Telecommunications Policy 50 (2026) 103266

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

Balancing privacy and public interest: ethical and legal aspects

Veronika Horielova [a,*], Olena Derevianko [b], Oleksii Yanushevskyi [c], Maksym Lysak [d]

[a] Department of State Law and Humanities, Educational and Scientific Institute of Humanities, V.I. Vernadsky Taurida National University, 33 John McCain Str., 01042, Kyiv, Ukraine
[b] Department of Advertising and Public Relations, Taras Shevchenko National University of Kyiv, 60 Volodymyrska Str., 01601, Kyiv, Ukraine
[c] Kyiv University of Intellectual Property and Law, 210 Kharkivske Road, 02121, Kyiv, Ukraine
[d] "KROK" University, 30-32 Tabirna Str., 03113, Kyiv, Ukraine

ARTICLE INFO

Keywords:
Data governance
Digital rights
Algorithmic accountability
Digital ethics
Ethical governance

ABSTRACT

Against the backdrop of rapid digital transformation and the proliferation of data-driven technologies, the tension between personal data privacy and the public interest has become increasingly complex and inadequately addressed by existing regulatory frameworks. Although modern legal regimes, including the GDPR, provide advanced data protection mechanisms, they remain predominantly focused on procedural compliance and offer limited instruments for evaluating the ethical legitimacy of data-processing practices. This study develops an integrated ethical-legal approach to personal data governance by combining doctrinal legal analysis with ethical reasoning. The methodology is based on a comparative examination of major regulatory regimes (GDPR, PIPL, LGPD, and CCPA), analysis of the case law of the European Court of Human Rights, and synthesis of contemporary legal and ethical theories. The study demonstrates that formally lawful data-processing practices may remain ethically problematic, particularly in the contexts of algorithmic decision-making, workplace monitoring, biometric surveillance, and transnational data flows. The comparative analysis reveals that existing regulatory models differ significantly in their underlying value orientations but none provides a comprehensive mechanism for assessing the substantive legitimacy of data processing beyond formal legal compliance. Based on these findings, the study identifies five interrelated criteria for evaluating the legitimacy of personal data processing—legitimacy of purpose, proportionality, transparency, accountability, and data-subject participation—and operationalises them within a structured assessment framework. The article further advances the theoretical debate by introducing the concept of digital solidarity as a normative principle that complements individual rights with collective responsibility in digital ecosystems. The findings contribute to existing scholarship by shifting the focus from procedural legality towards substantive ethical legitimacy and by providing an operational model applicable to regulatory analysis, ethical auditing, and digital governance policymaking.

* Corresponding author.
E-mail addresses: gorielova.veronika@tnu.edu.ua (V. Horielova), olena.derevianko@knu.ua (O. Derevianko), yanushevskyi_oleksii@edu-iosa.org (O. Yanushevskyi), LysakMY@krok.edu.ua (M. Lysak).

https://doi.org/10.1016/j.telpol.2026.103266
Received 27 January 2026; Received in revised form 4 June 2026; Accepted 7 June 2026
Available online 13 June 2026

1. Introduction

1.1. Rethinking privacy: Bridging legal norms and ethical imperatives

The rapid digital transformation and deep globalisation of information flows are radically changing the nature of the interaction between individuals, the state and technology. Personal data, once seen as a purely private resource, has become a central asset for social, economic and political development. In an environment where artificial intelligence, algorithmic control and the Internet of Things provide unprecedented opportunities to collect, analyse and disseminate information about people, the issue of privacy protection is gaining not only a legal but also a moral dimension. Despite the regulatory strengthening of digital rights - in particular, in the form of the General Data Protection Regulation (GDPR) - existing legal models remain fragmented, formalised and increasingly unable to adequately respond to the dynamics of moral challenges. Ukraine's ongoing alignment of its data protection standards with those of the EU in the context of digital governance reforms, once again highlights the practical relevance of these challenges in a transitional regulatory environment. Verkhovna Rada of Ukraine (2010) confirms the relevance of the issues raised in the article, especially in light of the challenges of harmonising digital legislation with ethical principles. The topicality of these challenges is borne out by empirical trends in the global data economy. According to the latest estimates, the total volume of data generated worldwide is expected to exceed 180 zettabytes by 2025, reflecting the exponential growth of digital information flows. At the same time, the economic value of data-driven markets continues to grow rapidly, and data-related activities make a significant contribution to global GDP.

Recent empirical data once again highlights the urgency of addressing the ethical and legal challenges surrounding the management of personal data. According to the IBM Cost of a Data Breach Report for 2025, the global average cost of a data breach remains above US$4.5 million per incident, whilst the critical infrastructure and healthcare sectors continue to suffer some of the highest losses associated with cyber incidents (IBM Cost of a Data Breach Report, 2025). At the same time, the OECD (2026) and UNCTAD (2025) report on the continuous expansion of cross-border data flows, which have become a key driver of the digital economy but also create growing regulatory and jurisdictional challenges regarding privacy protection. The rapid spread of artificial intelligence further exacerbates these concerns. Recent assessments indicate that AI-based systems are used in the fields of employment, finance, healthcare, public administration and law enforcement, often relying on the large-scale processing of personal data and automated decision-making. These developments demonstrate that contemporary privacy issues are no longer confined to individual legal disputes but constitute a systemic problem affecting economic security, democratic governance and fundamental rights on a global scale.

Alongside this expansion, the risks associated with the processing of personal data are increasing (Sposato et al., 2026). Reports point to a steady rise in large-scale data breaches and algorithmic decision-making systems that affect access to employment, credit and public services. The growing reliance on automated systems in both the public and private sectors highlights a structural imbalance between technological capabilities and the existing regulatory frameworks designed to govern them. These developments demonstrate that the tension between privacy and the public interest is not merely theoretical, but is grounded in measurable socio-economic transformations, thereby underscoring the need for a more integrated ethical and legal approach. This article proceeds from the conviction that the fundamental tension between the right to privacy and public interests should not be viewed as a conflict requiring compromise, but rather as a point of departure for shaping a new normative paradigm. At its core, this paradigm must rest not only on legal appropriateness but also on ethical justification. Law without ethics risks becoming a technocratic instrument that ensures only procedural legitimacy, while overlooking dignity, autonomy, and responsibility as central elements of digital existence. Ethics, on the contrary, provides contextual sensitivity and value orientation, which allows assessing not only the permissibility but also the legitimacy of interventions in the field of personalised information.

