Scientific Research Publishing

Beijing Law Review, 2025, 16(2), 1195-1213
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Three Standpoints in Risk-Based Regulation: Applying a Meta-Regulatory Framework to Personal Data Protection

Heloisa Bianquini

Faculty of Law, University of São Paulo, São Paulo, Brazil
Email: hbianquini@gmail.com

How to cite this paper: Bianquini, H. (2025). Three Standpoints in Risk-Based Regulation: Applying a Meta-Regulatory Framework to Personal Data Protection. *Beijing Law Review, 16,* 1195-1213.
https://doi.org/10.4236/blr.2025.162061

Received: May 31, 2025
Accepted: June 27, 2025
Published: June 30, 2025

Abstract

By distinguishing between three perspectives of risk-based regulation—namely, of the regulated entity, the regulated activity, and of the regulator itself (Black, 2010b)—this article aims to propose a meta-regulatory framework to investigate the regulation of risk in the field of personal data protection. Using insights from the institutional development of Brazilian data protection law and comparing it with the GDPR, this study clarifies how each jurisdiction operationalizes risk and provides examples to illustrate how each of the three standpoints may interact with other perspectives. The article supports meta-regulatory debates and research on personal data regulation by providing examples and connecting these categories to the key features of a "riskified" (Spina, 2017; Macenaite, 2017) data protection law.

Keywords

Risk-Based Regulation, Personal Data Protection, GDPR, LGPD, Comparative Law

1. Introduction

As personal data has come to assume a central role in the global economy, regulatory approaches to the processing of personal information have, in parallel, increasingly relied on a regulatory model interchangeably called "risk-based regulation". In fact, "risk-based regulation" has become a buzzword in the field of personal data protection, and it is for comprehensible reasons. This approach was widely promoted as a way to cut compliance costs, improve regulatory enforcement, and use regulation to boost economic development (Macenaite, 2017; Black, 2010a). Also, risk-based regulation has promised to provide a solid methodology and a clear framework for jus-

tifying policy decisions.

To understand the shift in personal data protection towards the so-called "*risk-based regulation*" or "*risk-based approach*"—a trend referred to by authors such as Spina (2017) and Macenaite (2017) as the "*riskification*" of data protection—it is helpful to outline the regulatory waves of data protection regulation that preceded the rise of this risk-based paradigm. Although the concept of privacy has long been subject to legal and philosophical debate, its meaning shifted significantly with the adoption of new technologies that enabled low-cost, large-scale data processing. What was once framed as a "*right to be left alone*"[1] became increasingly tied to control over personal information.

The adoption of data protection laws initially responded to public backlash against early attempts by governments to centralize personal data in public databases, such as the U.S. National Data Center and France's Safari Program (Doneda, 2019). Beginning in the 1970s, the first generation of such laws built organizational and technical safeguards for information security in an effort to limit state power. These frameworks have not yet defined individual rights over personal data, even though they have established oversight mechanisms such as data commissioners (Mayer-Schönberger, 1997).

The scope and ambitions of subsequent waves of data protection legislation evolved over time. While the first generation of privacy regulations focused on securing personal data from potential authoritarian purposes, the second wave instituted individual rights such as access and correction. A 1983 ruling from the German Constitutional Court inaugurated a third wave, introducing the German term "informational self-determination", which gave privacy a positive bent by reframing it not as a mere negative freedom but as the individual ability to make self-determined choices regarding the processing of personal data (Mayer-Schönberger, 1997).

Starting in the 1980s, commercial imperatives and political consensus laid the groundwork for international regulatory convergence[2] (Bennett, 1997: pp. 100-101). In the late 1980s and early 1990s, a fourth wave of data protection laws emerged, recognizing that individual rights alone were insufficient to foster informational self-determination (Mayer-Schönberger, 1997). For instance, the EU Directive 95/46/EC limited the possibility of renouncing or negotiating data protection rights such as access and correction and prohibited the use of sensitive data, with few exceptions, to grapple with structural power imbalances between data subjects and organizations.

[1]In Olmstead v. United States, 277 U.S. 438 (1928), U.S. Supreme Court Justice Louis Brandeis famously introduced this expression. Key constitutional provisions—such as the First and Fourth Amendments, which respectively safeguard privacy through the protection of freedom of thought and the prohibition of unreasonable searches and seizures—have supported the development of the concept of privacy in the United States via case law.

[2]Examples of this convergence can be found in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, issued by the Organisation for Economic Co-operation and Development (OECD, 1980) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, 1981).

The early 2000s, in turn, witnessed the emergence of a risk-based regulatory approach for data protection as an increasingly proposed solution for balancing the growing economic importance of free transnational data flows and the concern to provide more substantial data protection safeguards (Macenaite, 2017: p. 507; Spina, 2017; Gellert, 2015). Additionally, this transition was driven by a perceived gap between data protection "on the books" and "in action" (Macenaite, 2017: p. 534; Quelle, 2017; CIPL, 2014: p. 1). Risk-based regulation emerged as a way to bridge this gap by translating high-level privacy principles into real-world compliance in a more practical and achievable manner.

Though determining exactly when the idea of risk was first established in data protection law is complex, a critical moment was the enactment of the aforementioned EU Directive 95/46/EC, which required supervisory authorities to conduct prior assessments on processing activities posing threats to individual rights and freedoms (Gellert, 2015). Another important landmark is the Recommendation CM/Rec (2010) 13 on profiling, issued by the Council of Europe (Gellert, 2015). Nevertheless, the General Data Protection Regulation (GDPR), which set out novel safeguards for managing risks associated with personal data processing and employed vocabulary based on risk, can be considered the peak of this legislative movement.

Originating in the public health domain (Alemanno, 2016), the so-called "risk-based approach" prioritizes regulatory activities and allocates resources according to risk. The strategy became popular during the regulatory crisis that affected European nations in the 1980s and 1990s when interventionist regulation came under fire for allegedly hindering economic growth through overly prescriptive rules and high compliance costs (Macenaite, 2017: p 509).

