Data Protection Public Policies: An Analysis of the Court of Justice of the European Union's Decisions and Their Possible Implications for Brazil

Políticas públicas de protección de datos: un análisis de las decisiones del Tribunal de Justicia de la Unión Europea y sus posibles repercusiones en Brasil

Júlia Oselame Graf
Universidade de Santa Cruz do Sul • Santa Cruz do Sul - Brasil
https://orcid.org/0000-0002-2662-6963 • juliagrafadv@gmail.com

Caroline Müller Bitencourt
Universidade de Santa Cruz do Sul • Santa Cruz do Sul - Brasil
https://orcid.org/0000-0001-5911-8001 • carolinemb@unisc.br

Revista de Derecho de la UCB – UCB Law Review, Vol. 9 Nº 17, octubre 2025, pp. 61-87
ISSN 2523-1510 (en línea), ISSN 2521-8808 (impresa).
DOI: https://doi.org/10.35319/lawreview.202517105
Recibido: 30 de septiembre de 2024 • Aceptado: 22 de septiembre de 2025

Abstract

This article investigates the extent to which the case law of the Court of Justice of the European Union (CJEU) can serve as an interpretive parameter for the application of Brazil's General Data Protection Law (LGPD). A hypothetical-deductive method, in a comparative perspective, is adopted to analyze fourteen landmark CJEU judgments selected for their relevance in consolidating the principles of the General Data Protection Regulation (GDPR). The analysis demonstrates how the foundations established by the CJEU interact with the normative structure of the LGPD in key areas of data protection, allowing the identification of significant

convergences. The results show that these points of contact provide useful references for the actions of the Brazilian National Data Protection Authority, both in issuing regulations and in supervising and encouraging best practices, thereby strengthening public policies aimed at data protection in Brazil, without implying an automatic transposition of European jurisprudence.

Keywords: LGPD, data protection, public policies, GDPR, CJEU.

Resumen

Este artículo investiga en qué medida la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) puede servir como parámetro interpretativo para la aplicación de la Ley General de Protección de Datos (LGPD) en Brasil. Se adopta el método hipotético-deductivo, en perspectiva comparada, para analizar catorce sentencias paradigmáticas del TJUE, seleccionadas por su relevancia en la consolidación de los principios del Reglamento General de Protección de Datos (GDPR). El análisis evidencia cómo los fundamentos consolidados por el TJUE dialogan con la estructura normativa de la LGPD en temas centrales de la protección de datos, lo que permite identificar convergencias significativas. Los resultados muestran que estos puntos de contacto proporcionan referencias útiles para la actuación de la Autoridad Nacional de Protección de Datos de Brasil, tanto en la elaboración de reglamentos como en la fiscalización y el fomento de buenas prácticas, fortaleciendo las políticas públicas orientadas a la protección de datos en Brasil, sin que ello suponga una trasposición automática de la jurisprudencia europea.

Palabras clave: LGPD, protección de datos, políticas públicas, GDPR, TJUE.

1. Introduction

Brazil's General Data Protection Law (LGPD), Law No. 13,709/2018, was inspired by the European Union's General Data Protection Regulation (GDPR). Coming into effect in September 2020, the LGPD incorporated several principles and guidelines aimed at ensuring the protection of citizens' personal data, following the European model, which is considered a global benchmark in this field.

The development of European Community law, from its origins in the founding treaties of the European Union to its interpretation and application by the Court of Justice of the European Union (CJEU), is a key milestone not only in the legal sphere but also in the construction of a cohesive and integrated supranational order. This context justifies the analysis, in this article, of recent CJEU decisions and the potential impacts these decisions may have on the interpretation and application of the LGPD in Brazil.

In this context, the research problem to be addressed is: "How can decisions of the Court of Justice of the European Union on data protection impact the implementation of the LGPD in Brazil, considering institutional and cultural challenges to meeting international privacy and data security standards?"

Accordingly, the objective is to analyze the recent decisions of the Court of Justice of the European Union (CJEU) and their potential influence on the interpretation and application of Brazil's General Data Protection Law (LGPD), taking into account the latter's inspiration from the European legislation, the General Data Protection Regulation (GDPR), and its impact on the alignment of national practices with international privacy and data security standards.

Although CJEU decisions are not binding in the Brazilian legal system, they exert considerable influence on the debate surrounding data protection in the country. The CJEU's approach to the GDPR offers a reference for the implementation and interpretation of the LGPD, guiding Brazilian authorities, companies, and legal professionals in adopting best practices and harmonizing data protection standards with international norms.

2. Methodology

This study adopts the hypothetical-deductive method, which will allow the testing of hypotheses through the analysis of concrete evidence and data. The guiding hypotheses are: (i) CJEU decisions have a direct impact on the interpretation of the LGPD, contributing to the alignment of national practices with international data protection standards; (ii) the implementation of the LGPD in Brazil faces institutional and cultural challenges, such as a lack of training and resistance to change; and (iii) the adoption of CJEU guidelines could strengthen data protection in Brazil, provided it is accompanied by continuous efforts to strengthen institutions and raise public awareness.