The central thesis of this study is the justification for developing an integrated ethical-legal model that not only aligns regulatory standards with moral imperatives, but also provides a critical framework for evaluating decisions concerning the dissemination of personal data. This model aims to transform the dominant approach from reactive regulation to proactive responsibility, where ethical analysis is not a secondary but a primary tool for assessing digital practices. The purpose of this article is to develop a conceptual model that strikes a balance between the digital rights of an individual and the legitimate needs of society. To this end, the study undertakes: first, a comparative analysis of key legal regimes and judicial practices; second, a systematisation of fundamental ethical principles relevant to the domain of data; third, a reconstruction of typical ethical conflicts within the sphere of legal application; and finally, the development of analytical criteria for determining the boundaries of the lawful dissemination of personal information.

What is most important is that this study views the balance between privacy and public interests not as a binary opposition that must be resolved in favour of one value over the other, but as a structurally recurring tension that manifests itself in different ways across various regulatory models, judicial contexts and technological environments. Each component of the proposed model is designed to operationalise this balance in specific decision-making situations, offering an answer to the specific question of when and under what conditions an intrusion into privacy in the name of public interests can be considered not merely lawful, but truly justified.

1.2. Problem statement

Despite significant efforts by the international community to formalise personal data protection standards, the current legal framework reveals three specific and interrelated shortcomings that existing research has not adequately addressed. Firstly, regulatory documents such as the GDPR, PIPL, LGPD and CCPA establish the legal bases for data processing, including consent, legitimate interest and public interest, but do not provide a structured mechanism for assessing whether a particular processing practice is substantially justified from an ethical standpoint. The consequence of this is the well-documented compliance paradox: organisations can meet all

the formal requirements of the GDPR whilst simultaneously deploying algorithmic systems that lead to discriminatory outcomes or undermine user autonomy. The case of automated systems for credit scoring and determining eligibility for benefits illustrates this directly as practices that are formally lawful but produce outcomes that a reasonable ethical analysis would reject. Existing legal scholarship documents this contradiction (Arrieta et al., 2020; Dhirani et al., 2023) but does not provide an operational basis for resolving it.

Secondly, it is empirically shown that the principle of informed consent functions as a mechanism of legitimisation rather than as a genuine exercise of autonomy. Research into 'cookie fatigue' (Banks, 2025), the structural asymmetry between data subjects and controllers (Sampson, 2021) and the opacity of algorithmic profiling (Dhirani et al., 2023) consistently demonstrates that consent, in its current form, does not meet the ethical conditions it is intended to embody. However, neither legal nor ethical literature has produced an effective alternative assessment criterion that regulators and auditors could apply in practice. Proposals range from contextual integrity (Nissenbaum, 2004) to models of collective governance, but they remain largely theoretical and have not been translated into regulatory instruments.

Thirdly, the concept of public interest lacks any agreed ethical threshold. As demonstrated by the ECtHR's judgment in the case of S. and Marper v. the United Kingdom (2008), states regularly invoke security and public order to justify data-processing practices which the Court ultimately found to be disproportionate. However, no existing framework, whether legal or ethical, defines the point at which the public interest requirement shifts from a legitimate justification to a moral rationalisation. This gap is particularly acute in the context of AI-based public administration systems, where the scale and opacity of processing render subsequent judicial review an insufficient safeguard.

Despite the growing body of literature on data protection and digital ethics, there remains a critical gap in the systematic integration of ethical assessment into the legal framework governing the processing of personal data. Existing research tends to focus either on doctrinal legal analysis or on the development of abstract ethical principles, without providing operational models that combine these areas in a structured and applicable manner. Moreover, current regulatory approaches, including the GDPR and related frameworks, primarily ensure procedural compliance but offer limited tools for assessing the substantive ethical legitimacy of data processing practices, particularly in complex contexts such as algorithmic decision-making and transnational data flows. This gap between formal compliance with legal norms and ethical legitimacy is the central issue addressed in this study.

1.3. Research aim and objectives

The aim of this study is to develop an integrated ethical and legal model for assessing the legitimacy of personal data processing in the digital environment, which will bridge the gap between formal compliance with legal norms and a substantive ethical assessment. This model should enable critical scrutiny of the legitimacy of data processing decisions through the prism of not only legal norms, but also fundamental ethical principles such as autonomy, dignity, transparency, responsibility and fairness. To achieve this aim, the study aims to address the following objectives.

- to assess the capacity of existing regulatory frameworks, including the GDPR, PIPL, LGPD and CCPA, to address the procedural compliance and the substantive ethical legitimacy of data processing, thereby identifying specific regulatory gaps that the proposed model is intended to fill;
- to reconstruct the ethical and legal conflicts inherent in the case law of the European Court of Human Rights as empirical evidence of the instances in which formal legal reasoning fails to resolve the tension between privacy and public interests, thereby establishing a set of specific types of conflicts that must be taken into account in the assessment criteria;
- develop a structured framework comprising five interrelated criteria (legitimacy of purpose, proportionality, transparency, accountability and data subject participation), each designed to operationalise a specific dimension of the balance between privacy and public interests, which existing frameworks leave legally undefined;
- to suggest the concept of digital solidarity as a normative principle that extends the proposed model beyond a human rights-based analysis, and to demonstrate its added value compared to the principle of accountability, which is already enshrined in the GDPR;
- to operationalise the integrated model as a practical analytical tool for assessing regulatory impact, conducting ethical audits of digital systems and informing legislative reform, with specific application to the context of data governance in Ukraine.

Despite significant developments in data protection legislation and the emergence of complex regulatory frameworks such as the GDPR, a fundamental regulatory contradiction remains unresolved. Current legal regimes are primarily designed to assess the formal lawfulness of data processing, whereas many of the most controversial digital practices raise questions that go beyond compliance with the law and concern their ethical legitimacy. Situations involving algorithmic decision-making, biometric surveillance, workplace monitoring, predictive analytics and large-scale data processing in the public interest often reveal conflicts between individual autonomy and collective interests that cannot be adequately resolved using existing legal criteria alone. As a result, there is a growing gap between procedural legality and substantive legitimacy. The central issue addressed in this study is the lack of an integrated ethical and legal framework capable of assessing whether interference with personal data rights can be justified not only from a legal perspective, but also in terms of moral responsibility, fairness, transparency and respect for human dignity.