This article investigates how risk is regulated in personal data protection by employing a framework based on three standpoints for risk-based regulation, as identified by Black (2010b): the regulated entity, the regulated activity, and the regulator. This article deploys this framework by drawing on specialized literature on risk and regulation and risk-based regulation. To that end, it takes into account both theoretical discussions from the meta-regulation field and academic work applying such concepts to personal data protection. Also, it examines and compares Brazilian and European data protection regulations to illustrate how each perspective operationalizes the idea of risk to data protection.

Risk-based regulation is a relatively recent concept in regulation theory and lacks a universally precise definition. According to Black (2010b: p. 187), the term has been used *"to refer to anything from a loose agglomeration of approaches expressed in terms of risk, to highly structured and systematised decision making frameworks*". For the purposes of this article, risk-based regulation is understood as a regulatory strategy that relies on risk assessment and management methodologies to orient rulemaking, rule enforcement, organizational compliance, and the allocation of regulatory resources (Black, 2010a; Black, 2010b).

Additionally, this research adopts a "moderate" functionalist methodology (Husa,

2003; Michaels, 2006) in order to compare how the GDPR and the LGPD address a common regulatory challenge: managing privacy risks. These regulations were selected because they are among the most prominent contemporary data protection laws that explicitly incorporate elements of risk-based regulation, as further explained.

While the GDPR has become a global benchmark, illustrating what Bradford (2012) described as the "*Brussels effect*", the LGPD presents a more flexible and open-ended model, although clearly inspired by the European regime (Carrillo & Jackson, 2022; Mendes & Bioni, 2019). This inspiration facilitated the identification and comparison of similar legal solutions across both regulations.

A "moderate" functional comparative approach allows for a more detailed analysis of how each regulation conceptualizes and operationalizes the notion of risk through distinct regulatory strategies and institutional arrangements. Rather than seeking to merely establish equivalences between distinct legal institutions, this methodology aims to employ the functional relation between social problems (namely, privacy risks) and legal solutions as an analytical tool (Michaels, 2006: p. 371).

The article is structured as follows: Section 1 introduces the three perspectives on risk-based regulation. Sections 2, 3, and 4 apply each perspective to the increasingly "riskified" approach to data protection regulation, comparing how the GDPR and the LGPD operationalize risk-based regulation. The conclusion synthesizes the insights derived from the analysis, emphasizing the contributions of this typology to future research and policy design.

2. Disentangling Risk-Based Regulation from Three Standpoints: Regulated Entities, Economic Activities, and Regulators

The concept of risk has taken a central role in contemporary legal and policy debates, yet its meaning is far from consensual. Risk perceptions depend on context, culture, knowledge field, and methodology for their assessment. Some definitions (see Van der Heijden (2019) for a thorough literature review) focus on probabilities and measurable outcomes (Kaplan & Garrick, 1981), while others emphasize uncertainty and potential harm to human values (IRGC, 2005). Differences among concepts of risk frequently reflect broader tensions between realist approaches—which frame risk as objective and quantifiable—and constructivist views, which understand risk as socially and historically shaped (Van der Heijden, 2019; Rosa, Renn, & McCright, 2014).

Although this article does not aim to participate in a broader debate about the concept of risk, it takes the latter position, recognizing risk as an analytical construct shaped by institutions, public perception, and ever-evolving social demands. This work considers risk, ultimately, as a "*category of the understanding*" (Ewald, 1991: p. 199). The rise of risk-based approaches in data protection suggests that risk is historically and culturally contingent. The notion of "privacy risks", now

widely used by regulators and legal systems, reflects perceptions of how specific uses of personal data may harm something fundamentally human: privacy itself.

The risks faced by contemporary societies are varied, context-dependent, and can be framed and measured in myriad ways—and so are the institutional solutions devised to tackle them. However, some scholars have identified common patterns and objectives across different regulatory domains to better conceptualize risk regulation. For example, Alemanno (2016) outlines four core features of risk regulation: it tends to be goal-oriented and focused on public interest; it does not allow private interests to outweigh collective concerns; it centralizes enforcement and rulemaking; and it often arises in response to market failures that jeopardize socially relevant goals.

Hood, Rothstein, and Baldwin (2001) provide a more operational definition of risk regulation. They describe it as state intervention in market or social processes to control risks arising from negative externalities, involving three main elements. The first is information gathering, where regulators collect and monitor data to identify and measure risks through proactive inspections, disclosure obligations for regulated entities, or assessments from independent third parties. The second element, in turn, is standard-setting, which means establishing guidelines or targets to reduce risks, frequently through the definition of levels of risk tolerability. Finally, the third is behavior modification—using enforcement, incentives, awareness campaigns, or institutional design to steer behavior in ways that help mitigate risk.

However, not all risk regulation can be considered risk-based. Risk-based regulation is a specific model that relies on risk assessment methodology to guide compliance, monitoring, enforcement priorities, and rule-making in order to optimize resource allocation. It can be conceptualized according to three perspectives (Black, 2010b): the regulator, the regulated entity, and the economic activity.

The regulator's standpoint: Here, risk refers to the probability and severity of regulators failing to fulfill their institutional mission and objectives. Risk-based regulation assumes that regulators operate under constrained resources (resources are understood broadly, including time, knowledge, personnel, and political capital).

Regulators have always, implicitly or explicitly, made decisions that involved the acceptance, mitigation, or refusal of risks related to their functions (Black, 2010b). However, risk-based regulation stands out by clearly recognizing such limitations and requiring the explicit adoption of a methodology to assess such risks and guide the allocation of institutional resources, justifying regulatory interventions. From this viewpoint, risk-based regulation is ultimately a method to orient and rationalize decisions about what to regulate, how intensively to regulate, and when to intervene (Black, 2010b).

