REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

DATA PROTECTION AUTHORITIES (DPAS): A GLOBAL SURVEY USING THE 5W2H (KIPLING) TECHNIQUE AND THE INSTITUTIONAL CHARACTERISTICS THAT DISTINGUISH COUNTRIES WITH AND WITHOUT A DPA

AUTORIDADES DE PROTEÇÃO DE DADOS (APDS): LEVANTAMENTO GLOBAL POR MEIO DA TÉCNICA 5W2H (TÉCNICA KIPLING), E AS CARACTERÍSTICAS INSTITUCIONAIS QUE DIFERENCIAM OS PAÍSES COM E SEM UMA APD

AUTORIDADES DE PROTECCIÓN DE DATOS (APDS): ESTUDIO GLOBAL MEDIANTE LA TÉCNICA 5W2H (MÉTODO KIPLING) Y LAS CARACTERÍSTICAS INSTITUCIONALES QUE DIFERENCIAN A LOS PAÍSES CON Y SIN APD

Carlos Eduardo Costa Oliveira[1], Angelo Machado de Souza[2], Davis Souza Alves[3]

e2131
https://doi.org/10.67553/sol21.v.2i1.31

PUBLISHED: 09/2026

ABSTRACT

The worldwide diffusion of data protection laws has not produced a single model of institutional oversight. This study asks how Data Protection Authorities (DPAs) and alternative arrangements can be compared globally through the 5W2H technique, and which characteristics distinguish countries with and without a dedicated national authority. A documentary, descriptive, and comparative study was conducted using the 193 United Nations Member States as the reference universe. Legislation, official documents, global inventories, and scientific literature were examined while preserving each source's cutoff date and unit of analysis. The 5W2H framework was operationalized through variables concerning the existence of a law and an authority, legal basis, institutional nature, position within the State, chronology, governance, powers, resources, and outputs. The classification rules were explored in contrasting institutional arrangements using official sources. The survey confirmed 172 countries with privacy laws by March 2025, but showed that this figure is not the number of DPAs: available sources use different denominators, accreditation requirements, and territorial levels. Rather than forcing an unsupported count, the study proposes seven institutional types and identifies institutional position, appointment and removal, budgetary autonomy, human resources, powers, complaint channels, cooperation, and accountability as differentiating dimensions. Data

[1] Fundador da vBold LLC (EUA) e vBold Ltda (Brasil), empresas que prestam serviços de inovação e segurança em tecnologia a clientes nacionais e internacionais. Graduação em Direito, pós-graduação em Computação em Nuvem e cursando mestrado em Negócios Globais nos EUA. Autor do livro Navegando Pelos Desafios da Segurança da Informação, é membro da Mensa Internacional, Vice-Presidente da APDADOS e Imortal da ABRASCI, além de ter recebido o título Honoris Causa em Ciências Exatas pela WCU. Reconhecido por sua liderança e impacto, alia expertise em tecnologia à missão de transformar vidas e gerar oportunidades.

[2] Profissional Especialista em Segurança da Informação | Cibersegurança | Governança de TI | Privacidade de Dados na área de Tecnologia da Informação, com ênfase em Segurança da Informação, Governança de TI e Privacidade de Dados. Foco estratégico na proteção de ativos digitais e no fortalecimento da resiliência cibernética frente aos desafios do ambiente digital atual. Mestrado em Segurança da Informação pela Florida Christian University, com pesquisa voltada à conformidade com a LGPD. MBA em Gerenciamento de Projetos de TI e certificações internacionais, como Certified Information Security Officer (CISO), ISO/IEC 27001 Lead Implementer e DPO – EXIN.
Liderança de projetos em empresas como NTT Ltd., ISH Tecnologia e Grupo Cornélio Brennand, com atuação em mitigação de riscos, resposta a incidentes, conformidade regulatória e implementação de políticas de segurança.
Competência comprovada em: Conformidade com normas e legislações: ISO/IEC 27001, ISO 27002, LGPD, ITIL, ISO 31000, ISO 27005
Gestão de riscos e implementação de controles e políticas de segurança. Resposta a incidentes, análise de ameaças e continuidade de negócios. Coordenação de projetos de cibersegurança e gestão de equipes técnicas. Apoio a auditorias, criação de planos diretores de tecnologia (PDTI) e campanhas de conscientização. Alinhamento entre TI, compliance e objetivos de negócio, com forte habilidade de comunicação com stakeholders.

[3] Doutor em Administração de TI - Ph.D na Florida Christian University (EUA) convalidado no Brasil, Mestre em Administração com foco em TI Verde (2015), Extensão em Gestão de TI pela FGV/SP (2011), Pós-graduado em Gerenciamento de Projetos (2009), Graduado em Redes de Computadores e Internet (2008). Residiu para estudos nos Estados Unidos e Nova Zelândia. Possui as certificações PMP®, ITIL® Expert, C|EH®, ITIL® Professional (4 MP), COBIT®, ISO-20000®, ISO-27002®, EXIN® Agile Scrum Master, Lean IT, Green IT, ICS MCSA® Windows Server 2003, Cloud Computing, EXIN® Data Protection Officer (DPO), & EXIN ISO-27001 Professional (ISMP), Cyber Security, CompTIA Security+, EC-Council Certified Ethical Hacker, Psicanalista, CompuTIA Security+, DAC® Wireless, DCP® Switching, DSS® IP Surveillance. É consultor de Gestão de Sustentabilidade de TI, com produtos e consultorias em Green IT para órgãos públicos municipais do Brasil, além de Consultor em Privacidade de Dados (LGPD). DPO pioneiro no Brasil na área de Segurança da Informação & Ethical Hacker tendo formado mais de 5,5 mil DPOs no país.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

protection legislation, a dedicated authority, and operational capacity are therefore related but non-interchangeable analytical layers.

KEYWORDS: Data protection. Privacy. Regulatory authorities. Governance.

RESUMO
A disseminação mundial de leis de proteção de dados não produziu um modelo institucional único de supervisão. Este estudo pergunta como comparar, em escala global e por meio da técnica 5W2H, as Autoridades de Proteção de Dados (APDs) e os arranjos alternativos, bem como quais características diferenciam países com e sem autoridade nacional dedicada. Realizou-se pesquisa documental, descritiva e comparativa, tendo como universo de referência os 193 Estados-membros das Nações Unidas. Foram examinados legislação e documentos oficiais, inventários globais e literatura científica, preservando-se as datas de corte e as unidades de análise de cada fonte. O 5W2H foi operacionalizado em variáveis relativas à existência da lei e da autoridade, fundamento jurídico, natureza institucional, localização estatal, cronologia, governança, poderes, recursos e resultados. As regras de classificação foram testadas exploratoriamente em arranjos institucionais contrastantes, com base em fontes oficiais. O levantamento confirmou 172 países com leis de privacidade até março de 2025, mas demonstrou que esse total não equivale ao número de APDs: as bases disponíveis adotam denominadores, critérios de acreditação e níveis territoriais distintos. Em vez de forçar uma contagem não sustentada, o estudo propõe sete tipos institucionais e identifica como dimensões diferenciadoras a posição estatal, a nomeação e exoneração, a autonomia orçamentária, os recursos humanos, os poderes, os canais de reclamação, a cooperação e a prestação de contas. Conclui-se que legislação, autoridade dedicada e capacidade operacional são camadas analíticas relacionadas, porém não intercambiáveis.

PALAVRAS-CHAVE: Proteção de dados. Privacidade. Autoridades reguladoras. Governança.