2. Literature review

In the current discourse on the protection of personal data, academic approaches diverge along three fundamental lines: the

normative foundations of privacy, the adequacy of consent as a mechanism of legitimation, and the interrelationship between compliance with legal norms and ethical responsibility. The dominant strand of European legal scholarship views privacy as a fundamental right requiring strong state regulation, with the GDPR being the most sophisticated institutional expression of this position (Kuner et al., 2020). This rights-based perspective is widely shared by comparative legal scholars, who analyse its partial implementation in Brazil's LGPD, India's DPDP Act and South Korea's PIPA (Kloiber, 2021; Kolah, 2024).

However, this consensus breaks down when researchers examine non-European contexts. Cheung and Chen (2021) and Chorzempa et al. (2018) demonstrate that in China, privacy is institutionally subordinated to national security interests, creating a governance architecture that is formally regulatory but fundamentally incompatible with the autonomy-based rationale of the European model. The US market-oriented approach occupies a third position: privacy as a contractual variable shaped by sectoral context rather than a universal principle (FTC, 2024; Sanchez & Francis, 2024). These three positions are not merely different regulatory choices reflecting incompatible assumptions about the moral status of personal information, but rather a confirmation that a single legal model cannot resolve the tension between privacy and public interests without a fundamental ethical foundation capable of functioning across all three paradigms.

Much of the literature considers the adequacy of informed consent to be the primary mechanism for legitimising data processing; in particular, Sampson (2021) and Banks (2025) document how the formalisation of consent through complex, opaque user agreements transforms it from a genuine act of autonomous will into a mechanism for shifting risk from controllers to data subjects. Nissenbaum's (2004) concept of contextual integrity offers a theoretical alternative, arguing that the legitimacy of data flows should be assessed on the basis of social norms rather than individual consent. However, this approach has been criticised for its descriptive rather than normative nature: it identifies when norms are violated but does not specify how to resolve conflicts between competing contextual expectations (Dhirani et al., 2023). A third position, represented by models of collective governance and the concept of data solidarity, argues that consent is inherently insufficient, as data processing affects communities rather than just individuals (Kerasidou & Kerasidou, 2023). However, this strand of the literature, whilst theoretically compelling, has not produced operational regulatory tools. This study directly addresses this impasse: rather than resolving the debate on consent, it proposes criteria that function independently of consent as the primary mechanism of legitimation.

The relationship between compliance with the law and ethical responsibility should be considered not only in the context of data processing that meets the legal requirements of the GDPR, including purpose limitation, but also in terms of lawfulness from the perspectives of proportionality and transparency (European Commission, 2016). De Hert and Gutwirth (2020) partially challenge this view, arguing that the law should function not only as a protective tool but also as a mechanism for ethical guidance; however, their analysis remains at the level of normative aspirations rather than operational design. The literature on algorithmic governance is more critical: Arrieta et al. (2020) and Dhirani et al. (2023) demonstrate that formally compliant algorithmic systems can lead to discriminatory outcomes that legal mechanisms are structurally ill-equipped to detect or remedy. De Hert and Papakonstantinou (2022) advocate for ethics-by-design as a structural response, but acknowledge that the operationalisation of ethical principles within legal frameworks remains underdeveloped. The risk-based regulatory approach reflected in the GDPR and the EU Artificial Intelligence Act seeks to bridge this gap by differentiating the intensity of regulation according to potential harm (Shamov, 2025). As Beauchamp and Childress (2001) point out in their seminal critique of risk-based digital governance, risk assessment models are inherently limited when the harm in question is intangible, such as the violation of dignity or the loss of autonomy.

Empirical studies show that public trust in data-sharing practices is determined not by formal compliance, but by perceptions of fairness, the transparency of governance structures, and trust in accountability mechanisms (Eke & Stahl, 2024; Kerasidou & Kerasidou, 2023). Large-scale transnational analyses identify three interrelated clusters that structure global governance of digital ethics: responsible technological development, protection of digital rights, and institutional ethical governance, but also reveal persistent discrepancies in their implementation across different jurisdictions (Cao & Meng, 2025; Guenduez et al., 2025). Qiu and Hu (2025) and Dittmar et al. (2025) further document a shift towards life-cycle-based AI governance, with an emphasis on continuous monitoring and embedded accountability rather than compliance at a specific point in time. Although these contributions significantly enrich the management literature, they share a common limitation: they empirically describe how ethical aspects are institutionalised, rather than prescribing how conflicts between privacy and public interests should be resolved in specific decision-making contexts.

Overall, the literature reviewed reflects a genuine paradigm shift from purely doctrinal analysis to interdisciplinary, empirically grounded approaches. However, three specific gaps remain. Firstly, studies combining legal and ethical analysis (De Hert & Gutwirth,

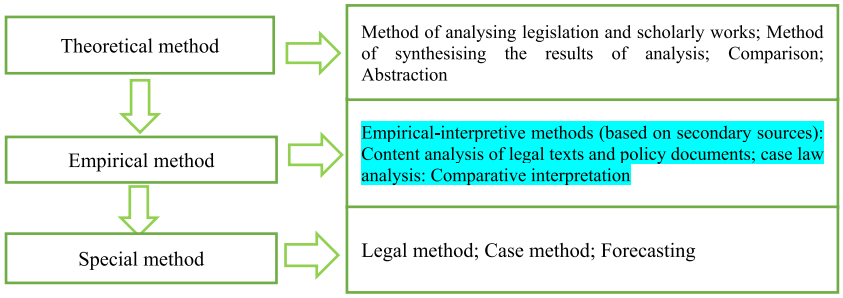

Fig. 1. Classification of research methods within the ethical-legal model of digital accountability.

2020; De Hert & Papakonstantinou, 2022) do not translate their normative conclusions into assessment criteria applied by regulators, auditors or policymakers. Secondly, empirical studies of data governance and algorithmic accountability (Eke & Stahl, 2024; Guenduez et al., 2025; Qiu & Hu, 2025) identify ethical aspects but do not integrate these aspects with the legal instruments that regulate data processing in practice. Thirdly, the governance frameworks emerging in the literature on AI ethics (Cao & Meng, 2025; Dittmar et al., 2025) address institutional structure but lack the normative specificity required to evaluate individual data processing decisions. This study directly addresses these gaps by proposing an integrated model that operationalises ethical criteria within a legally grounded evaluation framework.

3. Materials and methods

This study employs a doctrinal, comparative and conceptual research design grounded in interdisciplinary legal analysis and ethical reflection. The methodological framework does not rely on primary empirical data collection; instead, it systematically examines normative sources, case law and academic discourse to develop an integrated ethical-legal model of digital accountability. Fig. 1 illustrates the methodological logic of the study, demonstrating how doctrinal, conceptual and interpretative analyses interact in the development of the proposed model. Although schematic in nature, it reflects the sequential integration of different analytical levels underpinning the formulation of assessment criteria.