A central element of risk-based regulation is the development of internal tools and methodologies to identify, compare, and justify risk-based decisions. These frameworks often follow a sequential structure: identifying risk triggers, assessing their probability and impact, and defining acceptable thresholds of tolerance. Reg-

ulatory strategies are then aligned with this evaluation. This includes decisions such as whether to inspect a regulated entity or sector, how intensively to enforce a specific norm, or whether to issue interpretative guidance versus binding rules.

Literature on regulatory theory has explored some challenges regarding the adoption of this approach. Firstly, the risk appetite of regulators is not necessarily grounded only on methodology—ultimately, it has a close relationship with external factors such as political inclinations and interests; possible media repercussions; stakeholders' importance and demands; image and reputational concerns (Black, 2010b: p. 186). Secondly, although risk assessment methodologies do not promise to exclude political considerations from deliberation, but rather make them explicit, they may serve to disguise political choices under technical arguments, even when their relevance to the specific case has not been adequately assessed (Macenaite, 2017: p. 512).

Also, risk-based approaches may be instrumentalized by bureaucracies to avoid accountability, as their prerogatives to define which risks are tolerable may be used strategically to circumvent responsibilization when such risks are materialized (Black, 2010a: p. 323). Finally, there are some common limitations to this strategy regarding risk management methodologies—for instance, when such methods are not able to capture unexpected arising risks, or when risk mitigation measures are not properly implemented (Black, 2010b: p. 186).

Examples of risk-based regulation from a regulator standpoint include:

- **Institutional strategic planning:** Documents where regulators set out their medium- and long-term priorities, often based on an internal analysis of industry risks, available resources, and political or legal mandates.
- **Regulatory agendas:** Public-facing plans outlining and prioritizing which regulations will be created or reviewed within a specific period.
- **Key Performance Indicators (KPIs):** Metrics were first conceived to inform executive decision-making and later adopted by regulators to evaluate the effectiveness and efficiency of their actions. KPIs may track and even quantify how well regulatory interventions reduce specific risks.
- **Impact assessments for regulatory interventions:** Regulatory Impact Assessments are tools used early in the regulatory process to help policymakers understand the issue they intend to regulate and its context, compare alternatives, and assess potential costs, benefits, and unintended effects (Alves & Peci, 2011: p. 803).
- **Inspection and monitoring cycles/frameworks:** Inspection and monitoring frameworks help define when, where, and how regulatory supervision and inspection will be conducted.
- **Mandatory risk disclosure and reporting:** Regulatory requirements for entities to report high-risk events or activities to regulators. It helps regulators prioritize risks by acting as a filter, providing timely information on high-risk events.

The regulated entity's standpoint: Here, risk refers to the probability and se-

verity of consequences arising from regulated entities' non-compliance with regulatory standards, lack of diligence, and failure to properly manage risks. This standpoint expects organizations to perform context-specific assessments of their practices and implement governance measures proportional to the level of risk involved. This model demands that organizations acquire or develop internal expertise in identifying and managing regulatory risks, design internal controls to address such risks that can withstand scrutiny, and even anticipate how regulators may interpret their practices.

This standpoint entails a shift in responsibility: the burden of risk assessment and management is partially transferred from the State to private players. It also introduces important regulatory challenges. The first is epistemic: how should organizations define and measure risk? While some sectors have long-established standards to measure some risk categories—such as those related to information security or financial risk management—this is not a reality for every organization or industry. A second challenge is strategic: such delegation of powers and responsibilities can create incentives for organizations to shape their assessments in ways that minimize perceived exposure to regulatory enforcement. This can lead to underreporting, over-reliance on formalistic documentation, and opportunistic interpretation of rules to avoid real compliance—i.e., creative compliance (Parker & Braithwaite, 2005: p. 135).

Conversely, entities operating in high-risk sectors or under public scrutiny may adopt overly conservative approaches, leading to excessive compliance costs or defensive legalism. Also, the ability to engage with risk-based compliance is not evenly distributed. Larger or better-resourced entities are typically more capable of building sophisticated governance mechanisms, hiring experts, and engaging in dialogue with regulators. Also, companies from highly regulated sectors may be more able to build internal capacities to deal with new regulatory compliance requirements than other industries. This introduces a structural asymmetry: organizations are held to the same standard of demonstrating risk awareness, but do so under vastly different conditions.

This partial delegation of responsibilities, where regulated entities independently assess and mitigate risks, is a part of a broader context, conceptualized by regulation theory as "regulatory capitalism" (Levi-Faur, 2005). In regulatory capitalism, the State's role changes from direct governance to delegating regulatory powers to independent agencies and entities. In this framework, companies are expected to manage risks internally while the State maintains oversight, implying a reconfiguration of roles between the State, market, and society.

Examples of risk-based regulation from a regulated entity standpoint include:

- **Internal risk management frameworks:** Frameworks used by organizations to identify and manage risks internally. Such frameworks may be mandated by authorities, suggested by non-binding guidelines, or voluntarily adopted through codes of practice, certifications, global standards (like ISO standards), etc.
- **Organizational structures:** Specialized committees, governance bodies, or

functions overseeing risk management (such as risk committees, designated ombudsman, etc) to ensure accountability and senior leadership involvement in compliance efforts.

- **Context-specific risk assessments:** Evaluations that measure specific risks considering an organization's operations. They help prioritize resources and implement risk mitigation measures.
- **Audit and verification procedures:** Internal or external audits that assess the effectiveness of risk management practices and verify compliance with regulatory standards.
- **Scalable accountability:** Obligations and responsibility levels vary based on entity characteristics, such as its position in the value chain, size, sector, and revenue.