RESUMEN
La difusión mundial de leyes de protección de datos no ha producido un modelo único de supervisión institucional. Este estudio pregunta cómo comparar globalmente, por medio de la técnica 5W2H, las Autoridades de Protección de Datos (APDs) y los arreglos alternativos, y qué características diferencian a los países con y sin una autoridad nacional especializada. Se realizó una investigación documental, descriptiva y comparativa, tomando como universo de referencia los 193 Estados Miembros de las Naciones Unidas. Se examinaron legislación, documentos oficiales, inventarios globales y literatura científica, conservando las fechas de corte y las unidades de análisis de cada fuente. El 5W2H se operacionalizó mediante variables relativas a la existencia de la ley y de la autoridad, fundamento jurídico, naturaleza institucional, ubicación en el Estado, cronología, gobernanza, poderes, recursos y resultados. Las reglas de clasificación se probaron de forma exploratoria en arreglos institucionales contrastantes mediante fuentes oficiales. El estudio confirmó 172 países con leyes de privacidad hasta marzo de 2025, pero mostró que esa cifra no equivale al número de APDs, pues las fuentes disponibles utilizan denominadores, requisitos de acreditación y niveles territoriales distintos. En lugar de imponer un recuento sin respaldo, se proponen siete tipos institucionales y se identifican como dimensiones diferenciadoras la posición estatal, el nombramiento y la remoción, la autonomía presupuestaria, los recursos humanos, los poderes, los canales de reclamación, la cooperación y la rendición de cuentas. La legislación, la autoridad especializada y la capacidad operativa son capas analíticas relacionadas, pero no intercambiables.

PALABRAS CLAVE: Protección de datos. Privacidad. Autoridades reguladoras. Gobernanza.

1 - INTRODUCTION

The legal protection of personal information predates the platform economy. The 1970 law of the German state of Hesse is commonly regarded as the first modern data protection statute at

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

the subnational level, while Sweden enacted the first national law of its kind in 1973. In the following decade, the Guidelines of the Organisation for Economic Co-operation and Development consolidated principles for the protection of privacy and transborder data flows, and the Council of Europe's Convention 108 established the first legally binding international treaty dedicated to the automated processing of personal data (OECD, 1980; Council of Europe, 1981; Greenleaf, 2025b).

Directive 95/46/EC incorporated institutional supervision into the European model by requiring Member States to establish one or more public authorities responsible for monitoring its application. The General Data Protection Regulation, adopted in 2016 and applicable since May 25, 2018, further developed this architecture: Articles 51 to 59 address the establishment, independence, responsibilities, powers, and accountability of supervisory authorities. The presence of a DPA thus ceased to be merely an administrative arrangement and became part of the institutional guarantee of the right to data protection under European Union law (European Union, 1995, 2016).

The global expansion of data protection laws occurred alongside the digitalization of public and private services, the growth of cloud computing, and the intensive use of data in artificial intelligence systems. Greenleaf (2025a, 2025b) identified 172 countries with national privacy laws as of March 15, 2025, including 12 new laws enacted in 2023 and 2024. This growth, however, does not in itself demonstrate that all jurisdictions have a dedicated, independent authority or one with sufficient operational capacity to oversee compliance with these laws.

The central problem addressed in this article arises from this lack of equivalence. A law may assign supervisory responsibilities to a specialized authority, a ministry, a collegiate commission, a multisector regulator, or a combination of bodies. Even where a formally independent DPA exists, differences in budget, staffing, appointment procedures, investigative powers, sanctioning capacity, and access mechanisms for data subjects may result in significantly different levels of regulatory activity. Therefore, comparing only the existence of a law or the name of the supervisory body conflates legal design with institutional capacity.

The literature provides detailed evidence on independence, workload, enforcement strategies, and performance assessment, but remains concentrated on European contexts or specific groups of countries. Studies involving 13 or 18 authorities demonstrate significant heterogeneity, while broader global analyses focus primarily on the existence and content of laws (Puljak; Mladinić; Koporc, 2023; Sivan-Sevilla, 2024; Greenleaf, 2025a). There is therefore a methodological gap between the global inventory of data protection laws and the institutional comparison of the bodies responsible for their enforcement.

The research question is: how can the 5W2H technique be used to organize a comparable global survey of DPAs and alternative supervisory arrangements, and which institutional characteristics distinguish countries with and without a dedicated national authority? The general objective is to identify and compare, within the reference universe of United Nations Member States,

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

the dimensions necessary to classify supervisory models without assuming that legislation, the existence of a DPA, and independence are equivalent categories. Specifically, the study seeks to define inclusion criteria; operationalize the 5W2H framework; propose an institutional typology; and distinguish confirmed findings from documentary gaps.

The study makes two main contributions. From a methodological perspective, it presents a replicable data collection and coding protocol that preserves the source and date of each item of evidence. From an analytical perspective, it replaces the simple distinction between countries “with” and “without” a DPA with a graduated classification of supervisory arrangements. Following this introduction, the article reviews the literature, describes the methodology, presents the results of the documentary survey, discusses their implications, and concludes with findings proportionate to the available evidence.

2 – THEORETICAL FRAMEWORK

2.1 Personal Data Protection and Supervisory Mechanisms

Data protection laws establish principles, rights, obligations, and bases for accountability, but their effectiveness depends on mechanisms capable of translating normative requirements into observable practices. Bygrave (2014) and Kuner (2013) demonstrate that data regulation brings together fundamental rights, economic interests, and cross-border data flows. This combination requires interpretation, guidance, oversight, and dispute resolution—activities that cannot be accomplished merely through the enactment of legislation.

It is useful to distinguish four dimensions. Implementation refers to the establishment of administrative and technical conditions necessary to comply with the law. Supervision involves monitoring and oversight by a competent authority. Enforcement oversight concerns the examination of conduct and the handling of complaints or investigations. Enforcement encompasses the use of corrective measures, orders, sanctions, and other instruments intended to ensure compliance. A system may be normatively comprehensive and yet have limited capacity in one or more of these dimensions.

The European model makes this distinction explicit. The GDPR assigns authorities tasks involving monitoring, awareness-raising, advisory activities, complaint handling, and cooperation, while also granting them investigative, corrective, and authorization powers (European Union, 2016). The regulatory architecture therefore combines preventive and reactive functions. Fines are only one of several possible responses and, by themselves, do not represent institutional performance.

This distinction is crucial for global comparisons. The variable “has a law” describes regulatory coverage; “has a supervisory authority” identifies an administrative structure; and “has effective capacity” requires evidence regarding resources, powers, and actual activities. Using the first variable as a substitute for the others produces false positives, while treating the absence of a

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

dedicated DPA as a complete absence of supervision overlooks sectoral or distributed supervisory models.

2.2 The Role of Data Protection Authorities

DPAs occupy an intermediate position between the abstract formulation of the law and its application to specific situations. They receive complaints, conduct investigations, issue guidance, assess high-risk data processing activities, cooperate with other authorities, and may impose corrective measures. The relevance of each function varies according to the applicable legal framework and regulatory strategy. Therefore, a list of competencies becomes analytically meaningful only when associated with the mechanisms through which the authority can exercise them.

The Turkish experience examined by Kinikoglu (2023) demonstrates that implementing a new law simultaneously requires enforcement and the development of societal capacity. Data controllers and processors need to understand their obligations, while data subjects need to be aware of their rights and available complaint mechanisms. The educational function is therefore not merely ancillary: it reduces uncertainty, helps prevent violations, and increases the ability to make use of data protection mechanisms.

On the coercive side, formal investigative or sanctioning powers are relevant, but they depend on procedures, specialized personnel, and the capacity to implement decisions. The literature on the GDPR further demonstrates that cross-border cases require coordination among national authorities. Bastos and Pałka (2023) identify limitations in the European *one-stop-shop* model in cases of common concern, demonstrating that the territorial distribution of competencies also affects substantive protection.

The assessment of the institutional role should therefore combine inputs, processes, outputs, and outcomes. Based on interviews, a survey of professionals, and data from regulatory authorities, Buckley, Caulfield, and Becker (2024) identified a mismatch between the broad objectives assigned to regulators and the narrow criteria, often focused on sanctions, used to evaluate them. The number of fines may provide information about coercive activity, but it does not, by itself, measure guidance, responses to complaints, prevention, regulatory learning, or behavioral change.