The methodology is based on a doctrinal legal analysis applied to key regulatory instruments, including the European Union's General Data Protection Regulation (GDPR), China's Personal Information Protection Law (PIPL), Brazil's General Data Protection Law (LGPD) and the California Consumer Privacy Act (CCPA). This analysis focuses not only on the formal structure of legal provisions, but also on their underlying value assumptions and ethical implications. The starting point was a comparative doctrinal analysis of four main regulatory regimes, which was undertaken to identify the points at which the formal legal requirements of each regime prove incapable of ensuring an assessment of the substantive ethical legitimacy of data processing practices. Three diagnostic questions were posed for each regime: what legal grounds does it provide for restricting individual privacy in the name of the public interest; what mechanisms does it offer for assessing the proportionality and ethical justification of such a restriction; where does formal compliance end and substantive legitimacy begin. The answers to these questions formed a map of regulatory gaps as specific dimensions of the balance between privacy and the public interest, none of which are regulated in the regimes under study through legally binding mechanisms.

The application of a comparative approach makes it possible to analyse the differences between the legal systems of the European Union, the United States, China, Japan, India, and Brazil, and to identify the relationship between cultural paradigms and regulatory priorities. The comparative analysis also includes Ukrainian legislation, which demonstrates a desire for regulatory harmonisation with the ethical framework of European digital regulation. The comparative analysis is performed not only at the level of textual comparison of norms, but also taking into account the socio-cultural determinants that influence the interpretation of privacy and the admissibility of interference by the state or corporations. The comparative method is used to identify differences and similarities between legal systems, taking into account the cultural, political and institutional contexts that shape approaches to privacy and data management.

The study also includes an analysis of case law, in particular that of the ECtHR, as an interpretative tool for examining how abstract legal principles are applied in practice. The court rulings were examined as empirical manifestations of normative reasoning, i.e., situations in which judges were compelled to resolve conflicts between privacy and competing public interests in the absence of adequate regulatory guidance. For each case, the analysis determined: which specific dimension of the balance between privacy and public interest was called into question; which criterion the Court applied to resolve it; and which ethical principle underlies that criterion. This approach yielded a typology of conflicts, each linked to a specific evaluative dimension that can be operationalised within the proposed model. This made it possible to trace how abstract principles of law and morality are applied in specific cases, revealing tensions between values and the evolution of approaches to balancing individual rights and the public interest.

Based on a synthesis of these two levels, a conceptual analysis was carried out of five key regulatory categories: legitimacy of purpose, proportionality, transparency, accountability and data subject participation. Each criterion was included in the model only if three conditions were met simultaneously. Firstly, a comparative analysis of regulatory regimes had to identify a regulatory gap in this dimension, that is, existing legal instruments had to prove insufficient for assessing precisely this aspect of the balance between privacy and the public interest. Secondly, an analysis of case law had to identify at least one specific type of conflict in which this dimension acted as a decisive evaluative factor. Thirdly, the academic literature on legal and ethical theory was to provide a sufficiently developed normative content for this dimension so that it could function as an operational criterion for assessment, rather than merely a declarative principle. Criteria that met only one or two of these conditions were considered either legally redundant or ethically inoperative and were excluded. This convergence procedure ensures that the five criteria comprising the model are not arbitrary and do not merely replicate existing frameworks, but are specifically aimed at addressing the normative gaps identified in the earlier stages of the analysis.

The final step was to operationalise the integrated model: for each criterion, its legal basis in existing regulatory instruments, its ethical content as shaped by philosophical literature, its logic of application in specific data processing contexts, and its relationship with the four other criteria within the overall model were identified. At this same stage, the concept of digital solidarity was integrated as a normative principle governing the collective dimension of the model, which none of the five individual criteria covers on its own.

The object of the study is the globalised processes of collecting, processing and disseminating personal data, while the subject is the ethical and legal aspects of their regulation. The research is carried out in compliance with the principles of academic integrity, ethical impartiality, respect for confidentiality and prevention of plagiarism. This approach allows us to create not only an analytical, but also

a conceptual and normative framework capable of ensuring morally meaningful legal regulation of digital reality. It is important to note that, although the study does not involve the collection of primary empirical data, it draws on empirical findings from the current literature in the fields of data management and digital ethics. This enables the study to remain empirically grounded, whilst maintaining its primary focus on doctrinal and conceptual analysis.

4. Results and discussion

4.1. Between autonomy, innovation, and control: Ethical-legal models of data protection

The analysis of ethical and legal models of data protection in this chapter serves a specific purpose within the broader argument of this study: to demonstrate that the balance between privacy and public interests is not resolved in the same way across different regulatory systems, but is structured differently depending on the dominant value orientation of each model. Understanding these structural differences is a prerequisite for developing assessment criteria capable of functioning across different jurisdictions, which is the practical aim of the proposed system. Each model discussed below embodies a distinct answer to the question of when public interests may legitimately override the privacy of personal information, and each answer has specific ethical implications that formal compliance mechanisms do not take into account.

To ensure analytical clarity, the following discussion is structured around a sequential examination of three basic models: the law-oriented, market-oriented and state-centred models. Each is analysed through the prism of its dominant values, mechanisms of legitimation and practical implications for the data subject. In this study, the ethical and legal models of personal data protection are classified by the dominant value orientation and regulatory mechanism that determines the relationship between individual autonomy, market freedoms and state control. This criterion allows us to identify profound differences between normative approaches to digital privacy - not only in the formal legal, but also in the moral and philosophical plane. "It highlights how a particular legal system interprets the essence of privacy: as an inherent individual right, a market instrument, or an object of state governance. The chosen approach is key to understanding why regimes that are similar in form of regulation can differ significantly in terms of the balance between the interests of individuals, businesses and the state. On the basis of this criterion, three main ethical and legal models are distinguished: The right-centred model, the market-oriented (sectoral) model and the state-centred (control) model.

Comparative Table 1 helps identify systemic patterns, internal contradictions and structural paradoxes that are not apparent when analysing each model in isolation. In particular, the formal similarity of the regulatory architectures masks a profound incompatibility of values. The GDPR, PIPL and LGPD have a similar structure: all three define the legal grounds for data processing, establish the rights of data subjects and provide for supervisory mechanisms. However, in terms of the concept of privacy, they take diametrically opposed positions: an inalienable human right, a strategic instrument of public administration and a commercial variable, respectively. This means that regulatory convergence at the procedural level not only fails to eliminate but also masks the divergence in values at the level of normative foundations. That is why formal compliance with the requirements of one regime does not guarantee ethical legitimacy in the context of another.