The economic activity standpoint: This perspective identifies and manages the risks of particular economic activities. Its central premise is the recognition that some economic activities entail more risk than others due to potential negative externalities, such as environmental or consumer harm and market disruption. Thus, this regulatory technique generally identifies economic activities assumed to be "riskier" and establishes conditions for those activities based on such risks.

The central idea of this approach is that activities with the potential for greater harm or disruption require more rigorous oversight and regulation. Such risks are not necessarily intrinsic to the activity—they may arise from factors such as scale, context, culture, or specific practices involved in its execution. By identifying which activities pose a higher risk, regulators aim to implement safeguards that ensure they occur in a way that mitigates individual and societal risks and harms.

One key challenge in regulating high-risk activities is defining and measuring risks. This exercise can be subjective and influenced by various factors, including political, social, and economic considerations. In some cases, specific sectors or practices that could pose significant risks may not immediately be recognized as such, leading to the potential for under-regulation.

A key difficulty is to anticipate the risks of a given activity before it occurs. Regulating high-risk activities requires an ex-ante understanding of why they should be deemed "riskier," considering each activity's characteristics. Predicting such risks is complex, as the actual impact and severity of potential harms are not always obvious beforehand. Therefore, in many instances, regulators face the challenge of forecasting risks without concrete examples of how these activities will unfold.

This complexity increases considering the variety of risks across sectors and industries. As a result, regulators often use proxies or generalized criteria to classify activities as high-risk. However, these parameters may not fully estimate the potential risks and harms, and may lead to overestimating or underestimating risks. This strategy can lead to Type 1 errors, where necessary regulation is overlooked, or Type 2 errors, where overregulation hinders innovation and increases

compliance costs (Black, 2010b: p. 186).

Examples of risk-based regulation from the economic activity standpoint include:

- **Industry-specific risk frameworks:** Tailored frameworks that help organizations identify and manage industry-specific risks, frequently based on industry standards or regulatory guidelines, such as ISO certifications.
- **Risk-based licensing and certification:** Regulatory measures requiring businesses in high-risk sectors to obtain and maintain licenses or certifications, including regular audits to ensure compliance with operational standards.
- **Mandatory risk disclosure and reporting:** Regulatory requirements for entities to report high-risk events or activities to regulators. They help regulators prioritize risks by acting as a filter and providing timely information on high-risk events (Bianquini, 2024).
- **Establishment of high-risk activity lists**: Legislative or regulatory measures that categorize specific economic activities as high-risk based on their harm potential and assign specific obligations or conditions for agents who carry out such activities.

3. Comparative Analysis: GDPR and LGPD through Three Risk Regulation Perspectives

The European General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (LGPD) both adopt the so-called "riskified" regulatory approach and apply it to personal data protection. Having outlined three distinct standpoints within risk-based regulation—those of the regulator, the regulated entity, and economic activity—this section applies the framework to analyze the concept of risk throughout the GDPR and the LGPD.

Though both laws refer explicitly to risk as a guiding principle for establishing and calibrating obligations, their context, structure, and implementation strategies differ significantly.

3.1. Risk Regulation from the Regulator's Perspective: Comparing DPIA and Breach Notification Mechanisms in the GDPR and LGPD

The GDPR and Brazil's LGPD incorporate elements of risk-based regulation, positioning risk as a guiding principle for regulatory action. However, the depth and clarity with which each legal framework operationalizes this approach differ significantly, especially in how they enable regulators to prioritize oversight and enforcement.

Data Protection Impact Assessments (DPIAs)

Under the GDPR, Article 35 mandates a prior Data Protection Impact Assessment (DPIA) when a processing activity is "likely to result in a high risk to the rights and freedoms of natural persons". Recital 84 further clarifies that such assessments must consider the risk's origin, nature, particularity, and severity.

Specific cases that trigger this obligation are defined: large-scale processing of special categories of data; systematic and large-scale monitoring of publicly accessible areas; and systematic evaluation of personal aspects based on automated processing (including profiling) for decision-making that produces legal or similar effects. If the risk remains high despite mitigation, the controller must consult the authority before proceeding. These procedural steps ensure that regulators are informed before high-risk activities begin, allowing them to intervene early (Article 36 GDPR).

In contrast, the LGPD also adopts DPIAs as an instrument to assess and measure risks, but with looser operationalization. While Article 5, XVII defines the DPIA as a documentation concerning processing activities that "*may generate risks to civil liberties and fundamental rights*", the law does not specify when the report is mandatory. Articles 10, § 3˚ and 38 allow the ANPD to request the RIPD under certain conditions, such as when data processing is based on legitimate interest or involves sensitive data.

However, unlike the GDPR, the Brazilian framework does not require explicitly that this assessment is carried out prior to the processing activities, nor does it establish a clear list of scenarios that would require it, leaving the obligation vague and dependent on regulation to be issued by the ANPD (Gomes, 2020; Mendes & Bioni, 2019), which has not yet happened.

Personal Data Breach Notification

Article 33 of the GDPR and Recital 85 set out a straightforward risk-based approach to breach notification. They require controllers to report incidents to the supervisory authority within 72 hours if there is a likely risk to individuals. If no risk is identified, reporting is not mandatory. This approach ensures that regulators prioritize only higher-risk cases.

Article 48 of the LGPD follows a similar structure but refers to incidents causing "relevant risk or damage" to data subjects. The controller must report such incidents to the ANPD and data subjects, though the law does not define what constitutes "relevant" risk. This gap was addressed by ANPD Resolution No. 15/2024, which sets a 3-business-day deadline for breach notification (Article 6) and outlines criteria for assessing relevant risks.

These risks include incidents that significantly affect fundamental rights—with consequences such as as material harms or emotional distress; discrimination; identity theft, etc.—and involve specific types of data (sensitive data; data from children, teenagers, or the elderly; financial data; authentication data; data protected by legal, judicial, or professional confidentiality) or large-scale processing (as per Article 5).