In the protocol adopted in this study, competencies are recorded according to functional groups: rulemaking and guidance; assistance and protection of rights; investigation; corrective measures and sanctions; authorization or prior consultation; education; domestic cooperation; and international cooperation. This classification makes it possible to compare the institutional design of authorities without assuming that all of them perform the same tasks or that the formal existence of a power indicates how frequently it is exercised.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

2.3 Independence and Institutional Models of DPAs

Independence is not a binary variable. Schütz (2012) demonstrates that formal independence can be assessed through legal attributes such as appointment, term of office, removal, competencies, and organizational autonomy. Kuner et al. (2012) further argue that the issue involves tensions between protection against external interference and legitimate mechanisms of *accountability*. An authority does not become independent merely because the law describes it as such.

Article 52 of the GDPR requires supervisory authorities to act with complete independence, free from external influence, and provides for adequate human, technical, and financial resources. The subsequent articles regulate the qualifications and appointment of members, terms of office, duties of confidentiality, tasks, and powers (European Union, 2016). These elements make it possible to break down formal independence into verifiable indicators, thereby avoiding classifications based solely on institutional designation.

Functional independence, in turn, depends on the actual ability to make decisions and take action. Dimitrova and De Hert (2024), in their examination of Belgium, France, and Germany, show that national restrictions on the exercise of indirect access in law enforcement matters may limit the activities of DPAs even within a legal framework that formally guarantees their independence. The analysis therefore shifts the focus from the mere existence of the authority to the actual scope of its competencies.

Resources constitute another important dimension. Puljak, Mladinić, and Koporc (2023) identified highly heterogeneous procedures, deadlines, and workloads among the 13 European authorities participating in their study. Maggetti et al. (2025) examine how the expansion of responsibilities can simultaneously empower and challenge supervisory authorities. Taken together, these studies suggest that autonomy without adequate budget, personnel, or technical capacity may be insufficient to fulfill the legal mandate.

The comparison must also consider the authority's position within the structure of the State. Collegiate bodies, autonomous agencies, commissions, ministerial units, and multisector regulators are subject to different chains of command, budgetary controls, and forms of accountability. An administrative affiliation does not prove interference, just as separate legal personality does not prove operational autonomy. Classification therefore requires evidence regarding institutional mechanisms rather than inferences based on organizational labels.

For this reason, this article distinguishes between formal independence, administrative and budgetary autonomy, operational capacity, and accountability. Formal independence is coded only when supported by a legal provision; administrative and budgetary autonomy and operational capacity require data on organizational arrangements and resources; and accountability encompasses reporting, judicial review, financial oversight, and relationships with Parliament or the

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

government. No single index is constructed when the available sources do not allow these dimensions to be compared consistently.

2.4 Comparative Studies and the Literature Gap

Existing comparative studies differ in their units of analysis. Greenleaf (2025a) examines the worldwide diffusion of data protection laws; Belli et al. (2023) compare innovation and legal interoperability across the BRICS countries; Puljak, Mladinić, and Koporc (2023) examine procedures and workloads; Sivan-Sevilla (2024) compares *enforcement* strategies; and Buckley, Caulfield, and Becker (2024) investigate regulatory objectives and indicators of effectiveness. These research agendas are complementary, but their findings cannot be aggregated as though they measured the same phenomenon.

Table 1 highlights the distinction between breadth and depth. Global inventories achieve broad coverage but focus primarily on legislation. Institutional studies examine more detailed variables but rely on regional scopes and smaller samples. The gap does not simply consist of there being “few studies”; rather, it lies in the absence of a synchronized global matrix that links, for each country, the status of the law, the supervisory arrangement, the degree of independence, and operational indicators using consistent criteria.

Table 1 - Comparison of the Main Studies Used

Study	Scope and Method	Contribution	Limitations for the Global Survey
Greenleaf (2025a, 2025b)	Global survey of national laws and their adoption timeline.	Assesses the expansion of the legal framework and preserves cutoff dates.	Does not constitute a census of authorities or institutional capacity.
Belli et al. (2023)	Legal and institutional comparison of the five original BRICS countries.	Highlights convergence and innovations beyond the European context.	Limited scope and not designed for the global classification of DPAs.
Puljak, Mladinić e Koporc (2023)	Cross-sectional study based on responses from 13 European DPAs.	Compares procedures, deadlines, and workloads.	Partial response and findings that cannot be generalized to the global context.
Sivan-Sevilla (2024)	Study involving 18 European DPAs, interviews, and secondary sources.	Relates enforcement strategies to institutional capacities and the political context.	Regional concentration and focus on *enforcement* strategies.
Buckley, Caulfield e Becker (2024)	Interviews, a survey of 70 professionals, and regulatory activity datasets.	Proposes dimensions for assessing performance and comparability.	Objectives and metrics remain controversial and centered on the GDPR.

Source: Prepared by the author based on the studies cited.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

2.5 Analytical Framework: Autonomy, Capacity, and Effectiveness

Institutional comparison becomes more coherent when organized as an analytical chain. The first link consists of formal safeguards: legal basis, administrative position, rules governing appointment and removal, term of office, incompatibilities, and prohibition of external instructions. The second comprises the means of action: budget, staffing, technical expertise, information systems, and access to expert knowledge. The third link encompasses regulatory strategy, that is, the combination of guidance, prevention, investigation, corrective measures, sanctions, and cooperation. Measurable outputs, such as decisions and guidance, constitute the fourth link; effects on compliance, risk reduction, and the exercise of rights comprise the fifth. Moving directly from the first to the last link attributes outcomes to legal form that also depend on resources, choices, and context.

Autonomy can be broken down into at least five components. Structural autonomy concerns organizational separation from the entities subject to supervision; decision-making autonomy refers to the absence of instructions regarding specific cases; personnel autonomy relates to safeguards applicable to the authority's leadership; financial autonomy concerns the predictability and management of resources; and informational autonomy refers to the ability to obtain documents, conduct inspections, and access specialized expertise. Schütz (2012) provides the basis for assessing formal independence, while the GDPR associates freedom from external influence with the availability of adequate human, technical, and financial resources (European Union, 2016). This decomposition prevents a single legal provision from being treated as sufficient to conclude the analysis.

Institutional capacity cannot be reduced to the size of the budget either. Raw figures must be considered in relation to the scope of the mandate, the population served, economic complexity, the volume of complaints, territorial coverage, and the existence of additional responsibilities. A small authority may operate adequately in a smaller jurisdiction, whereas a larger body may be overburdened by multisectoral responsibilities. The findings of Puljak, Mladinić, and Koporc (2023) and Maggetti et al. (2025) demonstrate that workload and the expansion of responsibilities affect the ability to translate formal competencies into regulatory action.

Effectiveness, finally, requires an explicit theory of contribution. Guidance may reduce uncertainty; accessible channels may facilitate the exercise of rights; inspections may reveal hidden practices; orders may halt unlawful processing; and sanctions may have a deterrent effect. These mechanisms are plausible, but their effects cannot be presumed simply by counting regulatory actions. Buckley, Caulfield, and Becker (2024) show that broad objectives coexist with narrow metrics and subjective assessments, which is why this study does not adopt fines as a single composite indicator of effectiveness.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

The integrated framework guides the interpretation of the 5W2H technique. *Who* and *Where* identify the authority and its relationships of dependence; *What* and *How* record its mandate, powers, and processes; *When* preserves the institutional sequence; *How much* describes resources and outputs; and *Why* makes the formal purpose explicit. The technique organizes evidence throughout the analytical chain, but it does not replace causal research design, outcome indicators, or longitudinal comparison.

3 - METODOLOGY

3.1 Research Design and Scope

This is an international documentary, descriptive, and comparative study, employing qualitative synthesis and making limited use of descriptive statistics already published by the sources. The inclusion of numerical counts does not transform the research design into an inferential quantitative study. The objective is to establish comparable criteria, identify institutional patterns, and explicitly indicate where the available evidence does not support classification or generalization.

