambio di rotta: dalle richieste di regolamentazione alla deregolamentazione trumpiana’ (2025) *Altalex.*

https://www.altalex.com/documents/news/2025/05/13/ai-cambio-rotta-richieste-regolamentazione-deregolamentazione-trumpiana

Gardhouse K, ‘A Comparison of the Approaches to Generative AI in Japan and China’ (*Private AI*, 2024).

https://www.private-ai.com/en/blog/generative-ai-japan-china-comparison?utm

Gentile C, 'La saga Schrems e la tutela dei diritti fondamentali' (2021) *Federalismi.it.*

https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=44743&dpath=document&dfile=13012021225756.pdf&content=La%2Bsaga%2BSchrems%2Be%2Bla%2Btutela%2Bdei%2Bdiritti%2Bfondamentali%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B

Giacalone M, ‘Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework’ (2023) 8 *European Papers-European Forum.*

https://www.europeanpapers.eu/en/system/files/pdf_version/EP_EF_2023_I_009_Maria_Giacalone_00644.pdf

Gomstyn A and Jonker A, ‘Esplorare i problemi di privacy nell’era dell’AI’ (*IBM Think*, 2024).

https://www.ibm.com/it-it/think/insights/ai-privacy

Gong J, Dong M e Che J, ‘An In-depth Analysis of China’s Network Data Security Regime – Part II: Detailed Look at Data Protection Requirements’ (*Bird & Bird*, 2025).

https://www.twobirds.com/en/insights/2025/china/an-indepth-analysis-of-chinas-network-data-security-regime

Gorla S and Iaselli M, *Storia della Privacy*, 2015.

www.micheleiaselli.it/storiadellaprivacy.pdf.

Government of Japan, Act on the Protection of Personal Information (2022). https://www.ppc.go.jp/files/pdf/APPI_english.pdf.

Greenleaf G, 'China's Completed Personal Information Protection Law: Rights Plus Cyber-security' (2021) UNSWLRS 91, (2021) 172 *Privacy Laws & Business International Report.*

https://ssrn.com/abstract=3989775

Guarda P and Bincoletto G, *Diritto comparato della privacy e della protezione dei dati personali* (Ledizioni, 2023).

https://iris.unitn.it/retrieve/handle/11572/374792/630227/Diritto%20comparato%20della%20privacy_web.pdf

Guo Z, Hao J and Kennedy L, 'Protection Path of Personal Data and Privacy in China: Moving from Monism to Dualism in Civil Law and Then in Criminal Law' (2024) 52 *Computer Law & Security Review* 105928.

https://doi.org/10.1016/j.clsr.2023.105928

Harrington D, 'U.S. Privacy Laws: The Complete Guide' (*Varonis*, 2025).

https://www.varonis.com/blog/us-privacy-laws

Hartzog W and Solove DJ, 'The Scope and Potential of FTC Data Protection' (2015) 83 *George Washington Law Review 2230.*

https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4037&context=faculty_scholarship

He A, *State-Centric Data Governance in China* (CIGI Papers No 282, Centre for International Governance Innovation 2023).
https://www.cigionline.org/static/documents/no.282.pdf

Hoffmann T, *Data Protection by Definition: Report on the Law of Data Disclosure in* Japan (University of Passau IRDG Research Paper Series No 22-03, 2022).

Huddleston J, A Primer on Data Privacy Enforcement Options (*American Action Forum*, 2020).
https://www.americanactionforum.org/print/?url=https://www.americanactionforum.org/insight/a-primer-on-data-privacy-enforcement-options/

Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (2014).
https://edps.europa.eu/data-protection/our-work/publications/articles/eu-data-protection-law-review-directive-9546ec-and_en.

IAPP, 'US Litigation Series: Security Breaches' (*IAPP*, 2025).
https://iapp.org/resources/article/us-litigation-series-security-breaches/.