At the normative level, the study examines the legal instruments that structure data protection in both contexts: the General Data Protection Regulation (GDPR), the Brazilian General Data Protection Law (LGPD), Constitutional Amendment No. 115/2022, and the decrees that established and organized the Brazilian National Data Protection Authority (ANPD). At the jurisprudential level, the focus is the case law of the Court of Justice of the European Union (CJEU), based on the selection of landmark decisions capable of consolidating fundamental GDPR principles and establishing thematic dialogue with provisions of the LGPD.

To this end, a jurisprudential framework was defined, consisting of fourteen CJEU judgments distributed into two groups: (i) structural foundations of Union law (Van Gend en Loos, Costa v. ENEL, Politi, Van Duyn), essential for understanding the autonomy and effectiveness of European law; and (ii) construction and contemporary challenges of data protection (Lindqvist, Scarlet Extended, Digital Rights Ireland, Google Spain, Breyer, Wirtschaftsakademie, Fashion ID, Google v. CNIL, Schrems II, La Quadrature du Net, and OQ/SCHUFA). The selection followed criteria of normative relevance, prioritizing decisions capable of creating or consolidating principles applicable to the GDPR and, consequently, comparable to the provisions of the LGPD.

Judgments were retrieved from CURIA and EUR-Lex via systematic searches (keywords: data protection, GDPR, right to be forgotten, automated decision, and data transfer). Each decision was analyzed in full and indexed with identification of the case summary, legal reasoning, and dispositive elements. Subsequently, an analytical categorization was carried out in three dimensions: (i) the GDPR principle or provision interpreted in each decision; (ii) thematic correspondence with articles of the LGPD; and (iii) interpretive relevance for public policies aimed at data protection in Brazil.

In this way, the methodological design goes beyond the mere juxtaposition of legal texts. The comparison of principles, legal foundations, and practical consequences of European decisions makes it possible to understand the interpretive relevance for the LGPD and for public policies focused on data protection in Brazil, while taking into account the specificities of the Brazilian legal system and context.

3. Development

3.1. Data Protection Public Policies in Brazil: Advances and Challenges in the Digital Era

The protection of personal data has emerged as one of the main issues of the digital era, fueled by the exponential increase in the collection and use of sensitive data across all spheres of society. In Brazil, the enactment of the General Data Protection Law (LGPD) ushered in a new era of public policies aimed at ensuring the privacy and protection of citizens' personal data, in line with international regulations such as the European Union's General Data Protection Regulation (GDPR). However, the effectiveness of these policies still faces significant obstacles, requiring continuous efforts to ensure that data protection is genuinely guaranteed.

The rise of the digital society represents not merely a technological advance but a profound reconfiguration of the private sphere and

of the very conception of data protection. It is therefore relevant to recall that the internet itself was born under the sign of an almost unlimited freedom, presented as a space capable of overcoming political borders and ensuring privacy through anonymity and the difficulty of tracking. Castells highlights that "interactive computer networks are growing exponentially, creating new forms and channels of communication, shaping life and, at the same time, being shaped by it" (2002, p. 40), demonstrating that technical evolution and social organization mutually influence each other.

In this context of transformation, Jan van Dijk explores the concepts of the "information society" and the "network society" to describe the changes brought about by the increasing intensity of information processing across all spheres of social, economic, and political life. The author observes that the information society is characterized by the intensification of data production and processing in all domains of human activity, so that the economy, the labor market, and culture become increasingly dominated by information and processes that demand a high level of knowledge and education, affirming that "the intensity of information processing in all these spheres allows us to describe it as a new type of society" (Van Dijk, 2006, p. 19).

As Danilo Doneda (2020) notes, privacy, once understood as a simple "right to be let alone", shifts to a field in which the central element is the capacity to manage and control flows of personal information in highly complex digital environments. Tércio Sampaio Ferraz Júnior had already anticipated this change by asserting that the inviolability of data secrecy (Article 5, XII, of the Constitution) is inseparable from the fundamental right to privacy (Article 5, X), recognizing the individual's power to exclude from third-party knowledge whatever pertains to them and reveals their most intimate identity (Ferraz Júnior, 1993, p. 440).

Within this framework, part of the legal doctrine argues that the protection of personal data constitutes an autonomous fundamental right, even while maintaining a permanent dialogue with privacy. Lynskey (2015, p. 90) identifies three possible readings of

this relationship: (i.) separate but complementary rights; (ii.) data protection as a subset of privacy; and (iii.) data protection as an independent right designed to perform functions that go beyond the safeguarding of private life. This third perspective has gained strength due to the proliferation of secondary uses of data profiling, automated decision-making, mass surveillance — that are not limited to the risk of intrusion into intimacy.

Stefano Rodotà deepens the analysis by proposing the so-called "third paradox of privacy," which highlights four movements: from the right to be left alone to the right to control the information that concerns me; from privacy to informational self-determination; from privacy to non-discrimination; and from secrecy to control (2008, pp. 97-98). In an earlier work, the author had already warned that the classification of certain elements as "sensitive data" stems precisely from their potential for discriminatory use, requiring stricter circulation rules and prohibiting certain forms of collection and processing (Rodotà, 2008, p. 96).