It is worth noting that this table reveals a structural paradox in terms of adaptability and protection: models with the highest level

Table 1
Comparative characteristics of ethical and legal models of digital regulation of personal data.

Criterion.	Centre-right model	Market-oriented model	State-centred model
Dominant value	Dignity, autonomy, digital privacy	Freedom of choice, economic competition	Collective security, political stability
Legal source	GDPR (EU), LGPD (Brazil), DPDP (India), CCPA/CPRA (California)	HIPAA, GLBA, COPPA, sectoral regulation in the US	PIPL (China), cybersecurity law, data localisation
Ethical principles	Transparency, accountability, autonomy, fairness	Contractual agreement, self-regulation, innovation	Control, subordination, primacy of the state interest
The role of the data subject	Active holder of digital rights	The consumer with limited choice	Object of public administration
The mechanism of legitimisation of processing	Legal basis + ethical justification	Formal consent through privacy policies	State approval or security imperative
Oversight and enforcement mechanisms	Independent data protection authorities (DPAs); judicial protection; fines	Sectoral regulators; industry associations; self-regulation; class actions	State supervision; permissive control; limited appeal
AI and Big Data processing	Regulation of automated decisions; right to explanation; audit of algorithms	Ethical guidelines (voluntary); focus on eliminating bias post facto	Use of AI for surveillance; AI governance; opacity of algorithms
Cross-border data transfer	Adequacy decisions; SCCs; BCRs	Contractual terms; Privacy Shield (historically); certification	Data localisation; state authorisation; strict control
Advantages of the model	High level of legal protection; compliance with human rights	Flexibility; rapid adaptation; stimulation of innovation	Centralised management; efficient response
Disadvantages/risks	Formalisation of procedures; technical complexity of implementation	Illusory consent; unequal guarantees; conflict of interest	Non-transparency; censorship; lack of independent control
Ability to adapt	High, requires resources and regulatory updates	Very high; depends on the market	Limited; centralised decision-making
The concept of privacy	An inalienable human right	Commercial variable; the subject matter of a contract	A strategic management tool

of legal protection demonstrate the lowest capacity for adaptation, whilst models with the greatest flexibility provide the weakest protection of the subject's autonomy. The rights-based model is rated 'high' for adaptability but requires significant resources and regulatory updates; the market-oriented model is 'very high' for flexibility but creates illusory consent and unequal guarantees; the state-centric model guarantees stability, but at the cost of 'limited centralised decision-making'. This trade-off triangle demonstrates that none of the models is optimal across all dimensions simultaneously, which is a direct argument in favour of the integrated approach proposed in this study.

The most telling comparison is that between models in the fields of AI and big data and cross-border data transfers, particularly in those areas where technological development is outpacing regulatory capacity. The rights-based model attempts to regulate automated decisions through the right to explanation and algorithmic audit, but faces the 'black box' phenomenon, which makes effective oversight impossible. The market-oriented model is limited to voluntary ethical guidelines and reactive bias mitigation. The state-centric model uses AI primarily as a surveillance tool, maintaining the opacity of algorithms as an institutional advantage. None of the three models provides a mechanism for assessing whether a specific practice of algorithmic governance is not only formally lawful but also substantively justified, which is precisely the gap that the proposed system of criteria fills.

A comparison of the mechanisms for legitimising data processing reveals a fundamental asymmetry: the rights-based model requires a legal basis plus an ethical justification, whilst the market-oriented model requires either state approval or a security imperative. This asymmetry means that the same data processing practice may be lawful in one jurisdiction, unlawful in another, and formally neutral in a third, depending not on its nature but on which regime is assessing it. This makes it impossible to assess the legitimacy of transnational data flows uniformly through positive law alone and highlights the need for ethical criteria that operate independently of jurisdictional affiliation.

The comparative analysis presented above reveals not only structural differences between regulatory models, but also deeper divergences in their underlying regulatory priorities. Whilst some frameworks emphasise individual rights and procedural safeguards, others prioritise public interests or economic efficiency, resulting in varying degrees of protection for personal autonomy. Importantly, none of the models examined provides a fully integrated mechanism for assessing the ethical legitimacy of data processing beyond formal compliance. This limitation becomes particularly evident in contexts involving algorithmic decision-making, where legality does not necessarily imply fairness or accountability. These findings highlight the need to develop an assessment system that goes beyond a purely legal comparison and incorporates ethical criteria as a key component of the legitimacy assessment. The proposed model aims to address this gap by offering a structured approach that reconciles legal requirements with ethical imperatives.

The most striking embodiment of this model is seen in the GDPR, which represents a high level of regulatory specificity and ethical sensitivity. The GDPR declares privacy as a fundamental human right, backed by a system of binding data processing principles, such as lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy, storage restriction, integrity, confidentiality and accountability (European Commission, 2016). Of particular note is the concept of accountability, which transforms responsibility for compliance with standards from a formal obligation into an element of legal culture. Within this model, a clear list of legal grounds for data processing is provided, which precludes arbitrary interference by both the state and private entities.

A key feature of the right-centred approach is an expanded catalogue of data subject rights, including the right to access information, the right to rectify, delete, restrict processing, transfer, and object to automated decisions. These rights carry not only procedural significance but also profound ethical importance, as they embody the idea of personal autonomy as an individual's capacity to control the digital projection of their identity. At the same time, the regulatory design also provides for preventive protection mechanisms: data protection impact assessment (DPIA), mandatory appointment of a data protection officer (DPO), notification of security breaches, and high penalties for non-compliance (ICO, 2025). Particular attention should be paid to the strict regime of cross-border data transfer, which is allowed only if there is an adequate level of protection in the recipient state or additional legal instruments are applied (European Commission, 2016).

From an ethical and legal perspective, the strengths of the centre-right model lie in its ability to provide a proactive, value-based approach to regulation that goes beyond formal compliance with procedures. Its normative power is embodied in the creation of a system where individual rights are not an optional element, but are at the heart of digital interaction. The introduction of the principle of 'privacy by design' promotes ethical thinking in technological architectures at the design stage (Cavoukian, 2009). At the same time, despite its high regulatory complexity and depth, the model faces a number of challenges. The formalisation of informed consent, which is often implemented through non-transparent or difficult-to-understand user agreements, can devalue its ethical legitimacy. Implementation of the GDPR requirements requires significant administrative resources, especially in small organisations or in a cross-border context. In addition, even with a high level of legal detail, there are so-called 'grey areas' (for example, data processing for scientific purposes, artificial intelligence or national security) where the balance between privacy and the public interest remains morally tense.