Ichikawa T, 'Norms in New Technological Domains: Japan's AI Governance Strategy' (*CSIS – Center for Strategic & International Studies*, 2025).
https://www.csis.org/analysis/norms-new-technological-domains-japans-ai-governance-strategy

Inoue K and Kamata C, 'Japan's emerging framework for responsible AI: legislation, guidelines and guidance' (*International Bar Association*, 2025).
https://www.ibanet.org/japan-emerging-framework-ai-legislation-guidelines?utm

Ishiwaka K, *Japan's Personal Information Protection Legal Framework and Its International Initiatives* (Presentation, WTO Joint Statement Initiative on E-Commerce Workshop, 2025). https://www.wto.org/library/events/event_resources/ecom_0805202510/779_2422.pdf

Jia M, 'Authoritarian Privacy' (2024) 91(3) *University of Chicago Law Review*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4362527

Kibby C, 'US Litigation Series: Security Breaches' (*IAPP*, 2025). https://iapp.org/resources/article/us-litigation-series-security-breaches/

Kokas A, 'China's 2021 Data Security Law: Grand Data Strategy with Looming Implementation Challenges' (*China Leadership Monitor*, Winter 2021, Issue 70, 2021).

Korff D and Georges M, *The DPO Handbook: Guidance for Data Protection Officers in the Public and Quasi-Public Sectors on How to Ensure Compliance with the European Union General Data Protection Regulation* (2019). https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf

Krause D, The EU AI Act and the Future of AI Governance: Implications for U.S. Firms and Policymakers (*SSRN*, 2025). https://ssrn.com/abstract=5181797

Latham & Watkins, 'China Clarifies Privacy and Data Security Requirements in Network Data Security Management Regulations' (*Client Alert Commentary*, 2025). https://www.lw.com/thoughtLeadership/china-clarifies-privacy-and-data-security-requirements

Lee J, 'Hacking into China's Cybersecurity Law' 2018 53 *Wake Forest Law Review*. https://wakeforestlawreview.com/wp-content/uploads/2019/01/w05_Lee-crop.pdf

Lenaerts K, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2012) 8(3) *European Constitutional Law Review (EuConst).* https://www.cambridge.org/core/services/aop-cambridge-core/content/view/44E09CF275FAB8530096667DB525E2E6/S1574019612000260a.pdf/exploring-the-limits-of-the-eu-charter-of-fundamental-rights.pdf?utm_source

Li W and Chen J, 'From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China' (2024) *Computer Law and Security Review.* https://doi.org/10.1016/j.clsr.2024.105994

Li W and Chen J, 'From Brussels effect to gravity assists: Understanding the evolution of the GDPR-inspired personal information protection law in China' (2024) 54 *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2024.105994

Mammì Borruto F e Mantovani A, 'AI Act e GDPR: come si integrano le norme sulla protezione dei dati' (2024) *Agenda Digitale*. https://www.agendadigitale.eu/sicurezza/privacy/ai-act-e-gdpr-come-si-integrano-le-norme-sulla-protezione-dei-dati/?utm

Menne I, 'Training AI in Europa: tra protezione dei dati e competitività digitale' *Altalex* (2025). https://www.altalex.com/documents/news/2025/06/27/training-ai-europa-protezione-dati-competitivita-digitale

Miglietti L, "Profili storico-comparativi del diritto alla privacy." *Diritti Comparati* (2014). www.diritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/

Migliorini S, ‘China’s Interim Measures on generative AI: Origin, content and significance’ (2024) 53 *Computer Law & Security Rev* 105985.
https://doi.org/10.1016/j.clsr.2024.105985

Miller T, *How Privacy Policies Shape the Future of the Online Economy: A US–EU Comparison (*Mercatus Center, George Mason University 2025).
file:///C:/Users/AriPC/Downloads/5030-miller-privacypolicy-pr-v1b_1.pdf

Minárik T and Garcia A, ‘CJEU Determines Dynamic IP Addresses Can Be Personal Data but Can Also Be Processed for Operability Purposes’ (2016) *CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence*.
https://ccdcoe.org/incyder-articles/cjeu-determines-dynamic-ip-addresses-can-be-personal-data-but-can-also-be-processed-for-operability-purposes/

Ministero della Giustizia, Guida all’articolo 8 della Convenzione – Diritto al rispetto della vita privata e familiare. Corte Europea dei Diritti dell’Uomo (2021).
https://www.giustizia.it/cmsresources/cms/documents/guida_cedu_articolo8_agg31ago2021.pdf