Moreover, Caitlin Mulholland (2018, p. 172) finding that contemporary privacy encompasses situations in which the data subject protects and controls sensitive data shifts the classic "right to privacy" toward a logic of self-determination. Ingo Sarlet (2021, p. 80) adds that data protection must be understood as a fundamental right with a multilevel dimension, capable of ensuring not only the confidentiality of information but also the integrity of information systems and the autonomy of individuals in the face of state and private practices of large-scale data collection and processing. This complexity challenges the capacity of national and international legal orders to provide effective and timely responses (Sarlet, 2021, p. 57).

The tension between technological innovation and legal protection becomes even more evident when considering the advance of emerging technologies. Aurelia Tamò-Larrieux (2018, p. xxiii) analyzes the growing conflict between the ubiquity of connected devices and the need for safeguards for personal data, highlighting that the speed of technological evolution, especially in the context of the

Internet of Things (IoT), reduces social understanding of the complexity of collection and processing operations. The expansion of processing capacity and the development of predictive algorithms enable digital environments capable of acting autonomously on the basis of data correlations (Tamò-Larrieux, 2018, p. 2).

The entry into force of the LGPD was a milestone in raising awareness about the importance of personal data protection in Brazil (Brazil, 2018). The relevance of this issue was further emphasized with the approval of Constitutional Amendment No. 115/2022 (Brazil, 2022), which elevated data protection to the status of a fundamental right, ensuring its inclusion among the rights and guarantees enshrined in the Federal Constitution (Brazil, 2022). Additionally, Law No. 14,129/2021, which addresses Digital Government, introduced important innovations for public efficiency, particularly with respect to data interoperability and privacy protection (Brazil, 2021).

One of the public policies implemented in Brazil was the creation of the National Data Protection Authority (ANPD), a central body responsible for enforcing and overseeing the LGPD. The ANPD's role is to regulate, guide, and sanction violations of data protection, which is essential to ensuring compliance with the law. However, for this public policy to be effective, the government must continue investing in strengthening the ANPD institutionally, ensuring its autonomy and efficiency in its operations.

> The National Data Protection Authority was established by Provisional Measure No. 869 of December 27, 2018, later converted into Law No. 13,853 of July 8, 2019, which amended Law No. 13,709 of August 14, 2018, the General Data Protection Law (LGPD), and became operational with the appointment of its first Director-President by the Decree of November 5, 2020. In 2022, a new milestone was reached: Provisional Measure No. 1,124 of June 13, 2022, converted into Law No. 14,460 of October 25, 2022, amended Law No. 13,709 of August 14, 2018, and transformed the Authority into a special nature autonomous entity. On January 23,

> 2023, Decree No. 11,401 was published, linking the ANPD to the Ministry of Justice and Public Security. The ANPD's organizational structure and staffing were defined and approved by Decree No. 10,474 of August 26, 2020, amended by Decree No. 10,975 of February 22, 2022, then by Decree No. 11,202 of September 21, 2022, and recently by Decree No. 11,758 of October 30, 2023. It is important to emphasize that the ANPD has technical and decision-making autonomy, with its own assets, and serves as the central authority for interpreting the General Data Protection Law (LGPD), responsible for safeguarding personal data protection, guiding, regulating, and overseeing compliance with the legislation (Brazil, 2024).

Another significant public policy is the National Information Security Policy, established by Decree No. 9,637/2018, which provides guidelines for safeguarding information security in public agencies, including the handling of personal data. This policy is crucial in ensuring that the government adopts best practices in information management, protecting citizens' data from leaks and misuse. However, the implementation of this policy varies significantly across different levels of government, with many agencies still facing challenges in adapting their information systems to meet the security requirements mandated by the legislation (Brazil, 2018).

The Privacy Governance Program, adopted by both public and private institutions, represents progress in promoting a culture of privacy in Brazil. This program aims to establish internal mechanisms that ensure compliance with the LGPD, such as the adoption of technical and organizational measures for data protection. Nevertheless, one of the greatest challenges in implementing this public policy is the lack of knowledge and training among both managers and data operators. Cultural resistance in many sectors, coupled with insufficient training, hinders the full integration of LGPD standards into institutional practices.

Additionally, Decree No. 10,222/2020, which regulates the National Cybersecurity Strategy, underscores the need for a coordinated

approach between government, industry, academia, and society to protect cyberspace, focusing on information security - including data protection, cybersecurity, and cyber defense (Brazil, 2020).

Furthermore, it is necessary to highlight the Open Data Policy, provided for by Decree No. 8,777/2016, which, although aimed at public transparency, must coexist with personal data protection regulations. This policy promotes the release of government data to foster transparency and innovation, but it must be implemented with caution to avoid the undue exposure of personal data. Balancing these two directives - transparency and data protection - still requires careful consideration to avoid compromising citizens' privacy (Brazil, 2016).