The reference universe comprises the 193 Member States of the United Nations (United Nations, [n.d.]). Dependent territories, special administrative regions, and subnational authorities were not included as autonomous countries; when they appear in the databases consulted, they are recorded to explain differences in denominators. This decision avoids conflating the number of authorities with the number of States.

The primary unit of analysis is the country. The secondary unit of analysis is the institutional arrangement responsible for data protection supervision. A country may have more than one authority, and an authority may exercise only part of the relevant competencies. Therefore, the country–authority relationship is treated as potentially multiple rather than as a mandatory one-to-one correspondence.

3.2 Sources, Data Collection, and Verification

Data collection was conducted between August 9 and 18, 2026. The sources used included: the official list of United Nations Member States; Greenleaf's surveys published in 2025; UNCTAD's *Global Cyberlaw Tracker*; the Global Privacy Assembly (GPA) membership list, rules, and accreditation resolutions; legislation and official webpages concerning the institutional arrangements selected for exploratory application; European and international instruments; and scientific literature addressing functions, independence, resources, strategies, and performance. References from the original manuscript were retained only when their existence and relevance could be verified.

Each item of evidence preserves the source's cutoff date. The total of 172 laws refers to March 15, 2025; institutional webpages were accessed in August 2026; and academic studies use their respective data collection periods. These figures were not treated as representing a

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

simultaneous snapshot. Documents in Portuguese, English, and Spanish were reviewed directly; materials in other languages would only be used when an official version or a verifiable translation was available.

Verification follows a hierarchy: legislation and official documents; international organizations and regulatory authorities; peer-reviewed articles and academic books; specialized inventories; and, solely as an aid for locating information, secondary webpages. Divergences are recorded rather than resolved through averaging or an undisclosed preference for one source over another. A category is marked “not confirmed” when the available sources do not provide sufficient evidence to support a reliable determination.

3.3 Inclusion and Classification Criteria

Comprehensive legislation is defined as legislation that establishes general rules for the processing of personal data across multiple sectors, even if it contains exceptions. Exclusively sector-specific rules are recorded as partial coverage and are not automatically treated as equivalent to a comprehensive law. Draft bills and legislative proposals are kept separate from legislation that has been enacted and entered into force.

A DPA is defined as a public body to which a legal provision assigns, in an identifiable manner, responsibility for supervising data protection and at least some of the functions related to guidance, investigation, complaint handling, or the adoption of corrective measures. “Dedicated” means that data protection forms a core part of its mandate. Multisector regulators, ministries, and distributed structures are classified as alternative arrangements, without automatically implying that they are inferior.

Formal independence requires a legal basis addressing the absence of external instructions, appointment, term of office, removal, budget, or organizational autonomy. Functional independence is not presumed; it depends on evidence regarding the actual exercise of competencies. Statutory powers, available resources, and published outcomes are coded in separate fields.

Countries for which no dedicated national authority has been identified form a controlled residual category. This category does not mean “without any protection” and encompasses two situations that must be distinguished: supervision carried out through alternative institutional structures; or insufficient evidence to confirm the existence of an authority. This precaution prevents documentary silence from being interpreted as institutional absence.

3.4 Operationalization of the 5W2H Technique

The 5W2H technique is employed as a protocol for data collection, standardization, and comparison, rather than as a technique capable of demonstrating causality. The seven questions were translated into observable variables, as presented in Table 2. The *How much* field is assigned

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

values only when data on budget, personnel, complaints, investigations, or decisions are accompanied by an identifiable source, period, and unit of measurement.

The matrix distinguishes between the date of enactment of the law, the legal establishment of the authority, the beginning of its operations, and subsequent reforms. Likewise, it differentiates among the legal basis, institutional purpose, and policy rationales. The latter are not inferred unless supported by documentary evidence.

Table 2 - 5W2H Operationalization Matrix

Dimension	Variáveis observadas	Fonte preferencial	Regra de codificação
What	Comprehensive law; DPA; supervisory model; competencies.	Law, regulation, and official webpage.	Distinguish between normative, institutional, and operational existence.
Why	Legal purpose; protected rights; stated mandate.	Preamble, official explanatory documents, and founding act.	Do not attribute political motivations without documentary evidence.
Who	Name; legal nature; leadership; appointment process.	Founding act and official organizational chart.	Do not classify solely on the basis of the authority's designation.
Where	País; região; nível territorial; posição na estrutura estatal.	ONU, legislação e organograma.	Distinguir autoridade nacional, subnacional e setorial.
When	Country; region; territorial level; position within the State structure.	United Nations, legislation, and organizational chart.	Distinguish among national, subnational, and sectoral authorities.
How	Year of the law; establishment; commencement of operations; reform or dissolution.	Official gazette, legislation, and institutional reports.	Record dates separately and preserve the source's cutoff date.
How much	Governance; autonomy; powers; complaints; cooperation; *accountability*.	Legislation, regulations, reports, and academic literature.	Distinguish formal powers from their effectively documented exercise.

Fonte: Prepared by the author.

3.5 Analytical Procedure and Limitations

The analytical procedure consists of three stages. First, the global sources were compared in terms of their unit of analysis, cutoff date, and the phenomenon measured. Second, the literature and normative instruments were used to translate the 5W2H technique into observable fields and to construct the typology. Third, the rules were applied exploratorily to six contrasting institutional cases, selected based on variations in institutional design and the availability of official

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

documentation. The country-by-country census of the 193 States is specified as a subsequent stage and is not presented as a completed data collection process. Counts are reported only when the source clearly defines the universe and the applicable criteria; figures derived from different databases are neither added nor subtracted.

The study has relevant limitations. The original manuscript did not contain a country-by-country database, and the global sources consulted do not provide, within a single matrix, all the variables required for the analysis. Institutional changes may occur after the data collection period. Information on budgets, staffing, and regulatory activity has limited comparability. Consequently, the study presents confirmed global findings, classification criteria, and a typology, but does not claim to establish the exact worldwide frequency of each model or draw causal inferences.

3.6 Reliability, Auditability, and Updating

To ensure that the survey can be replicated, each record should retain the country, the authority's original name and its translation, legal basis, relevant legal provision, source address, document date, access date, supporting excerpt or page, the person responsible for coding, and verification status. A categorical value should never replace the evidence from which it was derived. This audit trail makes it possible to review classifications without losing their history and clearly distinguishes institutional absence from the absence of information.

Coding is conducted in two stages. The first identifies verifiable facts, such as enactment, establishment, commencement of operations, competencies, and administrative affiliation. The second interprets these facts according to the typology. Cases in which legislation, organizational charts, and institutional webpages diverge are flagged as conflicts and are not resolved through inference. In a census-based application, two researchers should independently code the critical fields and document the rationale underlying the consensus decision.

Temporal reliability requires clearly defined update events. The enactment of a new law, entry into force, establishment of the authority, transfer of competencies, changes to the appointment process, budgetary reform, and dissolution constitute distinct triggers. The date of the event and the date on which the source was accessed are kept separate, making it possible to reconstruct which classification was supported at any given point in time.

Table 3 consolidates rules for recurring situations. These rules prioritize caution: an enacted law is not automatically a law in force; an authority that has been legally established is not automatically operational; participation in an international network constitutes relevant institutional evidence but does not replace examination of the domestic legal instrument; and unpublished resource data remain unavailable rather than being assigned an estimated value.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Table 3 - Decision Rules and Quality Control

Observed Situation	Coding	Minimum Evidence	Risk Avoided
Law enacted but not yet fully in force.	Enacted; entry into force pending or phased.	Official text and entry-into-force provision.	Assuming regulatory coverage before it actually exists.
Authority established by law, without evidence of becoming operational	Legally established; operation not confirmed.	Establishment act, appointment, or evidence of active services.	Confusing legal existence with operational capacity.
More than one authority with relevant competencies	One-country/multiple-authorities relationship.	Provisions defining competencies and territorial level.	Counting authorities as countries or overlooking overlapping competencies.
International participation or accreditation	Supplementary evidence, with date and category.	Network membership list and resolution, together with a domestic source.	Treating membership as a universal census or as sufficient evidence on its own.
Budget, personnel, or activity data without a comparable period	Not reported or not comparable.	Official act and transition date.	Applying a historically valid classification to the present.
Reform, replacement, or dissolution	Close the previous version and create a new record.	Official act and transition date.	Applying a historically valid classification to the present.