Miyashita H, ‘EU–Japan Mutual Adequacy Decision’ (2020) *blogdroiteuropéen.*
https://blogdroiteuropeen.com/2020/06/25/eu-japan-mutual-adequacy-decision-by-hiroshi-miyashita/

Miyashita H, 'The Evolving Concept of Data Privacy in Japanese Law' (2011) 1(4) *International Data Privacy Law*.
https://doi.org/10.1093/idpl/ipr019

Moretti M, ‘Intelligenza artificiale e protezione dati: sinergie tra GDPR e AI Act’ (*Agenda Digitale*, 2025).

https://www.agendadigitale.eu/sicurezza/privacy/intelligenza-artificiale-e-protezione-dati-sinergie-tra-gdpr-e-ai-act/

Northrop K, 'China is betting on a real-world use of AI to challenge U.S. control' (*The Washington Post*, 2025).

https://www.washingtonpost.com/world/2025/07/31/china-ai-united-states-control/?utm

OECD, Recommendation of the Council on Artificial Intelligence (adopted 22 May 2019, amended 3 May 2024) OECD/LEGAL/0449.

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

OneTrust DataGuidance, *Comparing privacy laws: GDPR v. PIPL* (2021).

https://www.dataguidance.com/sites/default/files/gdpr_v_pipl_.pdf

Organisation for Economic Co-operation and Development, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, (No. 0188, 2013).

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

Organisation for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (2002).

https://doi.org/10.1787/9789264196391-en.

Orito Y and Murata K, 'Privacy Protection in Japan: Cultural Influence on the Universal Value' (2005) *Electronic Proceedings of Ethicomp 5*.

https://www.isc.meiji.ac.jp/~ethicj/Privacy%20protection%20in%20Japan.pdf

Privacy International and Law and Technology Centre of the University of Hong Kong, *The Right to Privacy in China: Stakeholder Report, Universal Periodic Review, 17th Session – China* (2013). https://upr-info.org/sites/default/files/documents/2013-12/js8_upr17_chn_e_main.pdf

Qi A, Shao G and Zheng W, 'Assessing China's Cybersecurity Law' 2018 34 *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2018.08.007

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence [2024] OJ L1689/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

Renda A, Beyond the Brussels Effect: Leveraging Digital Regulation for Strategic Autonomy (*Foundation for European Progressive Studies*, 2022). https://feps-europe.eu/publication/853-leveraging-digital-regulation-for-strategic-autonomy/

Sayre MA, 'The Right to Privacy and the Japanese Constitution' (2024) 2 *Student Journal of Information Privacy Law*. https://digitalcommons.mainelaw.maine.edu/sjipl/vol2/iss1/3

Scaffidi Runchella L, 'Il GDPR e la tutela del titolare dei dati personali fra public e private enforcement nelle ipotesi di trattamento transfrontaliero' (2023) 11 *Cuadernos de Derecho Transnacional*. https://doi.org/10.20318/cdt.2023.8083

Shaffer G, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards' (2000) 25 *Yale Journal of International Law* L 1.

https://openyls.law.yale.edu/bitstream/handle/20.500.13051/6405/06_25YaleJIntlL1_2000_.pdf?sequence=2

Shahmar M, 'Ethical Implications of AI in Data Collection: Balancing Innovation with Privacy' (2025). https://doi.org/10.36719/2706-6185/38/40-55

Shahmar Mirishli, 'Ethical Implications of AI in Data Collection: Balancing Innovation with Privacy' *(arXiv*, 17 2025). https://doi.org/10.48550/arXiv.2503.14539

Sirojov S, *Data Privacy Challenges in Artificial Intelligence Overview* (2025). https://www.researchgate.net/publication/389088825

Solove DJ and Schwartz PM , 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 *New York University Law Review* 1814. https://www.law.berkeley.edu/files/bclt_Schwartz-Solove_NYU_Final_Print.pdf

Stix C, 'The ghost of AI governance past, present and future: AI governance in the European Union' (*Eindhoven University of Technology*, *pre-print*, 2021). https://doi.org/10.48550/arXiv.2107.14099

Stradella E, 'Le fonti nel diritto comparato: analisi di scenari extraeuropei (Stati Uniti e Cina)' (2022) 51(1) *DPCE Online.* https://doi.org/10.57660/dpceonline.2022.1569

Sugihara N, 'Japan Makes Amendments to Their Act on the Protection of Personal Information: Establishing an Obligation to Report Data Breaches to the PPC' (*Talking Tech*, 2020).

https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2020/06/amendments-to-the-protection-of-personal-information-act-of-japa.html.