Thus, Brazilian public policies on data protection represent a significant advance in ensuring the rights to privacy and data protection in an increasingly digital environment. However, their effectiveness depends on continuous efforts to strengthen institutions, train those involved, fully comply with the LGPD, and invest in technological infrastructure.

3.2. Historical Perspective on the Primacy of European Law and the Influence of the General Data Protection Regulation (GDPR) on the General Data Protection Law (LGPD)

European Union law takes precedence over national law, meaning that, although not hierarchically superior, its application takes priority. Thus, the principle of primacy dictates that European law prevails over the national law of Member States, applying to all binding European acts and preventing Member States from contravening EU rules.

According to Agustín Ureta, the principle of primacy serves to resolve conflicts between legal systems, ensuring that one takes precedence over the other in specific cases. Unlike hierarchical relationships within a specific legal system, this involves a matter of normative precedence. Initially valid in themselves, rules or acts

that conflict cannot be applied simultaneously in concrete cases (Ureta, 2021, p. 151).

The Court of Justice of the European Union (CJEU) established the principle of primacy in the 1964 Costa v. ENEL case. In this ruling, the Court affirmed that law emanating from European institutions integrates into the legal systems of Member States, obligating them to respect it. Therefore, if a national rule conflicts with a European provision, Member State authorities must apply the European provision. National law is not annulled or amended, but its binding force is suspended. The Court later specified that the primacy of European law applies to all national acts, regardless of whether they were adopted before or after the European act in question.

> As a result, Union law, created by virtue of powers conferred by treaties, takes precedence over any and all conflicting national legal norms. It prevails not only over prior national legislation but also over subsequent legislative acts. In short, when the Court delivered the Costa v. Enel judgment, it did not challenge the nationalization of the electricity sector in Italy but unequivocally established the primacy of Union law over national law. The legal consequence of this principle of primacy is that, in case of a conflict between laws, the national provision contrary to the European Union provision ceases to be applicable, and no new internal provisions contrary to Union legislation can be introduced (Borchardt, 2011, p. 133).

The primacy of European law over national law is absolute, meaning that all acts benefit from this primacy. No state can argue that its national constitution contradicts community law, as such an argument has no legal effect. Non-compliance with this principle implies liability for its breach. In addition to the aforementioned cases, other notable cases related to the principle of primacy include Simmenthal (1978), Factortame (1990), Elchinov (2010), and Aklagaren vs Hans Fransson (2013).

The principle of direct effect allows individuals to invoke European Union law before national or European courts, a principle

established by the CJEU in the 1963 Van Gend en Loos case. It is worth highlighting a passage from this judgment to clarify that EU law imposes obligations not only on Member States but also on individuals:

> Indeed, the fact that the mentioned articles of the Treaty allow the Commission and Member States to bring an action against a state that has failed to fulfill its obligations does not deprive individuals of the possibility, where appropriate, to invoke those obligations before national courts; similarly, the fact that the Treaty provides the Commission with means to ensure compliance with the obligations imposed on subjects does not preclude individuals from invoking the breach of those obligations in disputes between individuals before a national court (CJEU, 1963).

Article 288 of the Treaty on the Functioning of the European Union (TFEU) establishes that regulations are directly applicable in EU countries, meaning they always have direct effect. The Politi ruling (1971) illustrates the Court of Justice's position regarding the full direct effect of regulations. Directives, on the other hand, are acts addressed to EU countries for transposition into national law. However, the Court of Justice, in some cases, grants direct effect to protect individuals' rights. Case law emphasizes the need for unconditional, clear, and precise provisions.

Moreover, it is important to note that the Treaty on the Functioning of the European Union (TFEU) represents a political, legal, and social project. The distinctive feature of the European Union, compared to other communities, is the guarantee of rights provided by the CJEU. These treaties not only shaped the European Union in its current form but also reflect the Member States' ongoing commitment to European integration, promoting peace, stability, and prosperity.

The implementation of public data protection policies in Brazil, particularly with the General Data Protection Law (LGPD), did not occur in isolation. There was a strong influence from international frameworks, particularly the European Union's General Data Pro-

tection Regulation (GDPR), and the decisions of the Court of Justice of the European Union (CJEU). The CJEU, through its interpretations of the GDPR in landmark cases, has shaped the global understanding of privacy and data security, and its decisions are increasingly reflected in the public policies of countries outside the EU, including Brazil.

The GDPR, implemented in 2018, consolidated the European Union as a global model for data protection. Its guidelines and requirements were designed to ensure that companies and governments handle personal data in a transparent, secure, and respectful manner.

However, beyond legislative provisions, CJEU decisions are critical for refining and applying the GDPR, setting specific standards on complex issues such as international data transfers, the right to be forgotten, and data retention. These decisions directly shape public data protection policies across the European Union, and as Brazil seeks alignment with the GDPR through its own legislation, it absorbs part of this influence through the LGPD.

3.3. Data Protection Overseas: Landmark Cases of the Court of Justice of the European Union and Possible Impacts in Brazil

Public policies for the protection of personal data have become an increasing necessity in a world that is ever more digitalized. The advancement of technology has raised concerns about individual privacy, forcing states to develop legislation that ensures the security of personal data.