Conclusion: Risk as a Filtering Mechanism

Risk functions as a filtering mechanism in both laws, determining what the regulator will or will not know. However, this "filter" is first applied by the regulated entity, not the authority. The controller—not the regulator—assesses whether the processing activity or breach presents a high risk. While the GDPR offers struc-

tured guidance, the Brazilian regulation has left such determinations largely to the controller's discretion without providing clear criteria or tools until ANPD issued Resolution No. 15/2024.

This framework reinforces the idea that the effectiveness of risk-based regulation depends on how it is delegated. Even if the authority can issue guidelines or request documentation later, the regulated actor initially decides what gets reported and how. The decision to notify, the framing of an incident, and the content of a risk assessment are shaped by the controller's interpretation of risk, which may downplay the issue or rely on fragmented or unreliable metrics. This means that what reaches the regulator is filtered through a potentially biased or inconsistent lens.

3.2. Risk Regulation from the Regulated Entity's Perspective: Comparing Privacy by Design, Responsibilities for Controllers and Processors, and Scaling of Obligations in the GDPR and LGPD

The GDPR and LGPD prioritize risk-based regulation from the regulated entity standpoint by assigning extensive responsibilities to regulated players to ascertain and self-manage their risks. Nonetheless, how these frameworks operationalize this responsibility varies. The GDPR offers a more structured method, providing specific guidelines for organizations to address risks through mechanisms like privacy by design and security measures. The LGPD deploys such instruments in a less detailed fashion, leaving room for organizations to decide how to approach risk mitigation, and consequently creating a less prescriptive regulatory environment.

Privacy by Design

Privacy by design (PbD) is an important instrument of risk-based regulation applied to personal data protection, particularly from the standpoint of regulated entities. The concept proposes that privacy considerations should be integrated into systems and technologies from conception, with privacy set as the default in all processes. This approach suggests a shift from reactive compliance, where organizations respond to breaches or complaints, to a more proactive model, where organizations are expected to anticipate and address risks early on.

The GDPR formalizes this concept through Article 25, mandating that organizations implement privacy by design and default. According to this provision, organizations must embed privacy safeguards such as technical and organizational measures into their products and services to reduce risks and the likelihood of privacy violations. The objective behind PbD is to make privacy an intrinsic part of the system's architecture rather than a separate compliance task. In theory, PbD contributes to risk-based regulation by encouraging organizations to take responsibility for privacy risks before they emerge.

Article 46, § 2° of the LGPD is also inspired by the concepts of privacy by design and default, though in a fragmented and vague format. It broadly states that security measures must be adopted from the design phase of products or services without more specific references to risk. This approach differs from the one embraced by the GDPR, which specifically ties the adoption of such measures to the preven-

tion of risks to individuals' rights and freedoms, thus linking privacy by default to risk-based regulation.

From the perspective of the regulated entity, adopting PbD could be seen as a cost-effective strategy—adjustments made early in the design phase may be cheaper than dealing with the consequences of non-compliance, such as fines or reputational damage. However, this benefit is contingent on how effectively PbD is implemented. For regulators, the self-management of risks by the regulated entity can act as a "filter," reducing the need for active enforcement and allowing for a more focused allocation of regulatory resources.

Ultimately, while privacy by design is framed as a key tool for managing risks, its actual effectiveness in mitigating risks remains an open question. The potential benefits of PbD largely depend on how well organizations integrate it into their systems and the extent to which privacy is genuinely considered in the design and operation of new technologies. Thus, while this approach is touted as a proactive measure for risk-based regulation, its practical impact requires further evaluation.

Responsibilities for Controllers and Processors

The GDPR and LGPD both differentiate and assign specific responsibilities to controllers and processors, recognizing that distinct roles impose different risks. While controllers are in charge of determining the purposes and means of personal information processing, processors are expected to act on their behalf. The GDPR assigns primary responsibility for compliance to controllers, requiring them to ensure that the processing complies with legal obligations, including conducting DPIAs and duly implementing security measures.

The LGPD draws a similar distinction between controllers and processors. However, there is less specificity regarding processors' obligations. While both parties should provide security and compliance, the LGPD is less prescriptive in defining how processors should assess and manage risk. This places a greater burden on controllers to define the scope of risk and implement safeguards in the context of their relationship with processors through contractual provisions, due diligence, vendor onboarding policies and processes, and day-to-day supervision.

Scaling Obligations Based on the Size of the Entity

Both the GDPR and the LGPD recognize that the scale of an organization should influence its compliance obligations. For example, the GDPR (Article 30, 5) waives the requirement for Records of Processing Activities (ROPA) for organizations with fewer than 250 employees unless the processing is likely to result in high risks to individuals' rights and freedoms. This approach of scalable obligations reflects the understanding that smaller entities may generate fewer risks (or at least, if such risks materialize, the impacts are less extensive) and thus require less extensive documentation.

Similarly, the LGPD allows for some scaling of obligations but is more reluctant to establish waivers. For instance, ANPD Resolution No. 2/2022 does not exempt micro and small companies (SMEs) from documenting processing activities through ROPA but instead provides a simplified ROPA template that such processing agents

may adopt (Article 9).

Nonetheless, both frameworks emphasize that the size and complexity of an organization should not exempt it from managing risks appropriately. Smaller organizations still must assess and mitigate risks where necessary, particularly in cases where their processing activities involve sensitive data or pose significant risks to individuals.

Conclusion: Risk and regulatory delegation

Considering the regulated entity perspective of risk-based regulation, it is noticeable that, in the GDPR and LGPD, regulatory delegation is key to risk-based regulation, redirecting the responsibility for managing risks onto the regulated entities. The GDPR provides a framework that clearly defines the obligations of organizations, such as implementing privacy by design and default. In contrast, the LGPD offers more flexibility by granting organizations autonomy to determine how to address risks, with less detailed guidance on implementing privacy by design or risk assessments, leaving more room for interpretation and self-management.