A particular challenge is the exercise of the right to an explanation in the context of automated decisions, which are increasingly made by artificial intelligence systems based on opaque algorithms. In the context of the 'black box' phenomenon, explaining the mechanism behind a specific decision becomes technically challenging, thereby undermining the effectiveness of legal protection. Moreover, the global scope of the regulation, which applies to all companies processing data of EU citizens, gives rise to jurisdictional conflicts and criticism from other states that perceive extraterritoriality as an intrusion into their own sovereignty.

The reflection of the centre-right model in legal systems is not limited to the European Union. Its principles have been partially adapted in Brazil's General Data Protection Law (LGPD) (IAPP, 2020), Korea's PIPA (Global Privacy Laws, 2025), India's Digital Personal Data Protection Act (DPDP Act), as well as in some US states, including California, where the CCPA/CPRA provisions focus on consumer rights in the spirit of the European model (Bloomberg Law, 2025; California Privacy Protection Agency, 2025). All of these jurisdictions, despite their cultural and political differences, demonstrate the growing need for regulatory protection of information

autonomy as a basis for digital dignity. That is why the right-centred approach remains the leading model that national legislators and international organisations are guided by in their search for a normative and ethical response to the challenges of the digital age.

In contrast to the right-centric model, which removes privacy from the realm of human rights and ensures its protection through detailed state regulation, the market-oriented or sectoral model forms a completely different view of the nature of personal data and mechanisms for its protection. Within this model, informational privacy is not regarded as an absolute moral right, but rather is construed as a variable shaped by market processes determined by contractual consent, self-regulation, and commercial viability. The most representative example of this model is the US legal system, where there is no single national law on personal data protection. Instead, there is a fragmented approach based on sectoral regulation, with specific laws only applicable to specific industries: HIPAA for healthcare (CDC, 2024), GLBA for financial services (FTC, 2024; ITLawCo, 2024), COPPA for child protection (FTC, 2025). This structure demonstrates a functional approach, where data protection is carried out in accordance with the economic context of its use, rather than universal legal standards.

At the same time, the Federal Trade Commission (FTC) plays a key role in enforcing privacy standards, primarily by overseeing compliance with companies' public data processing promises under the unfair or deceptive practices provisions of Section 5 of the FTC Act (FTC, 2024; Sanchez & Francis, 2024). The peculiarity of the American model is the emphasis on the freedom of action of market participants, which provides for the ability of companies to formulate internal privacy policies on their own, and users to enter into contractual agreements that actually determine the limits of their data use. Such dynamics give rise to a powerful role of self-regulation: industry codes of conduct, voluntary standards, certification mechanisms and contractual obligations become the basis for privacy protection. In addition, judicial mechanisms that provide protection through individual or class action lawsuits play an important role in the US (FTC, 2024).

From an ethical and legal point of view, the strengths of the market-oriented model are its flexibility, ability to quickly adapt to technological changes, and the reduction of administrative pressure on business, which stimulates innovation and the development of the digital economy (Olivero & Folks, 2024). The ethical argumentation for this model is often based on freedom of choice, market competition, and the principle of mutual benefit between the user and the company. However, this conceptual framework has serious vulnerabilities. The dependence of privacy protection on sectoral affiliation or state jurisdiction results in uneven guarantees, creates regulatory 'blind spots', and enables the evasion of strict oversight in less protected areas. (FPF, 2024).

Moreover, the principle of voluntariness is often illusory, as users are compelled to accept policies that are not always comprehensible or genuinely optional. Formal consent, given under conditions of informational asymmetry, loses its moral legitimacy and becomes a mechanism for shifting risk from the company to the user. Another ethically vulnerable element of the model is the dominance of corporate interests, which in practice often prevail over the rights of users, especially in the context of a monopolised digital services market. The absence of a unified ethical standard makes it difficult to develop a sustainable privacy policy, and trust in business becomes a condition rather than a consequence of effective regulation. The model places responsibility for the ethical management of personal data on actors interested in its commercial use, which creates an obvious conflict of interest (California Privacy Protection Agency, 2025).

Nevertheless, the market-oriented model remains a powerful regulatory alternative that is consistent with the philosophy of minimal government intervention and the priority of economic freedom. Elements of this approach can also be found in the legal systems of some Asian countries, such as Singapore, Japan, India and South Korea, where the government's digitalisation strategy places greater emphasis on innovation, self-regulation and a flexible regulatory environment (PDPC, 2023; Law.asia, 2022). The next logical step in the study is to analyse the state-centred model, which, unlike the right-centred and market-centred models, moves the problem of personal data out of the plane of rights or the market into the paradigm of national security, social order and centralised control. In this context, the determining factor is not the protection of individual autonomy or economic efficiency, but the ability of the state to manage information flows in the interests of political stability and strategic management (Cheung & Chen, 2021; Chorzempa et al., 2018).

The state-centric model establishes an alternative ethical-legal paradigm in which informational privacy is not treated as a sui generis value, but rather as a variable subordinated to public interests. A clear manifestation of this model can be observed in the legal system of the People's Republic of China, where the Personal Information Protection Law (PIPL), alongside the Cybersecurity Law and other regulatory instruments, establishes a centralised architecture for the control of personal data. (Bloomberg Law, 2022; Digichina, 2021). The main feature of this approach is the dominance of the state as the only legitimate entity that determines the rules for collecting, processing, storing and transmitting information, including the requirements for data localisation and the permissive nature of processing (China Briefing, 2025; Privacy Matters, 2025).

In addition, the regulatory framework includes the possibility of using personal information within the social credit system, a mechanism that assesses the behaviour of individuals and legal entities, affecting their ability to access services, employment and freedom of expression (Internet Society Foundation, 2024; StratCom, 2021). Despite the formal existence of data subject rights, the actual mechanism for their implementation remains limited, which creates an ethical dilemma between legitimate security and institutionalised surveillance that erodes the idea of personal autonomy (Chorzempa et al., 2018; Murrell, 2018).