The LGPD was largely motivated by the need to align with international standards, facilitating the exchange of information and cooperation between Brazil and other countries, particularly European nations. Brazilian public policies on data protection thus reflect an attempt to conform to global standards, ensuring legal security for companies and citizens in an increasingly interconnected environment.

The European Union, through the General Data Protection Regulation (GDPR), has emphasized the need for strict rules for data protection. The decisions of the Court of Justice of the European Union (CJEU), in particular, have had a significant influence on the formulation of public policies in other countries, including Brazil. In this context, the General Data Protection Law (LGPD) directly reflects these influences, demonstrating how foreign legislation can shape the Brazilian legal and administrative landscape.

In the context of data protection, the General Data Protection Regulation, in effect since May 25, 2018, repealed Directive 95/46 and sought to standardize and avoid contradictions among EU Member States. In Portugal, Law No. 58/2019, implemented in August 2019, ensures the enforcement of the GDPR and defines the sanctions regime applicable to organizations that fail to comply with its provisions. Furthermore, Law No. 59/2019 transposed Directive (EU) 2016/680, establishing specific rules for data processing in the context of crime prevention and repression.

Other complementary legislation, such as Law No. 34/2009, which regulates data processing within the judicial system in Portugal, and Resolution of the Council of Ministers No. 41/2018, which establishes technical guidelines for the Public Administration regarding network security, reinforce compliance with the GDPR. The uniformity of these regulations is crucial for ensuring the protection of privacy rights across the European Union.

The CJEU plays a vital role in interpreting these laws, ensuring the uniform application of personal data protection rules. Even before the GDPR came into force, important court decisions had already set significant precedents. Cases such as “Google Spain” (C-131/12) and “Schrems II” (C-311/18) have helped shape the application of data protection regulations, even beyond the borders of the EU. The table below contains the key judgments of the Court of Justice of the European Union on data protection.

Table 1: Key Judgments of the Court of Justice of the European Union on Data Protection

JUDGMENT	DATE	OBSERVATIONS
Lindqvist (C-101/01)	06/11/2003	The first CJEU judgment to apply Directive 95/46 to the processing of data on the Internet.
Scarlet Extended (C-70/10)	24/11/2011	Established that internet service providers cannot be required to install general traffic-filtering systems to prevent copyright infringements, reinforcing the principle of proportionality between data protection and intellectual property rights.
Digital Rights Ireland (C-293/12 e C-594/12)	08/04/2014	Declared the entire Directive 2006/24/EC on the retention of communication data invalid for violating the fundamental rights to privacy and data protection, with retroactive effect (ex tunc).
Google Spain (C-131/12)	13/05/2014	Recognized the "right to be forgotten" in the European Union, requiring search engines to comply with requests for the de-indexing of links that are inadequate, irrelevant, or excessive, even when the information remains available at the original source.
Breyer (C-582/14)	19/10/2016	Held that dynamic IP addresses can constitute personal data when the data controller has legal means to identify the user, expanding the notion of identifiable data.
Wirtschaftsakademie Schleswig-Holstein (C-210/16)	05/06/2018	Recognized the existence of joint responsibility between a Facebook fan page administrator and the platform itself when both determine the purposes and means of processing visitor data.
Fashion ID (C-40/17)	29/07/2019	Reaffirmed joint responsibility between a website operator and the provider of social plug-ins (Facebook "like" button), requiring a legal basis for the collection and transmission of user data.

JUDGMENT	DATE	OBSERVATIONS
Google v. CNIL (C-507/17)	24/09/2019	Defined the territorial scope of the right to be forgotten: de-indexing orders must produce effects in all EU Member States but not necessarily on a global scale.
Schrems II (C-311/18)	16/07/2020	Invalidated the Privacy Shield agreement for EU-U.S. data transfers due to insufficient safeguards against U.S. government surveillance; reaffirmed the requirement of supplementary measures for international transfers.
La Quadrature du Net (C-511/18, C-512/18 e C-520/18)	06/10/2020	Rejected generalized and indiscriminate retention of traffic and location data, allowing only targeted retention proportionate to serious threats to national security.
SCHUFA / OQ v Land Hessen (C-634/21)	07/12/2023	Interpreted Article 22 of the GDPR, concluding that the generation and use of credit scoring by third parties may constitute a decision based solely on automated processing, requiring transparency, information to the data subject, and the possibility of human review.

Source: Prepared by the authors based on the repository of the CJEU.

In recent years, data protection has become a central issue in the European Union. The implementation of the GDPR represented a significant advancement, establishing strict rules for the processing of personal data and guaranteeing rights for European citizens. In this context, it is worth noting that European Union law constitutes a distinct legal order, as established in the "Van Gend en Loos" case of 1963, creating a new legal order for Member States. This jurisprudence is not rigid but constantly evolves through court decisions, which define guiding principles (CJEU, 1963).