The delegation of responsibility is also evident in how the regulations assign duties to controllers and processors. The GDPR places primary responsibility on controllers to ensure compliance, including conducting DPIAs and implementing security measures, while processors follow the controller's instructions. The LGPD mirrors this division but is less detailed in terms of roles and responsibilities.

These regulations recognize the varying risk levels of different organizations and scale obligations accordingly. Nonetheless, the burden of managing risks falls mainly on the regulated entities, highlighting the central role of regulatory delegation in risk-based approaches.

3.3. Risk Regulation from the Standpoint of Regulated Activities: Comparing High-Risk Activities, Restrictions on Sensitive Data Processing, and DPIAs in the GDPR and LGPD

Both the GDPR and LGPD aim to manage and mitigate the risks arising from data processing activities, but their approaches to risk-based regulation differ significantly. While the GDPR provides a more structured framework for identifying proactively high-risk activities, the LGPD offers a more flexible approach, leaving much to the interpretation of the regulator and the regulated entity.

In this section, we explore how these regulations shape the perspective of the regulated activity, focusing on high-risk activities, restrictions on the processing of sensitive data, and the role of Data Protection Impact Assessments (DPIAs).

High-Risk Activities in the GDPR and the LGPD

One of the most prominent distinctions between the GDPR and LGPD is their strategies for identifying which processing activities can be considered high-risk. The GDPR provides clear guidelines on what constitutes high-risk activities, with Recital 75 and Article 35 specifically listing types of processing likely to result in high risks to individuals' rights and freedoms.

These include activities such as large-scale processing of sensitive data, systematic profiling, and processing data on a large scale in publicly accessible areas. The

regulation also identifies risks for vulnerable groups, like children, and activities that could lead to significant economic or social harm, such as identity theft or discrimination.

In contrast, the LGPD does not provide such detailed lists of high-risk activities. The law takes a more general approach, prescribing data controllers to assess risks concerning their processing activities. While Article 5, XVII states that a DPIA is to be carried out when processing activities may generate risks to civil liberties and fundamental rights, it does not anticipate which specific activities automatically require such scrutiny.

This open-ended framework allows for more flexibility in risk assessment but also places a greater burden on regulated entities to determine which risks associated with their activities should merit this assessment. However, the ANPD has, over time, expressed its understanding of what constitutes high risk across multiple regulations.

For instance, on personal data breach reporting, ANPD Resolution No. 15/2024 lists criteria for categorizing a data breach as entailing "relevant risk" (see page 11). Such criteria do not list specific processing activities but highlight types of personal data that could cause more risks if processed in a way that causes a security incident and consequences of data processing, which could generate high risk.

ANPD Resolution No. 2/2022 provides more detailed guidance. It sets out a simplified compliance regime for "small-scale processing agents" (such as SMEs, startups, etc.). This simplified regime excludes small-scale processing agents that carry out high-risk processing activities from its scope. The Resolution considers data processing to be high-risk if it meets at least one of the general criteria and one of the specific criteria set out in Article 4.

The general criteria include large-scale data processing or activities that could significantly impact data subjects' fundamental rights and interests. The specific criteria are: processing involving emerging technologies; surveillance in publicly accessible areas; decisions based solely on automated data processing, including those aimed at defining personal, professional, health, consumption, and credit profiles or aspects of the data subject's personality; or the use of sensitive data, or data from children, adolescents, and the elderly.

On one hand, the GDPR's more prescriptive approach offers organizations relatively clear direction and guidance, and thus helps reduce the complexity associated with complying with data protection rules. The GDPR clearly specifies activities considered high-risk processing, thus directing organizations to allocate their efforts and resources to establish safeguards for "riskier" processing activities.

On the other hand, this approach can be limiting, as it might not fully account for new or unexpected risks, especially in fields such as AI or emerging technologies. While the GDPR provides a list of activities that may be considered high-risk, it's important to remember that this list is not exhaustive. The regulation offers these examples to guide organizations and authorities in identifying high-risk activities, but it also leaves room for other activities to be considered high-

risk depending on the context.

However, this approach can lead organizations and authorities to focus only on these listed activities. As a result, they might overlook other important factors or emerging risks that aren't included. The LGPD's structure is more flexible and gives more responsibility to the entity to assess risks according to a set of criteria. By not defining a list of high-risk activities, the LGPD offers a more resilient framework for future changes, making it potentially more "future-proofed" compared to the GDPR.

Nevertheless, this methodology can also prove to be challenging for both regulators and regulated entities, as it places significant responsibility on organizations to carry out risk assessments without detailed guidance, which could lead to inconsistencies or even opportunistic behavior from organizations. It is also important to note that these criteria were formally outlined only in regulations directed at small-scale processing agents.

Restrictions on Processing of Special Categories of Data

One critical area where the GDPR and LGPD have similarities is in their framework for the processing of special categories of data. Both regulations recognize that processing specific categories of data—such as health, political opinions, racial or ethnic origin, and sexual orientation—poses higher risks to individuals' privacy and freedoms, requiring more rigorous safeguards.

Under the GDPR, Article 9 explicitly prohibits the processing of special categories of data unless one of the specified exceptions applies, such as the explicit consent of the data subject or processing for substantial public interest, public health purposes, or scientific research. The regulation clearly outlines the conditions under which special categories of data can be processed, offering a structured approach to ensure risks are properly mitigated.

Similarly, the LGPD also restricts the processing of special categories of data (or "sensitive data") under Article 11, requiring that such processing activities meet at least one of the specified legal bases, such as the data subject's explicit consent or when processing is necessary for compliance with a legal obligation, health-related purposes, or protection of data subjects' life. While the LGPD provides more flexibility in some areas, its regulatory approach to sensitive data processing is aligned with the GDPR in form and substance.

Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) are important instruments in LGPD and GDPR for identifying and mitigating risks caused by data processing activities. However, their structure and requirements differ significantly. Under the GDPR, Article 35 mandates DPIAs for high-risk activities, specifically those that involve sensitive data, large-scale profiling, or systematic monitoring.

The regulation sets clear guidelines on when a DPIA is required, ensuring that regulated entities know beforehand which activities will likely result in risks to individuals' rights and freedoms. In contrast, the LGPD does not provide the same clarity on when a DPIA is required, as it lacks specific guidance on which processing activities trigger the need for this assessment. This results in a more flexi-

ble, yet less structured, approach to risk assessment.

It also places a challenging responsibility on organizations: determining and evaluating what constitutes high risk without direct guidance. Although the intention is to offer flexibility and reduce compliance costs, this can, in practice, increase them. The complexity of figuring out which activities require a DPIA and which do not can make it more difficult and costly for organizations to understand and navigate the law.

Conclusion: Risk and assessment methodologies

The GDPR and LGPD handle high-risk activities differently, with varying levels of regulatory delegation to the entities to adopt methodologies and conceptual frameworks to identify risk in their activities. The GDPR is more prescriptive, establishing specific hypotheses of high-risk activities like large-scale processing of sensitive data and systematic profiling, which helps organizations direct resources where needed. However, this structure may not fully account for emerging risks.

In contrast, the LGPD gives more flexibility to organizations, leaving them to assess risks independently, which can be advantageous for adaptability but burdensome and complex without clear guidance. Both regulations acknowledge the higher risks of sensitive data processing and require Data Protection Impact Assessments (DPIAs). The GDPR specifies when a DPIA is required, making it easier for organizations to comply. The LGPD, however, offers less clarity, putting the responsibility on organizations to determine when and how they should carry out this assessment.

While this provides flexibility, it can confuse organizations and increase compliance challenges. This is supported by a recent empirical study carried out by Dalle Rocha et al. (2023), which found that ICT professionals often struggled to implement LGPD principles, citing "*a lack of knowledge about implementation techniques*" as a key obstacle. This study highlights that privacy compliance is not limited to legal or privacy professionals but involves technical actors throughout the development lifecycle. In this context, the absence of concrete guidance can compromise privacy compliance across different organizational functions.

4. Conclusion

This article proposed a structured framework for analyzing risk-based regulation in personal data protection by distinguishing among three standpoints: the regulator, the regulated entity, and the economic activity (Black, 2010b). This approach allowed for a more precise understanding of how "risk"—a concept that remains normatively vague and operationally contested—is constructed, mobilized, and negotiated across different layers of the regulatory ecosystem.

The regulator's standpoint is characterized by prioritizing regulatory actions based on risk assessments. This model helps regulators decide which areas or activities need the most oversight based on their potential risks. The perspective of the regulated entity shifts the focus to how businesses assess and manage risk in their operations. Lastly, the economic activity standpoint focuses on the inherent risks in particular activities and which methodologies and strategies can be adopted

to conceptualize, calculate, and regulate such risks.

Considering the regulators' perspective, the GDPR and the LGPD incorporate risk-based regulation with different approaches. The GDPR provides clear, structured guidelines for DPIAs and breach notifications. In contrast, while the LGPD, coupled with subsequent regulation, also offers clarity on data breach notification, the DPIAs have weaker operationalization, which can lead to inconsistencies. Despite these differences, both frameworks use DPIAs and breach notifications as filtering mechanisms to control the flow of information to regulators, ensuring that high-risk situations are reported.

From the regulated entity's perspective, both the GDPR and LGPD emphasize the importance of risk-based regulation, shifting the compliance burden from a fixed checklist of obligations to a more context-specific, interpretive exercise. Both frameworks require organizations to assess, document, and justify their data processing activities, making risk management a core component of their internal governance. However, while the GDPR provides more prescriptive guidance, including mandatory DPIAs, detailed security measures, and more precise definitions of incident reporting, the LGPD offers a more flexible approach, placing greater responsibility on the entity to interpret and assess risks.

From the lens of economic activities, the GDPR and LGPD differ significantly in how they address the regulation of high-risk data processing and the use of Data Protection Impact Assessments (DPIAs). Nevertheless, they adopt similar regimes for restricting sensitive data processing. The GDPR provides a more structured, prescriptive framework, offering clear guidelines on what constitutes high-risk activities.

In contrast, the LGPD offers a broader, more flexible framework that places greater responsibility on regulated entities to interpret which activities can be considered as such. While this flexibility allows organizations more room for maneuver, it also increases the complexity and costs of compliance and may result in a less consistent approach to risk-based regulation across different types of activities.

Theoretically, deploying this tripartite categorization to personal data protection clarifies how its regulatory instruments are operationalized in practice. It helps disentangle legal form from institutional function. It shows how the same concept—"risk"—can acquire different meanings depending on who interprets it, how it is used, and to what end. It also reveals where tensions emerge: for example, when a regulator's risk prioritization does not align with how an entity defines its obligations or when economic logic transforms a protective safeguard into a cost-reduction mechanism.

This categorization is valuable for policymakers and regulators because it helps clarify how different regulatory strategies work in practice. By distinguishing between the perspectives of the regulator, the regulated entity, and the economic activity, it becomes easier to design regulations that address specific privacy risks and needs. Understanding these differences helps identify gaps, improve consistency, and ensure that data protection regulations are applied effectively, managing risks across different approaches.

This framework opens up new directions in regulation theory for future research in personal data protection. Researchers could explore how to create more coherent regulatory strategies, aiming to align how regulators prioritize privacy risks, how businesses self-manage their internal risks, and how the risks of processing activities are understood and measured. This could offer practical insights into how data protection regulations are conceived and applied and help improve the design of regulatory frameworks across different sectors.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Alemanno, A. (2016). Risk and Regulation. In A. Burgess, A. Alemanno, & J. O. Zinn (Eds.), *Routledge Handbook of Risk Studies* (pp. 191-203). Routledge.