Fonte: Prepared by the author.

4 - RESULTS

4.1 Legal Expansion and Non-Equivalence Across Inventories

The first confirmed finding is the widespread diffusion of data protection legislation. Greenleaf (2025a, 2025b) identifies 172 countries with privacy laws as of March 15, 2025. This figure demonstrates that legal protection has become widespread on a global scale, but it cannot be directly converted into a percentage of the 193 UN Member States because the inventory and the universe adopted in this article do not necessarily treat territories and jurisdictions in the same manner.

The second finding is both methodological and substantive: global inventories do not measure the same phenomenon. UNCTAD classifies 194 economies according to the status of different categories of digital legislation. The GPA, in turn, accredits authorities that meet its participation requirements and may include more than one authority from the same jurisdiction. Neither database, considered independently, constitutes a harmonized census of national DPAs.

This difference prevents the intuitive operation of subtracting the number of laws from the number of countries to determine “countries without a DPA,” or using the number of GPA members as equivalent to the number of countries with an authority. Table 4 summarizes what each source

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

does and does not allow researchers to conclude. This lack of comparability is not merely a technical detail: it affects the research findings and defines the limits of certainty of the classifications.

Recent institutional changes further reinforce this point. The accreditation resolution of the GPA's 47th Closed Session recorded new members, discussed aspects concerning the independence and autonomy of the Saudi authority, and reported the dissolution of Mexico's INAI in March 2025; Saudi Arabia's accreditation was subsequently confirmed in April 2026 following the submission of additional documentation and the absence of objections (*Global Privacy Assembly*, 2026). Institutional *status* is therefore time-dependent and may change without an immediate corresponding change in legislative inventories.

Table 4 – Scope and Limitations of Global Sources

United Nations	Unit and Date	What it Measure	What It Does Not Allow Researchers to Infer
United Nations	193 Member States; consulted in 2026.	Universo político de referência.	Political reference universe.
Greenleaf (2025a, 2025b)	Countries/jurisdictions; cutoff date: March 15, 2025.	Adoption and revision of national privacy laws.	Exact number of authorities, their independence, or performance.
UNCTAD – *Global Cyberlaw Tracker*	194 economies; dynamic database consulted in 2026.	Status of digital legislation, including data protection.	Direct correspondence with the 193 UN Member States or a census of DPAs.
GPA – Accredited Members	National, subnational, or sectoral authorities; dynamic list.	Authorities accepted under the GPA's participation rules.	All countries with a DPA, all authorities within each country, or the absence of supervision.

Source: Prepared by the author based on United Nations ([n.d.]), Greenleaf (2025a, 2025b), UNCTAD ([n.d.]), and Global Privacy Assembly ([n.d.], 2024, 2026).

4.2 Patterns Revealed by the 5W2H Matrix

The application of the *What* dimension demonstrated the need for three separate records: comprehensive legislation, supervisory authority, and set of competencies. The mere existence of a law does not determine whether a DPA exists; likewise, the existence of an authority does not indicate whether it is dedicated, multisectoral, or executive in nature. The survey must therefore preserve these responses in separate fields.

The *Who* and *Where* dimensions reveal a many-to-many relationship. Federal and decentralized systems may have both national and subnational authorities; certain sectors may be supervised by different bodies; and regional structures may coordinate domestic authorities. Therefore, the unit "authority" cannot automatically replace the unit "country."

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

REVISTA CIENTÍFICA SOL21
STANDARD OPEN LITERATURE - ISSN 3086-089X

The *When* dimension demonstrated that the enactment of legislation, the establishment of an authority, and the commencement of its operations are distinct events. The dissolution, replacement, or reform of an authority requires data versioning. The Mexican case documented by the GPA illustrates that a classification valid in one year may become inaccurate in the following year without the country ceasing to have data protection rules.

The *How much* dimension is the most incomplete. The literature identifies heterogeneous procedures and reporting practices, and several authorities do not publish comparable time series on budgets, staffing, or workloads (Puljak; Mladinić; Koporc, 2023; Buckley; Caulfield; Becker, 2024). The absence of standardized information should be treated as a finding concerning transparency and comparability rather than filled through estimation.

4.3 Proposed Institutional Typology

The data and the literature support seven analytical types. These are ideal types rather than an automatic hierarchy, and they may require dual coding when a country distributes competencies among different bodies. Classification depends on the predominant mechanism and should be accompanied by a note addressing any ambiguities.

The typology distinguishes among declared independence, institutional affiliation, and the distribution of competencies. This approach avoids classifying every specialized authority as "independent" or every country without a dedicated authority as having "no authority." Table 5 presents the classification criteria.

Table 5 – Typology of Supervision Arrangements

Type	Inclusion Criterion	Indicative Configuration	Analytical Caution
1. Independent and dedicated national DPA	Data protection as a core mandate and formal guarantees of independence.	Specialized authority, its own powers, and freedom from external instructions.	Confirm resources and functional independence; the legal designation alone is insufficient.
2. Dedicated DPA with significant executive affiliation	Specialized authority that is administratively embedded within or supervised by the Executive Branch.	Agency, commission, or unit with partial autonomy.	Administrative affiliation does not prove interference; examine appointment procedures, budget, and decision-making.
3. Collegiate commission or board	Decision-making authority assigned to a collegiate body with a data protection mandate.	National commission, council, or *board*.	The collegiate body may fall under Type 1 or Type 2 depending on its institutional safeguards.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Type	Inclusion Criterion	Indicative Configuration	Analytical Caution
4. Multisector regulator	Data protection forms part of a broader regulatory mandate.	Communications, consumer protection, information, or market regulator.	Verify whether the authority has specific powers concerning personal data.
5. Distributed, federal, or sectoral model	Competencies are divided according to territory, sector, or subject matter.	National and subnational authorities or multiple supervisory bodies.	Avoid counting authorities as countries and identify potential coordination gaps.
6. Executive or ministerial structure	Supervision is concentrated within a ministry or government unit without a dedicated DPA.	Department, secretariat, or central government administration.	Record oversight mechanisms, resources, and the ability to review the government's own activities.
7. No confirmed dedicated national authority	No dedicated authority has been identified, or the available evidence is insufficient.	Alternative or fragmented supervision, or lack of documentary evidence.	Do not interpret this category as the absence of legislation or of any protective mechanism.

Source: Prepared by the author based on Schütz (2012), Kuner et al. (2012), European Union (2016), Dimitrova and De Hert (2024), and Global Privacy Assembly (2024).

4.4 Characteristics Distinguishing Countries With and Without a Dedicated DPA

The first difference concerns the legal basis and institutional position. Countries with a dedicated DPA concentrate the mandate and organizational identity within a specialized authority, whereas alternative models distribute functions among bodies whose primary responsibilities may involve consumer protection, communications, security, information, or public administration. This concentration may facilitate specialization and institutional visibility, but it does not, by itself, guarantee independence or performance.

The second difference concerns governance. Appointment procedures, length of terms of office, grounds for removal, incompatibility rules, and prohibitions on external instructions may reduce or increase exposure to external pressures. The discussion documented during the GPA accreditation process of the Saudi authority demonstrates that autonomy and independence require documentary examination, even when an institution already performs data protection functions (*Global Privacy Assembly*, 2026).

The third difference involves resources. A dedicated budget, technical personnel, access to specialists, and adequate infrastructure determine whether formal competencies can effectively be exercised. Authorities with broad responsibilities and stable resources operate under different conditions from small ministerial units or multisector regulators that must allocate their capacity

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

across several mandates. The expansion of responsibilities may increase an authority's influence while simultaneously placing additional strain on the organization (Maggetti et al., 2025).