Article 16 of the Treaty on the Functioning of the European Union (TFEU) establishes that "everyone has the right to the protection of personal data concerning them." In this regard, the CJEU has played an important role in interpreting and applying these norms, as seen in the case of Google Spain SL vs. Agencia Española de Protección de Datos. In this case, the court established the "right to be

forgotten," an important protection for individuals to control their information online. Mario Costeja González requested that Google remove links to a newspaper article mentioning an auction of his property due to debts (CJEU, 2014).

Moreover, the CJEU ruled that search engines are responsible for processing personal data and must comply with requests to remove links that are inadequate, irrelevant, or excessive. This decision reinforced individuals' right to control their personal information available online, promoting privacy and data protection in the digital age.

In 2020, the CJEU ruled on another important case involving the widespread and indiscriminate retention of traffic and location data by electronic communication service providers for national security purposes. In the Privacy International and La Quadrature du Net cases, the court held that such practices are incompatible with EU law, which protects personal data privacy. The court emphasized that while national security is a legitimate objective, data retention must be strictly proportional to the intended goal and cannot be applied indiscriminately, thus balancing national security with the protection of citizens' fundamental rights (CJEU, 2020).

The Schrems II case, also from 2020, had a significant impact on international data transfers. Maximilian Schrems, a privacy activist, challenged the "Privacy Shield," an agreement that allowed the transfer of personal data between the EU and the US. The CJEU concluded that the agreement did not provide sufficient protection against US authorities' surveillance of the data, violating the privacy rights of EU citizens. This decision required companies and authorities to revise their transfer mechanisms to ensure compliance with EU data protection standards (CJEU, 2020).

Another notable case is the Digital Rights Ireland case, decided in 2014, where the CJEU invalidated the EU Data Retention Directive. This directive required Member States to ensure the retention of telecommunications data for at least six months for crime-fighting purposes. The court found that the directive disproportionately

interfered with fundamental rights to privacy and personal data protection. The decision reinforced the principle that any data retention measure must be necessary and proportionate, protecting citizens' rights against excessive interventions (CJEU, 2014).

The CJEU's decisions in cases related to data protection illustrate the complexity and importance of ensuring that legislation keeps pace with technological and societal changes. These judgments not only reaffirm the EU's commitment to protecting fundamental rights but also serve as a global reference in the formulation of privacy and data security policies. It is thus evident that balancing security, innovation, and privacy remains a constant challenge.

In the cases Wirtschaftsakademie (C-210/16) and Fashion ID (C-40/17), the Court of Justice of the European Union (CJEU) held that different actors may be considered joint controllers when they co-determine the purposes and means of processing. This interpretation strengthens shared accountability between platforms and page or social plug-in administrators, providing parameters for applying the concepts of controller and processor set forth in the LGPD, particularly within platform-based economic environments.

Turning to Google v. CNIL (C-507/17), the Court addressed the territorial scope of the right to erasure, concluding that de-indexing orders issued by European authorities need not have global reach but must be effective across all Member States of the Union. For Brazil, this precedent sheds light on the debate over the enforcement of data removal orders in cross-border scenarios, especially in view of the growing international circulation of information.

With regard to Breyer (C-582/14), the CJEU recognized that dynamic IP addresses can constitute personal data whenever the identification of the data subject is possible through additional information. This decision holds particular significance for cybersecurity policies and for interpreting the concept of personal data under the LGPD, which likewise adopts the notion of contextual identifiability.

More recently, in case C-634/21, OQ v. Land Hessen, with the intervention of SCHUFA Holding AG, the CJEU examined the compatibility of credit scoring with Article 22 of the GDPR, which prohibits decisions based solely on automated processing when such decisions produce legal effects or similarly significant impacts on the data subject. The dispute concerned the practice of SCHUFA, a private company that calculates credit scores used by financial institutions and other entities to assess the solvency of individuals. The central issue was whether the generation and use of a credit score, when decisive for the conclusion or refusal of contracts, constitutes an automated decision subject to the safeguards provided in the European regulation.

Moreover, the Court concluded that when the score is decisive for contractual purposes, its generation and use by third parties may amount to an automated decision, thereby imposing enhanced obligations of information, transparency, and the possibility of human review on the controller. The judgment emphasized that the assessment depends not only on the absence of human intervention in the calculation but also on the practical relevance of the result for the data subject's legal sphere, so that a mere claim of statistical purpose is insufficient to exclude the applicability of Article 22.

To make the correspondence between European case law, the principles of the General Data Protection Regulation (GDPR), and the provisions of the Brazilian General Data Protection Law (LGPD) more visible, a comparative matrix is presented below. Table 2 synthesizes, from a normative dialogue perspective, the main judgments analyzed, highlighting which LGPD articles align with the grounds emphasized by the CJEU and which potential public-policy implications may be drawn for the Brazilian context.