In this context, the state-centred model appears as an instrument of legal, but not always legitimate, interference, which demonstrates the asymmetry of power between the state and the individual. Its elements can also be traced in the legal systems of other countries with a centralised political structure, where state interference is disguised as technical regulation or cybersecurity (RUSI, 2025). Thus, the state-centred model demonstrates the antithesis of the right-centred approach, emphasising a radically different value hierarchy, where the rights of the individual are derived from the interests of the state. Together with the market and right-centred models, it forms a triangle of conceptual tension, in which each party offers its own answer to the question: who owns the right to personal information - the individual, the market or the state. Ukrainian regulatory practice is in the process of finding a

balance between these models, with a gradual shift towards a right-of-centre approach that combines regulatory clarity with moral sensitivity.

As the analysis shows, none of these models is universal or perfect. Each of them has its own advantages and limitations, and creates a different balance between freedom, responsibility and control. The next chapter will summarise the comparative analysis of the three approaches and substantiate the need for an integrated ethical and legal model capable of combining regulatory clarity with moral sensitivity in the era of globalised information systems. To summarise the results of the typological analysis, it should be emphasised that the three main ethical and legal models of personal data protection form fundamentally different approaches to defining the nature of privacy, the limits of permissible interference and the role of the main subjects of digital interaction. The right-centred model is based on the supremacy of human dignity, focuses on the protection of individual autonomy, and provides strict regulatory control through preventive legal mechanisms. The market-oriented approach treats data as an object of contractual relations and a subject of economic exchange, delegating responsibility for privacy protection to market participants. The state-centric model, in turn, institutionalises the idea of digital sovereignty, where personal data is seen as a strategic resource of state security and a tool of social governance.

What is decisive is not only the normative architecture of each model, but also the ethical lens it reproduces. In the first case, the moral dominant is individual autonomy; in the second, freedom of choice within market conditions; and in the third, the primacy of the collective good, interpreted through the prism of state interest. These value orientations define the specifics of legal application, the nature of conflicts, and the boundaries of permissible interference. Accordingly, any analysis of the legitimacy of personal data processing that fails to account for the value foundations of the model risks remaining formalistic and disconnected from the moral reality of the digital world.

At the same time, none of the models under consideration provides a complete answer to the challenges of the globalised information environment. The centre-right approach demonstrates normative strength but needs to be adapted to rapid technological change and new forms of digital interaction. The market model creates favourable conditions for innovation, but suffers from ethical ambivalence and fragmentation. The state-centred system guarantees stability and control, but often at the cost of narrowing personal freedom and restricting civil rights. In this context, there is a need to rethink the regulatory framework for data protection not only as a legal category, but as an interdisciplinary category that requires the integration of ethical standards at the level of systemic practice.

Thus, the classification of ethical-legal models serves not only an analytical but also a conceptual function: it enables the identification of the underlying sources of normative diversity, reveals the nature of the ethical dilemmas accompanying the regulation of personal data, and provides a foundation for the further development of an integrated approach. The following chapters will analyse specific conflicts that arise at the intersection of law, ethics and technology, and develop our own model of ethical and legal responsibility based on the principles of digital dignity, solidarity and normative proportionality in the era of algorithmic governance.

Thus, the typology developed here enables us not only to describe the differences between regulatory approaches, but also to identify their underlying value logic. This, in turn, lays the groundwork for moving from abstract modelling to the analysis of specific conflict situations in which these approaches manifest themselves in practice. It is appropriate to refer to judicial practice, which serves as an empirical indicator of the effectiveness of ethical and legal models. The selected cases illustrate various types of conflicts between privacy and the public interest and allow us to trace how these conflicts are resolved in the application of the law.

Judicial cases, particularly the rulings of the ECtHR, serve as a kind of 'litmus test' for revealing the hidden ethical tensions that arise at the intersection of the right to privacy and the public interest. This analysis examines three illustrative cases, each of which illustrates a different configuration of the moral conflict surrounding the processing of personal data and demonstrates how judicial logic attempts to find a balance in complex digital contexts. The case of S. and Marper v. the United Kingdom can be considered a fundamental precedent that questioned the legitimacy of state storage of biometric data of persons not found guilty of a crime. The UK police kept the DNA profiles, fingerprints and photographs of two citizens after their acquittal, citing security concerns. However, the ECtHR recognised that massive and indefinite storage of sensitive data violates the right to privacy guaranteed by Article 8 of the Convention (European Court of Human Rights, 2008). The main ethical dilemma in this case is the conflict between preventive security and the presumption of innocence, which makes the principle of proportionality an ethical and legal tool.

Another illustrative example is the case of Bărbulescu v. Romania, in which an employee was dismissed for using his work email for personal correspondence. The ECtHR in the Grand Chamber judgement concluded that the employer's interference with private communication without clear warning violated Article 8 of the Convention (European Court of Human Rights, 2017; Global Freedom of Expression, 2023). The Court emphasised the need for predictability, transparency and proportionality of monitoring, which points to the ethical dilemma of the limits of digital autonomy in the context of hierarchical dependence.

The third case, which illustrates the conflict between privacy and the right to public memory, is M.L. and W.W. v. Germany. The applicants, who had been convicted of a serious crime, requested the removal of archival materials about the case from media online resources. The German courts, and subsequently the ECtHR, rejected the claim, citing the public interest in preserving historical information and the right to freedom of expression. (European Court of Human Rights, 2018; Columbia Global Freedom of Expression, 2023). The main ethical tension lies in the opposition between the right to be forgotten and the public's right to access public information, which raises the issue of digital stigma and the transformation of publicity in the digital age. The analysed case law provides empirical justification for the criteria proposed in this study. In particular, the principle of proportionality, which is frequently emphasised in the case law of the ECtHR, influences the corresponding criterion in the model. Similarly, issues relating to transparency and accountability, as identified in judicial reasoning, confirm the inclusion of these dimensions as key elements of the ethical and legal assessment. Thus, case law does not merely illustrate the problem, but also plays a constitutive role in shaping the structure of the proposed system, ensuring that it reflects not only theoretical considerations but also practical models of legal reasoning.

The analysis of the relationship between law and ethics encompasses not only areas of conflict but also areas of complementarity.