The fourth difference lies in powers and access for data subjects. The ability to request information, conduct audits, issue orders, impose sanctions, suspend processing activities, and bring matters before the courts increases the authority's capacity to respond. Free complaint channels, defined deadlines, procedural transparency, and the availability of appeals make these powers more accessible to data subjects. Specific legal limitations may weaken protection even where authorities are formally independent (Dimitrova; De Hert, 2024).

The fifth difference concerns coordination. Distributed models require clear rules regarding jurisdiction, information sharing, and conflicts of competence. Under the GDPR, cross-border cooperation seeks to reduce fragmentation, although the literature identifies difficulties with this arrangement in complex cases (Bastos; Pałka, 2023). In countries without a dedicated DPA, coordination among sectoral regulators may perform part of this function, provided that responsibilities and referral mechanisms are clearly identifiable.

The sixth difference is accountability. Public reports, regulatory activity data, financial oversight compatible with institutional independence, judicial review, and engagement with Parliament or civil society make it possible to assess the authority's activities. The absence of standardized metrics prevents simple rankings; nevertheless, the consistent publication of definitions, data series, and decisions improves comparability and reduces reliance on narrow indicators such as the monetary value of fines (Buckley; Caulfield; Becker, 2024).

4.5 Exploratory Application to Contrasting Institutional Arrangements

To determine whether the categories distinguish real-world configurations, the protocol was applied exploratorily to cases selected for maximum institutional variation and the availability of official documentation. This exercise does not constitute a representative sample or a census; its purpose is to test the consistency of the rules, identify fields that require dual coding, and demonstrate why the name of an institution alone is insufficient for classification.

The GDPR provides the most explicit normative benchmark. It requires one or more independent public authorities in each Member State, defines their tasks and powers, and establishes cooperation mechanisms for cross-border processing activities (European Union, 2016). Modernized Convention 108 extends beyond the European Union the requirement for supervisory authorities with investigative and intervention powers that act independently and impartially (Council of Europe, 2018). These instruments provide a reference framework, but they do not justify assuming that every DPA worldwide follows the same institutional design.

Brazil and the Philippines illustrate dedicated authorities with distinct institutional configurations. In Brazil, Law No. 14,460/2022 transformed the ANPD into a special-status autonomous agency, endowed with technical and decision-making autonomy while preserving its

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

statutory competencies (Brazil, 2022). In the Philippines, the *National Privacy Commission* describes itself as an independent body and performs rulemaking, advisory, educational, monitoring, investigative, adjudicatory, and enforcement functions (Philippines, [n.d.]). The concentration of the data protection mandate is common to both cases; their governance structures, safeguards, and institutional trajectories remain separate variables.

India demonstrates the importance of decomposing the *When* dimension. The 2023 law provided for the *Data Protection Board*; on November 13, 2025, the Central Government formally established the body and brought into force the provisions concerning its organization. The legislation provides for the Board to function as an independent body with a digital-by-design structure, while also providing for the appointment of its Chairperson and Members by the Central Government, a two-year term of office, and prior government approval for the appointment of staff (India, 2023, 2025a, 2025b). Appropriate coding simultaneously records its collegiate structure, declared autonomy, and institutional affiliation mechanisms without converting these characteristics into an automatic judgment regarding performance.

Australia and China demonstrate why the category “without a dedicated DPA” cannot be interpreted as the absence of supervision. The *Office of the Australian Information Commissioner* is an independent statutory agency that combines privacy protection, access to information, and other regulatory functions, placing it closer to the multisector regulator type (Australia, 2025). Chinese law, in turn, dedicates a chapter to departments responsible for personal information protection and distributes responsibilities between the national cyberspace administration and other competent departments, a configuration more closely aligned with distributed executive supervision (China, 2021). In both cases, institutions and powers exist; what differs is the concentration of the mandate and the authority’s position within the State structure.

Mexico demonstrates that classifications must be versioned over time. The GPA resolution recorded the dissolution of INAI in March 2025, while the federal decree issued during the same period enacted new transparency and data protection laws and reorganized institutional responsibilities (*Global Privacy Assembly*, 2026; Mexico, 2025). It would be methodologically inappropriate either to retain indefinitely the classification assigned to the dissolved authority or to conclude, solely on the basis of its dissolution, that all protective mechanisms had disappeared. The case requires a new record containing the transition date and identifying the successor competencies.

The comparison confirms three descriptive propositions. First, “dedicated,” “independent,” and “collegiate” are attributes that may coexist rather than mutually exclusive categories. Second, a multisector regulator or distributed arrangement may possess substantial competencies, although it faces different challenges concerning prioritization and coordination. Third, classifications are time-dependent: legal establishment, commencement of operations, reform, and dissolution affect

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

different 5W2H responses. Table 6 summarizes the exploratory application without ranking the cases by quality.

Table 6 - Exploratory Application of the Protocol to Contrasting Cases

Case and Evidence	5W2H Summary	Provisional Type	Interpretive Caution
Brazil – Law No. 14,460/2022	Dedicated ANPD; special-status autonomous agency; formal technical and decision-making autonomy.	1 – Independent and dedicated DPA	The legal structure should be complemented by evidence on resources, decision-making practices, and accountability.
Philippines – NPC official webpage	Independent, collegiate, and dedicated commission; preventive, adjudicatory, and enforcement functions.	1 and 3 – Dedicated/collegiate DPA.	Confirm the institutional structure, resources, and exercise of competencies through official acts and reports.
India – 2023 law and 2025 acts	*Collegiate and digital Board; formally declared independence; appointments and staffing linked to the Central Government.*	2 and 3 – DPA with executive affiliation/collegiate structure.	Distinguish legal establishment, phased entry into force, and observed operational capacity.
Australia - OAIC	Independent statutory agency; privacy combined with access to information and other mandates.	4 – Multisector regulator.	A multiple mandate does not imply weaker protection; prioritization and resource allocation must be examined.
China – 2021 PIPL	Responsibilities assigned to the national cyberspace administration and other competent departments.	5 and 6 – Distributed/executive model.	A multiple mandate does not imply weaker protection; prioritization and resource allocation must be examined.
Mexico – 2025 reform	Dissolution of INAI and legal reorganization of responsibilities.	Record in transition; recoding required.	Do not carry forward the classification of the dissolved authority or infer a regulatory vacuum without identifying successor bodies.

Source: Prepared by the author based on Brazil (2022), Philippines ([n.d.]), India (2023, 2025a, 2025b), Australia (2025), China (2021), Mexico (2025), European Union (2016), and Global Privacy Assembly (2026).

4.6 Confirmed Findings and the Boundaries of the Evidence

The survey confirms: the expansion to 172 countries with data protection laws by March 2025; the coexistence of different units and criteria across global databases; the inadequacy of a binary classification; and the usefulness of the 5W2H dimensions for distinguishing institutional

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

design, position, chronology, capacity, and outcomes. The exploratory application further confirms that the seven types must accommodate combined attributes, temporal transitions, and cautionary notes rather than functioning as rigid labels.

Without a synchronized country-by-country database, it was not possible to confirm the exact number of Member States with a dedicated DPA, the worldwide frequency of each type, or causal relationships between institutional models and effectiveness. Presenting such figures would go beyond the available evidence. The protocol identifies precisely the fields that need to be completed so that a subsequent census-based stage can produce auditable counts.

5 - DISCUSSION

5.1 From Dichotomy to Layered Analysis

The findings demonstrate that the question “does the country have a DPA?” needs to be broken down into multiple layers. The first is normative: is there comprehensive legislation, and what is its scope? The second is organizational: who is responsible for supervision, and where is that body positioned within the institutional structure? The third is functional: what powers, resources, and procedures are available? The fourth is empirical: what activities and effects can be observed? Affirmative answers at the initial levels do not guarantee affirmative answers at the subsequent ones.

This interpretation explains why the diffusion of laws observed by Greenleaf (2025a) does not automatically produce institutional convergence. Countries may adopt similar principles while developing different forms of implementation and enforcement. The contribution of the BRICS studies lies precisely in demonstrating that normative convergence can coexist with institutional innovation and different institutional trajectories (Belli et al., 2023).