Surace M, 'Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà'(2005) *ADIR - L'altro diritto*. https://www.adir.unifi.it/rivista/2005/surace/cap2.htm.

Takase K et al, 'Japan: Personal Data Protection Commission – Announces Interim Report of Triennial Review' *(Baker McKenzie InsightPlus,* 2024). https://insightplus.bakermckenzie.com/bm/data-technology/japan-personal-data-protection-commission-announces-interim-report-of-triennial-review_1

Tallberg J et al, 'The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research' (2023) 25 *International Studies Review*. https://doi.org/10.1093/isr/viad040

Tamim J, The Brussels Effect and the GDPR: EU Institutions as Catalysts for Global Data Protection Norms (*European Digital Policy Initiative,* 2024). 10.13140/RG.2.2.28132.59529

Treaty on European Union (Consolidated Version) [1997] OJ C340/145. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:11997M/TXT

Treaty on European Union (Consolidated Version) [2012] *OJ C326/13.* https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

Treaty on the Functioning of the European Union [2012] OJ C326/47. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT

TrustArc, ‘China PIPL Whitepaper’ (2021).

https://info.trustarc.com/rs/846-LLZ-652/images/China%20PIPL%20Whitepaper%20%282%29.pdf

U.S. Department of Veterans Affairs, Fair Information Practice Principles (FIPPs) Factsheet (2023).

https://department.va.gov/privacy/wp-content/uploads/sites/5/2023/01/VA-Privacy-Factsheet-FIPPS-v2.pdf

UNESCO, Recommendation on the Ethics of Artificial Intelligence (SHS/BIO/PI/2021/1, 2022).

https://unesdoc.unesco.org/ark:/48223/pf0000380455

United Nations Economic and Social Council, Commission on Human Rights, Sub-Commission on Prevention of Discrimination and Protection of Minorities, 21 July 1988.

https://digitallibrary.un.org/record/465986.

United Nations General Assembly, The Right to Privacy in the Digital Age, Resolution A/RES/68/167. (2013).

https://digitallibrary.un.org/record/764407

United Nations General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*. (1990).

https://www.refworld.org/policy/legalguidance/unga/1990/en/13761

United Nations General Assembly. Resolution A/78/L.49: Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (2024).

https://docs.un.org/en/A/78/L.49.

United Nations Human Rights Council, Report of the Special Rapporteur on the right to privacy. A/HRC/37/62 (2018).

https://documents.un.org/doc/undoc/gen/g18/324/47/pdf/g1832447.pdf

United Nations System Chief Executives Board for Coordination, Summary of deliberations: United Nations system white paper on artificial intelligence governance, UN Doc CEB/2024/1/Add.1 (2024).

https://unsceb.org/sites/default/files/2024-11/UNSystemWhitePaperAIGovernance.pdf

United Nations, Guidelines for the Regulation of Computerized Personal Data Files: Final Report Submitted by Mr. Louis Joinet, Special Rapporteur (1988).

https://digitallibrary.un.org/record/43365?v=pdf

Voss G and Houser G, 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies' (2019) *American Business Law Journal.*

Wang F, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) 33(2) *Harvard Journal of Law & Technology.*

https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf?utm_source

Zou M and Zhang L, 'Navigating China's regulatory approach to generative artificial intelligence and large language models' (2025) 1 *Cambridge Forum on AI: Law and Governance e8.*

https://doi.org/10.1017/cfl.2024.4

'The Hiroshima AI Process: Leading the Global Challenge to Shape Inclusive Governance for Generative AI' (JapanGov – The Government of Japan, 2024).

https://www.japan.go.jp/kizuna/2024/02/hiroshima_ai_process.html?utm

‘Un confronto comparato tra la regolamentazione dell’IA negli Stati Uniti ed in Europa’ (2025) *Rivista Diritto di Internet* 1.

https://dirittodiinternet.it/wp-content/uploads/2025/01/Un-confronto-comparato-tra-la-regolamentazione-IA-UE-e-USA.pdf