Alves, F. N. R., & Peci, A. (2011). Análise de Impacto Regulatório: Uma nova ferramenta para a melhoria da regulação na Anvisa. *Revista de Saúde Pública, 45,* 802-805. https://doi.org/10.1590/s0034-89102011000400023

Bennett, C. (1997). Convergence Revisited: Toward a Global Policy for the Protection of Personal Data? In P. E. Agre, & M. Rotenberg (Eds.), *Technology and Privacy: The New Landscape* (pp. 99-123). MIT Press.

Bianquini, H. (2024). *Personal Data Protection and Risk-Based Regulation: Institutional Development of Regulatory Frameworks by the Brazilian Data Protection Authority*. Ph.D. Thesis, University of São Paulo.

Black, J. (2010a). The Role of Risk in Regulatory Processes. In R. Baldwin, M. Cave, & M. Lodge (Eds.), *The Oxford Handbook of Regulation* (pp. 302-348). Oxford University Press. ttps://doi.org/10.1093/oxfordhb/9780199560219.003.0014

Black, J. (2010b). Risk-Based Regulation: Choices, Practices and Lessons Being Learnt. In OECD (Eds.), *Risk and Regulation: OECD Reviews of Regulatory Reform* (pp. 185-236). OECD Publishing.

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review, 107,* 1-67.

Carrillo, A. J., & Jackson, M. (2022). Follow the Leader? A Comparative Law Study of the Eu's General Data Protection Regulation's Impact in Latin America. *ICL Journal, 16,* 177-262. https://doi.org/10.1515/icl-2021-0037

CIPL (Centre for Information Policy Leadership) (2014). *A Risk-Based Approach to Privacy: Improving Effectiveness in Practice.* https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf

Council of Europe (1981). *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.* Council of Europe. https://rm.coe.int/1680078b37

Dalle Rocha, L., Sousa Silva, G. R., & Canedo, E. D. (2023). Privacy Compliance in Software Development: A Guide to Implementing the LGPD Principles. In *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing* (pp. 1352-1361). ACM. https://doi.org/10.1145/3555776.3577615

Doneda, D. (2019). *Da privacidade à proteção de dados pessoais* (2nd ed.). Revista dos Tribunais.

Ewald, F. (1991). Insurance and Risk. In G. Burchill, C. Gordon, & P. Miller (Eds.), *The Foucault Effect: Studies in Governmentality* (pp. 197-210). University of Chicago Press.

Gellert, R. (2015). Understanding the Notion of Risk in the General Data Protection Regulation. *Computer Law & Security Review, 31,* 497-508.

Gomes, M. C. O. (2020). Entre o método e a complexidade: Compreendendo a noção de risco na LGPD. In F. Palhares (Coord.), *Temas atuais de proteção de dados* (pp. 245-271). Revista dos Tribunais.

Hood, C., Rothstein, H., & Baldwin, R. (2001). *The Government of Risk: Understanding Risk Regulation Regimes.* Oxford University Press.

Husa, J. (2003). Farewell to Functionalism or Methodological Tolerance? *Rabels Zeitschrift für ausländisches und internationales Privatrecht, 67,* 419-447. https://doi.org/10.1628/0033725033631996

IRGC (2005). *Risk Governance: Towards an Integrative Approach.* International Risk Governance Council.

Kaplan, S., & Garrick, B. J. (1981). On the Quantitative Definition of Risk. *Risk Analysis, 1,* 11-27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Levi-Faur, D. (2005). The Global Diffusion of Regulatory Capitalism. *The Annals of the American Academy of Political and Social Science, 598,* 12-32. https://doi.org/10.1177/0002716204272371

Macenaite, M. (2017). The "Riskification" of European Data Protection Law through a Two-Fold Shift. *European Journal of Risk Regulation, 8,* 506-540. https://doi.org/10.1017/err.2017.40

Mayer-Schönberger, V. (1997). Generational Development of Data Protection in Europe. In P. E. Agre, & M. Rotenberg (Eds.), *Technology and Privacy: The New Landscape* (pp. 219-241). MIT Press.

Mendes, L. S., & Bioni, B. R. (2019). O regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados Brasileira: Mapeando convergências na direção de um nível de equivalência. *Revista de Direito do Consumidor, 124,* 157-180.

Michaels, R. (2006). The Functional Method of Comparative Law. In M. Reimann, & R. Zimmermann (Eds.), *The Oxford Handbook of Comparative Law* (pp. 339-382). Oxford University Press.

Organisation for Economic Co-Operation and Development (OECD) (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf

Parker, C., & Braithwaite, J. (2012). Regulation. In M. Tushnet, & P. Cane (Eds.), *The Oxford Handbook of Legal Studies* (pp. 119-145). Oxford Academic. https://doi.org/10.1093/oxfordhb/9780199248179.013.0007

Quelle, C. (2017). Privacy, Proceduralism and Self-Regulation in Data Protection Law. *Teoria Critica della Regolazione Sociale*, 89-106. https://ssrn.com/abstract=3139901

Rosa, E., Renn, O., & McCright, A. (2014). *The Risk Society Revisited: Social Theory and Governance.* Temple University Press.

Spina, A. (2017). A Regulatory *Mariage de Figaro*: Risk Regulation, Data Protection, and Data Ethics. *European Journal of Risk Regulation, 8,* 88-94. https://doi.org/10.1017/err.2016.15

van der Heijden, J. (2019). *Risk Governance and Risk-Based Regulation: A Review of the International Academic Literature.* Te Herenga Waka-Victoria University of Wellington. https://ir.wgtn.ac.nz/items/e02c2440-ab62-43dd-81bb-e86fc871fe17