The typology also avoids equating alternative arrangements with institutional deficiencies. Multisector or distributed regulators may bring together relevant expertise, institutional reach, and regulatory instruments. However, they need to make competencies, priorities, coordination mechanisms, and conflict-prevention measures transparent. The absence of a dedicated authority is analytically significant because it changes the concentration of the mandate, not because it proves the absence of protection.

Conversely, establishing a DPA does not eliminate capacity-related challenges. If the authority lacks personnel, budget, access to information, or enforceable powers, its formal independence may result in limited protection. This finding is consistent with the literature distinguishing legal attributes, institutional practices, and resources (Schütz, 2012; Puljak; Mladinić; Koporc, 2023; Dimitrova; De Hert, 2024).

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

5.2 Independence, Capacity, and Accountability

Independence protects decision-making from undue interference, but it does not imply the absence of oversight. A separate budget, fixed terms of office, and restricted grounds for removal may coexist with financial audits, publication of reports, and judicial review. The comparative challenge is to distinguish *accountability* mechanisms that are compatible with autonomy from mechanisms that allow political direction over specific cases.

The analysis of powers should follow the same logic. Legal authority to investigate or impose sanctions is an institutional condition; the number of fines is an output; and the protection of data subjects is a broader outcome. Conflating these categories leads to superficial assessments. Buckley, Caulfield, and Becker (2024) demonstrate that perceptions of effectiveness are subjective and frequently focused on sanctions, even though regulators pursue broader objectives.

Data on complaints and decisions also require appropriate denominators. A high volume may indicate accessibility, workload, a higher incidence of violations, or different reporting practices. Without information on population, period, scope, and procedures, comparisons cannot support reliable inferences about performance. The *How much* field should therefore preserve metadata and allow for missing values.

Institutional design should thus be assessed through a balanced set of dimensions: independence safeguards; resources; powers; accessibility; transparency; coordination; and oversight mechanisms. No single variable provides a basis for universally ranking supervisory authorities.

5.3 Implications for the Global Survey

A future census should publish the country-by-country matrix, the decision rules, and the version history. Each row should identify the primary source and its date, and every change should preserve the previous value. This architecture makes it possible to audit complex cases and update records concerning dissolutions, reforms, or the commencement of operations without retrospectively rewriting the database.

The classification should accommodate multiple authorities and overlapping competencies. For regional comparisons, the denominator should be the number of States within the reference universe, rather than the number of authorities. For organizational comparisons, the authority itself may serve as the unit of analysis, provided that the results are not subsequently converted into country-level figures. Transparency regarding the unit of analysis prevents the principal error identified across the inventories.

Ambiguous cases should be assigned a provisional category rather than being subjected to a forced classification. GPA accreditation documentation demonstrates that criteria concerning autonomy may require clarification and subsequent updating. From a scientific perspective,

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

documenting uncertainty is more informative than reducing complex institutional phenomena to a simple “yes” or “no.”

5.4 Limitations and Research Agenda

This study does not replace primary data collection covering all 193 countries. Its global empirical findings are limited to published and comparable indicators, and the proposed typology still needs to be applied and tested on a case-by-case basis. Institutional dynamics, language barriers, and the scarcity of operational data may result in provisional classifications.

The next stage should combine independent double coding, a protocol for resolving disagreements, and validation through official sources. Data on budgets, staffing, and workloads require time series, documented currency conversion procedures, and standardized definitions. Only after these steps will it be possible to estimate the distribution of the different types and test associations between institutional design and outcomes.

Nevertheless, these limitations do not diminish the study’s contribution. By identifying what can be stated, what cannot be inferred, and which variables remain unavailable, the 5W2H framework transforms the absence of data into methodological information and provides a verifiable pathway for further developing the global survey.

5.5 Institutional Implications and Propositions for Future Research

For countries considering the establishment of a dedicated DPA, the decision should not be limited to the choice of legal form. It is necessary to define the coordination problem that the new authority is intended to address, which sectors and processing activities will fall within its scope, how overlapping competencies will be managed, and what resources will accompany the mandate. Centralization may promote specialization, a clear public identity, and a single point of contact for data subjects; it may also create bottlenecks if broad responsibilities are concentrated without proportional institutional capacity.

For existing authorities, the assessment should cover the entire analytical chain. Safeguards concerning appointment and removal protect decision-making; budget and staffing enable action; powers and procedures structure regulatory responses; and transparency and review mechanisms make the authority’s activities subject to oversight. Reforming only one link in this chain may shift the problem rather than resolve it. Brazil’s transition to a special-status autonomous agency, India’s collegiate model, and Australia’s multisector mandate demonstrate that formal changes need to be accompanied by continuous assessment of how institutional mechanisms operate in practice.

The publication of a minimum dataset would improve comparability without imposing a universal *ranking*. This core dataset should include executed budget, staffing by function, complaints received and closed, processing times by case category, ex officio investigations, guidance, orders,

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

sanctions, appeals, and judicial outcomes. Each indicator should specify its period, denominator, definition, coverage, and any breaks in the time series. Aggregated data should neither expose data subjects nor compromise ongoing investigations.

The framework makes it possible to formulate testable propositions that have not yet been demonstrated by this study. P1: formal guarantees of independence will be more consistently associated with autonomous decision-making when accompanied by financial and informational autonomy. P2: the expansion of responsibilities will increase regulatory outputs only until staffing and infrastructure become constraining factors. P3: distributed arrangements will achieve greater coherence when public rules governing competencies, referrals, and information sharing are in place. P4: accessible complaint mechanisms will increase observed demand, meaning that a higher number of cases should not automatically be interpreted as evidence of weaker protection.

Testing these propositions requires longitudinal panel data and a comparative strategy that controls for legal, economic, and political context. Paired case studies may investigate mechanisms; configurational analyses may identify sufficient or necessary combinations of conditions; and regulatory activity time series may examine changes following institutional reforms. The 5W2H framework provides the descriptive infrastructure for case selection and variable construction, but inference requires an additional research design.

6 - CONCLUSIONS

The study examined how to organize a global survey of DPAs and alternative supervisory arrangements using the 5W2H framework. The evidence confirms the widespread diffusion of privacy laws, with 172 countries identified as of March 2025, but does not support treating this figure as the number of supervisory authorities. Global databases use different units, dates, and criteria; moreover, a country may have multiple authorities, while a single authority may exercise only a partial mandate. The theoretical analysis and exploratory application to contrasting institutional arrangements demonstrate that the most discriminating characteristics are the legal basis and institutional position, appointment and removal procedures, decision-making and budgetary autonomy, human resources, powers, access mechanisms for data subjects, coordination, and accountability. Countries without a dedicated DPA may adopt executive, multisectoral, or distributed supervisory arrangements, while countries with a DPA may combine collegiate structures, executive affiliation, and safeguards of autonomy to varying degrees.

The study's main contribution is a comparable, auditable, and updatable protocol, accompanied by a typology of seven supervisory arrangements that distinguishes legislation, organization, capacity, outputs, and outcomes. The study does not establish the exact worldwide number of DPAs or the frequency of each type because neither the original manuscript nor the sources consulted contain a synchronized matrix covering all 193 UN Member States. This limitation prevents rankings and causal inferences, but it defines a clear research agenda: country-by-country

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

data collection, independent double coding, documented resolution of disagreements, institutional versioning, and standardization of resource and activity indicators. The 5W2H framework is useful as a structure for data collection and auditing; explaining effectiveness requires longitudinal data and a complementary causal research design.

REFERENCES

AUSTRÁLIA. Office of the Australian Information Commissioner. *What we do*. Canberra, 26 maio 2025. Disponível em: https://www.oaic.gov.au/about-the-OAIC/what-we-do. Acesso em: 16 ago. 2026.