Table 2: Comparative Jurisprudential Mapping

CJEU CASE	GDPR PRINCIPLE (S)	THEMATIC CORRESPONDENCE IN LGPD	INTERPRETIVE RELEVANCE FOR PUBLIC POLICIES IN BRAZIL
Lindqvist (C-101/01)	Lawfulness, fairness and transparency; purpose limitation	Arts. 5, 6, and 7	Guidelines from the ANPD on publications in digital environments and the need for consent or another appropriate legal basis.
Scarlet Extended (C-70/10)	Proportionality; data minimization; integrity and confidentiality	Arts. 6, 46, and 50	Parameters to avoid indiscriminate monitoring obligations in cybersecurity policies.
Digital Rights Ireland (C-293/12 e C-594/12)	Purpose limitation; data minimization; proportionality; necessity	Arts. 6, 37, and 46-50	Guidelines for targeted retention of communication data and the need for impact assessments.
Google Spain (C-131/12)	Accuracy; storage limitation; lawfulness and transparency	Arts. 18 and 16	Criteria for requests to delete or de-index personal data before search engines and public authorities.
Breyer (C-582/14)	Identifiability; lawfulness; data minimization	Art. 5 (I) and(V)	Clarification of the notion of personal data in access records and government portal logs.
Wirtschaftsakademie Schleswig-Holstein (C-210/16)	Accountability; transparency	Arts. 5 (VI) and (VII), and 42	Reinforcement of joint controllership between platforms and administrators of institutional pages.

CJEU CASE	GDPR PRINCIPLE (S)	THEMATIC CORRESPONDENCE IN LGPD	INTERPRETIVE RELEVANCE FOR PUBLIC POLICIES IN BRAZIL
Fashion ID (C-40/17)	Accountability; transparency; lawfulness	Arts. 7, 9 and 42	Need for information and a valid legal basis for data collection by widgets or third-party tools.
Google v. CNIL (C-507/17)	Storage limitation; accuracy; transparency	Arts. 18 e 33-36	Criteria for complying with data removal orders in cross-border scenarios.
Schrems II (C-311/18)	Integrity and confidentiality; accountability; adequacy of safeguards for international transfers	Arts. 33-36	Guidance on standard contractual clauses and additional measures for Brazil–EU data transfers.
La Quadrature du Net (C-511/18, C-512/18 e C-520/18)	Proportionality; data minimization; integrity and confidentiality	Arts. 6 and 46-50	Parameters for data retention requests by security agencies and the need for proportionality control.
SCHUFA / OQ v Land Hessen (C-634/21)	Lawfulness, fairness and transparency; human intervention/ informational self-determination; accountability	Art. 20	Requirement of transparency, information to the data subject, and the possibility of human review in credit scoring systems.

Source: Prepared by the authors based on the repository of the CJEU.

In this way, the jurisprudential evolution of the CJEU demonstrates that data protection in the European Union is the result of a continuous interpretive process aimed at keeping pace with technological and social transformations. The decisions that define data retention, international transfers, automated decision-

making, and the territorial scope of the right to be forgotten consolidate a normative model that articulates individual guarantees, transparency requirements, and the functioning of economic and administrative activities. For Brazil, which is advancing in the implementation of the LGPD, these precedents provide interpretive benchmarks for the LGPD and for public policies focused on data protection, adapted to the specific characteristics of the Brazilian legal system and context.

4. Conclusion

The European Union has established a sophisticated and interconnected legal system that ensures the effective and uniform application of its laws among Member States, with the principle of the primacy of EU law playing a central role in the harmonization of standards within the bloc. This principle, enshrined by the Court of Justice of the European Union in the Costa v. Enel case, is one of the main tools to ensure that EU law prevails over national law in the event of a conflict.

Based on the analysis, CJEU decisions have a direct impact on the interpretation of the General Data Protection Law (LGPD) in Brazil. The influence of these decisions significantly contributes to aligning Brazilian practices with international data protection standards.

In Brazil, the LGPD represents a significant step forward in protecting citizens' privacy rights, but its full implementation still faces challenges. Among the main obstacles are the need to strengthen the institutional capacity of the National Data Protection Authority (ANPD), to train data managers and operators, and to build a culture of compliance with data protection standards across all sectors of the economy and public administration.

Despite the evident parallels between the General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD), it must be recognized that the case law of the Court of Jus-

tice of the European Union serves primarily as a theoretical framework and a source of inspiration, rather than as a binding mandate in the Brazilian context. Institutional differences, such as Brazil's federal structure, the regulatory competencies of the National Data Protection Authority, and the mechanisms for oversight and the application of sanctions, require a context-sensitive interpretation. Moreover, sector-specific particularities and the stage of national regulatory development call for caution so that the references to European experience are properly contextualized, ensuring that comparative analyses do not overlook the normative specificities and the broader socioeconomic context of Brazil.

Thus, although the LGPD was inspired by the GDPR, its effectiveness requires ongoing efforts to strengthen institutions and raise public awareness about the importance of data protection. Brazil still has work ahead, but the foundation is already being laid. Aligning national practices with international standards is an important step in this process, contributing to the creation of a safer and more reliable environment for personal data protection.

5. References

5.1 Doctrine

Borchardt, K.-D. (2011). *O ABC do direito europeu.* Publications Office of the European Union.

Castells, M. (2002). *A sociedade em rede.* Paz e Terra.

Doneda, D. (2020). *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. Thomson Reuters Brazil.