BASTOS, Filipe Brito; PAŁKA, Przemysław. Is centralised General Data Protection Regulation enforcement a constitutional necessity? *European Constitutional Law Review*, Cambridge, v. 19, n. 3, p. 487-517, 2023. DOI: https://doi.org/10.1017/S1574019623000202.

BELLI, Luca et al. Data protection in the BRICS countries: legal interoperability through innovative practices and convergence. *International Data Privacy Law*, Oxford, v. 13, n. 1, p. 1-24, 2023. DOI: https://doi.org/10.1093/idpl/ipac019.

BRASIL. Lei nº 14.460, de 25 de outubro de 2022. Transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e altera a legislação correlata. *Diário Oficial da União*: seção 1, Brasília, DF, 26 out. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14460.htm. Acesso em: 21 ago. 2026.

BUCKLEY, Gerard; CAULFIELD, Tristan; BECKER, Ingolf. GDPR and the indefinable effectiveness of privacy regulators: can performance assessment be improved? *Journal of Cybersecurity*, Oxford, v. 10, n. 1, tyae017, 2024. DOI: https://doi.org/10.1093/cybsec/tyae017.

BYGRAVE, Lee A. *Data privacy law: an international perspective*. Oxford: Oxford University Press, 2014. DOI: https://doi.org/10.1093/acprof:oso/9780199675555.001.0001.

CHINA. *Personal Information Protection Law of the People's Republic of China*. Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress, 20 ago. 2021. Beijing, 2021. Disponível em: https://www.npc.gov.cn/npc/c2597/c5854/bfflywwb/202311/t20231117_433007.html. Acesso em: 17 ago. 2026.

CONSELHO DA EUROPA. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)*. Strasbourg, 28 jan. 1981. Disponível em: https://rm.coe.int/1680078b37. Acesso em: 18 ago. 2026.

CONSELHO DA EUROPA. *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223)*. Strasbourg, 10 out. 2018. Disponível em: https://rm.coe.int/16808ac918. Acesso em: 19 ago. 2026.

DIMITROVA, Diana; DE HERT, Paul. DPA independence and 'indirect' access - illusory in Belgium, France and Germany? *Maastricht Journal of European and Comparative Law*, [s. l.], v. 31, n. 1, p. 82-105, 2024. DOI: https://doi.org/10.1177/1023263X241237688.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

FILIPINAS. National Privacy Commission. *Powers & functions*. Quezon City, [s. d.]. Disponível em: https://privacy.gov.ph/powers-functions/. Acesso em: 21 ago. 2026.

GLOBAL PRIVACY ASSEMBLY. *GPA Rules and Procedures*. Consolidated version, nov. 2024. Disponível em: https://globalprivacyassembly.com/wp-content/uploads/2024/12/GPA-Rules-and-Procedures-November-2024-amended.pdf. Acesso em: 20 ago. 2026.

GLOBAL PRIVACY ASSEMBLY. *List of accredited members*. [S. l.], [s. d.]. Disponível em: https://globalprivacyassembly.com/participation-in-the-assembly/list-of-accredited-members/. Acesso em: 18 ago. 2026.

GLOBAL PRIVACY ASSEMBLY. *47th Closed Session of the Global Privacy Assembly: Accreditation Resolution*. 19 set. 2025, atualização de 9 abr. 2026. [S. l.], 2026. Disponível em: https://globalprivacyassembly.com/wp-content/uploads/2026/06/47th-GPA-Accreditation-Resolution.pdf. Acesso em: 19 ago. 2026.

GREENLEAF, Graham. Global data privacy laws 2025: 172 countries, 12 new in 2023/24. *Privacy Laws & Business International Report*, [s. l.], n. 194, p. 1, 3-9, 2025a. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5275559. Acesso em: 18 ago. 2026.

GREENLEAF, Graham. 172 countries with data privacy laws - year by year 1973-2025. *Privacy Laws & Business International Report*, [s. l.], n. 195, p. 16-17, 2025b. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5189972. Acesso em: 17 ago. 2026.

ÍNDIA. *The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)*. New Delhi, 11 ago. 2023. Disponível em: https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf. Acesso em: 19 ago. 2026.

ÍNDIA. Ministry of Electronics and Information Technology. Notification G.S.R. 844(E), 13 November 2025: establishment of the Data Protection Board of India. *The Gazette of India: Extraordinary*, New Delhi, Part II, Section 3(i), n. 758, 13 nov. 2025a. Disponível em: https://www.meity.gov.in/static/uploads/2025/11/cc217843dc3bcb37b2b05bcc3b4e031f.pdf. Acesso em: 21 ago. 2026.

ÍNDIA. Press Information Bureau. *Government notifies DPDP Rules to empower citizens and protect privacy*. New Delhi, 14 nov. 2025b. Disponível em: https://pib.gov.in/PressReleasePage.aspx?PRID=2190014. Acesso em: 18 ago. 2026.

KINIKOGLU, Batu. Implementing a new data protection law: lessons from the Turkish experience. *International Data Privacy Law*, Oxford, v. 13, n. 1, p. 25-46, 2023. DOI: https://doi.org/10.1093/idpl/ipad001.

KUNER, Christopher. *Transborder data flows and data privacy law*. Oxford: Oxford University Press, 2013. DOI: https://doi.org/10.1093/acprof:oso/9780199674619.001.0001.

KUNER, Christopher; CATE, Fred H.; MILLARD, Christopher; SVANTESSON, Dan Jerker B. The intricacies of independence. *International Data Privacy Law*, Oxford, v. 2, n. 1, p. 1-2, 2012. DOI: https://doi.org/10.1093/idpl/ipr021.

MAGGETTI, Martino; SALIHI, Blerta; PAGLIARIN, Edoardo; VAGIONAKI, Thenia. Empowered but challenged: the impact of task expansion on data protection authorities. *Policy & Internet*, [s. l.], v. 17, e70001, 2025. DOI: https://doi.org/10.1002/poi3.70001.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

MÉXICO. Decreto por el que se expiden la Ley General de Transparencia y Acceso a la Información Pública; la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; y se reforma el artículo 37, fracción XV, de la Ley Orgánica de la Administración Pública Federal. *Diario Oficial de la Federación*, Ciudad de México, 20 mar. 2025. Disponível em: https://dof.gob.mx/index_113.php?day=20&month=03&year=2025. Acesso em: 18 ago. 2026.

NAÇÕES UNIDAS. *Member States*. New York, [s. d.]. Disponível em: https://www.un.org/en/about-us/member-states. Acesso em: 19 ago. 2026.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD, 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 19 ago. 2026.

PULJAK, Livia; MLADINIĆ, Anamarija; KOPORC, Zvonimir. Workload and procedures used by European data protection authorities related to personal data protection: a cross-sectional study. *BMC Research Notes*, London, v. 16, art. 41, 2023. DOI: https://doi.org/10.1186/s13104-023-06308-z.

SCHÜTZ, Philip. Assessing formal independence of data protection authorities in a comparative perspective. In: CAMENISCH, Jan et al. (ed.). *Privacy and Identity Management for Life*. Berlin: Springer, 2012. p. 45-58. DOI: https://doi.org/10.1007/978-3-642-31668-5_4.

SIVAN-SEVILLA, Ido. Varieties of enforcement strategies post-GDPR: a fuzzy-set qualitative comparative analysis (fsQCA) across data protection authorities. *Journal of European Public Policy*, [s. l.], v. 31, n. 2, p. 552-585, 2024. DOI: https://doi.org/10.1080/13501763.2022.2147578.

UNIÃO EUROPEIA. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. *Official Journal of the European Communities*, Luxembourg, L 281, p. 31-50, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046. Acesso em: 21 ago. 2026.

UNIÃO EUROPEIA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. *Official Journal of the European Union*, Luxembourg, L 119, p. 1-88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 21 ago. 2026.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. *Global Cyberlaw Tracker*. Geneva: UNCTAD, [s. d.]. Disponível em: https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide. Acesso em: 19 ago. 2026.

This article is published in open access under the Creative Commons Attribution 4.0 International License (CC-BY), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.