Ferraz Júnior, T. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito*, Universidade de São Paulo, 88, 439–459. https://www.revistas.usp.br/rfdusp/article/view/67231

Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford University Press.

Rodotà, S. (2008). *A vida na sociedade da vigilância*: a privacidade hoje. Renovar.

Sarlet, I. W. (2021). *Fundamentos constitucionais*: o direito fundamental à proteção de dados. En D. Doneda et al. (Eds.), *Tratado de proteção de dados pessoais*. Forense.

Tamò-Larrieux, A. (2018). *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things.* Springer Nature.

Ureta, A. (2021). *Princípio do primado no direito da União Europeia.* In Estudos de Direito Europeu. Editora ABC.

Van Dijk, J. (2006). *The Network Society: Social Aspects of New Media.* Sage.

5.2 Legislation

Brazil. *Decreto nº 8.777, de 11 de maio de 2016* [Decree No. 8.777 of May 11, 2016]. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8777.htm

Brazil. *Decreto nº 9.637, de 26 de dezembro de 2018* [Decree No. 9.637 of December 26, 2018]. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm

Brazil. *Decreto nº 10.222, de 5 de fevereiro de 2020* [Decree No. 10.222 of February 5, 2020]. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

Brazil. *Emenda Constitucional nº 115, de 10 de fevereiro de 2022* [Constitutional Amendment No. 115 of February 10, 2022]. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm

Brazil. *Lei nº 13.709, de 14 de agosto de 2018* [General Data Protection Law – LGPD]. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Brazil. *Lei nº 13.853, de 8 de julho de 2019* [Law No. 13.853 of July 8, 2019]. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm

Brazil. *Lei nº 14.129, de 29 de março de 2021* [Digital Government Law]. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14129.htm

Brazil. *Medida Provisória nº 869, de 27 de dezembro de 2018* [Provisional Measure No. 869 of December 27, 2018]. Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm

5.3 Electronic Sources

Brazil. Ministry of Justice and Public Security. (n.d.). *Legal basis of the organizational structure and competencies of the National Data Protection Authority.* Government of Brazil. https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/base-juridica

5.4 Jurisprudence

Court of Justice of the European Union (Second Chamber). Breyer v. Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779 (Oct. 19, 2016). https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

Court of Justice of the European Union (Judgment of the Court). Costa v. ENEL, 6/64, ECLI:EU:C:1964:66 (July 15, 1964). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61964CJ0006

Court of Justice of the European Union (Grand Chamber). Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems (Schrems II), C-311/18, ECLI:EU:C:2020:559 (July 16, 2020). https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN

Court of Justice of the European Union (Grand Chamber). Digital Rights Ireland Ltd and Seitlinger and Others, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238 (Apr. 8, 2014). https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

Court of Justice of the European Union (Second Chamber). Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, C-40/17, ECLI:EU:C:2019:629 (July 29, 2019). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0040

Court of Justice of the European Union (Grand Chamber). Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), C-507/17, ECLI:EU:C:2019:772 (Sept. 24, 2019). https://curia.europa.eu/juris/document/document.jsf?docid=218105&doclang=EN

Court of Justice of the European Union (Grand Chamber). Google Spain SL and Mario Costeja González v. Agencia Española de Protección de Datos, C-131/12, ECLI:EU:C:2014:317 (May 13, 2014). https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN

Court of Justice of the European Union (Grand Chamber). La Quadrature du Net and Others, Joined Cases C-511/18, C-512/18 & C-520/18, ECLI:EU:C:2020:791 (Oct. 6, 2020). https://curia.europa.eu/juris/document/document.jsf?docid=232084&doclang=EN

Court of Justice of the European Union (Judgment of the Court). Lindqvist, C-101/01, ECLI:EU:C:2003:596 (Nov. 6, 2003). https://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=EN

Court of Justice of the European Union (First Chamber). OQ v. Land Hessen (SCHUFA Holding AG intervening), C-634/21, ECLI:EU:C:2023:950 (Dec. 7, 2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0634

Court of Justice of the European Union (Judgment of the Court). Politi s.a.s. v. Ministry for Finance of the Italian Republic, 43/71, ECLI:EU:C:1971:122 (Dec. 14, 1971). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61971CJ0043

Court of Justice of the European Union (Third Chamber). Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs (SABAM), C-70/10, ECLI:EU:C:2011:771 (Nov. 24, 2011). https://curia.europa.eu/juris/document/document.jsf?docid=115202&doclang=EN

Court of Justice of the European Union (Judgment of the Court). Van Duyn v. Home Office, 41/74, ECLI:EU:C:1974:133 (Dec. 4, 1974). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61974CJ0041

Court of Justice of the European Union (Judgment of the Court). Van Gend en Loos v. Nederlandse Administratie der Belastingen, 26/62, ECLI:EU:C:1963:1 (Feb. 5, 1963). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61962CJ0026

Court of Justice of the European Union (Grand Chamber). Wirtschaftsakademie Schleswig-Holstein v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, C-210/16, ECLI:EU:C:2018:388 (June 5, 2018). https://curia.europa.eu/juris/document/document.jsf?docid=202543&doclang=EN