This makes it possible to identify the conditions under which legal regulation is capable of effectively implementing ethical imperatives, and those under which it reveals its limitations. Thus, the case studies not only illustrate the tension between law and ethics but also corroborate the study's thesis regarding the necessity of normative integration of moral principles into the framework of digital regulation. A detailed analysis of the mechanisms of such integration, as well as the identification of points of synergy and conflict between the legal and ethical dimensions, will be undertaken in the following subsection. After analysing theoretical models and reconstructing specific ethical conflicts in practice, this chapter focuses on an in-depth examination of the interaction between legal norms and ethical principles in the context of personal data protection. This concerns not merely the coexistence of two spheres - legal and moral - but their potential complementarity or tense opposition. The aim is to identify both moments of normative synergy, where law effectively realises ethical imperatives, and zones of divergence, where legal logic reveals insufficiency or even contradicts moral sensitivity.

In cases of normative synergy, we can talk about situations where ethical principles are not only declared but also implemented through effective legal mechanisms. One of the most prominent examples is the enshrinement of the principles of Privacy by Design and Privacy by Default in Article 25 of the GDPR. These provisions require that data protection be integrated at the design stage of digital systems and implemented automatically by default, without the need for any additional actions on the part of the user. From an ethical point of view, this is an implementation of the fundamental principle of proactive responsibility, according to which data developers and controllers should anticipate potential privacy risks before they actually occur. Moreover, these provisions represent an ethical imperative of transparency - they require the creation of clear, predictable, and accessible information architectures that users can comprehend. In this context, the synergy manifests in the legal requirement compelling technological design to be ethically oriented: moral ideals - such as autonomy, respect for personal space, and harm prevention - gain institutional force and are translated into concrete engineering and business decisions.

Another example of regulatory synergy is the detailing of data subjects' rights in the GDPR structure, which significantly strengthens the concepts of autonomy, dignity and fair control. The expanded catalogue of rights - access to information, its correction, deletion, transfer, restriction of processing, as well as the right to object and prevent automated decision-making - is not only a legal toolkit, but also an ethical expression of respect for the individual as an active subject of digital interaction. Each of these rights concretises a moral understanding of control over personal information, providing mechanisms to protect against manipulation, power asymmetries or stigmatisation. The right to data erasure, in particular, reflects a deep ethical intuition about the need for limits to publicity, the right to 'digital renewal' or even to be forgotten - as an expression of the idea that an individual should not be tied to the past in a way that makes moral rehabilitation impossible.

Cases of normative synergy should also include the growing role of ethical codes, recommendations, and interdisciplinary guidelines, which, although not legally binding, increasingly influence the development of legal standards. For example, the European Commission's guidelines on the ethics of artificial intelligence, which include the principles of fairness, impartiality, security, responsibility and human control, are already reflected in regulatory initiatives at the EU level. Such dynamics demonstrate that ethics can perform the function of a conceptual vanguard - it not only accompanies law, but also gives it a value orientation, shaping society's expectations and directing lawmaking towards moral sensitivity. Along with positive examples of synergy between law and ethics, there are serious cases of divergence in the field of personal data protection. Most often, this is due to the formalisation of legal procedures, insufficiency of regulatory mechanisms or their inability to adapt to new moral challenges posed by technological progress (Lee, Zankl, & Chang, 2016; Dhirani et al., 2023).

The first critical area is the erosion of the ethical content of informed consent, which formally remains the key basis for processing personal data (Article 6 of the GDPR), but is increasingly losing its moral legitimacy. In actual practice, consent to privacy policies is achieved through complex, voluminous and non-transparent agreements that users sign mechanically without understanding the content or consequences (Sampson, 2021). The phenomenon of 'cookie fatigue', the asymmetry of knowledge between the user and the data controller, and limited opportunities for alternative choices turn consent from an act of autonomous expression of will into a tool for legalising interference (Banks, 2025). The case of Bărbulescu v. Romania clearly demonstrates this problem: although the legal requirements for awareness were formally met, the ethical tension between the employee's autonomy and the employer's power remained unresolved (European Court of Human Rights, 2017). This indicates that legal compliance does not equal moral justification.

Another problem area is the ethical neutrality of algorithms and complex digital systems. Despite attempts at legal regulation, in particular in Article 22 of the GDPR on automated decision-making, in practice, regulatory mechanisms are limited (GDPR-Text.com, 2025; ICO, 2025). Most modern algorithms function as black boxes whose internal processes are not transparent even to their developers (Dhirani et al., 2023). This makes it impossible not only to control effectively, but also to hold accountable for consequences that may be discriminatory, biased or unpredictable. Ethical requirements - transparency, accountability, fairness - become declarative rather than practical in such circumstances. A situation of blurred or delegated responsibility arises, in which none of the parties bears full moral obligation towards the victim.

The third case of conflict is the blurring of the boundaries of the public interest, which is especially relevant in state-centric regulatory regimes. (Sampson, 2021). Formulations such as national security, social stability, or the protection of public order are often employed to legitimise mass data collection without adequate ethical justification. Such legal provisions set dangerous precedents when the privacy of citizens is sacrificed for the sake of abstract collective goals. In the case of S. and Marper v. the United Kingdom, the ECtHR clearly stated that even security considerations do not justify the indefinite storage of biometric data of persons not found guilty (European Court of Human Rights, 2008). This decision reveals the ethical limit beyond which the state loses the moral right to intervene, even if it is formally lawful. In contemporary normative thinking, ethics is increasingly moving beyond the status of an external commentator or an after-the-fact critic of law. It is emerging as a fundamental co-founder of normative legitimacy - not only complementing legal constructions, but also shaping their value foundations, guidelines and limits. In the realm of personal

data, where the law encounters the challenges of digital autonomy, complex responsibility, and algorithmic opacity, ethics can serve as a moral compass, enabling the timely identification of risks and the distinction between what is formally permissible and what is substantively acceptable.

A legal norm devoid of an ethical basis risks becoming formal, technocratic or even repressive. Its compliance with the letter of the law does not guarantee moral legitimacy, especially in cases where legal instruments outpace society's ability to comprehend their consequences or, conversely, lag far behind the pace of technological transformation. In this context, ethics performs a dual function: first, as a source of normative sensitivity that points out potential risks before they are legally formalised; second, as a platform for social consensus, without which legal regulation loses its legitimation. This transition is especially relevant in the context of the latest challenges associated with the development of artificial intelligence, biometric systems and global digital platforms. Initiatives such as 'ethics by design' or 'responsible innovation' are already demonstrating the potential of ethics as a preventive mechanism that is integrated into technical design, policy planning, and legal rulemaking. Such an ethic is not an abstract morality - it has a structural and institutional form that can audit digital policies, influence the development of standards, and change the logic of legal thinking from formal to value-based.

Thus, the analysis of the interaction between law and ethics in the field of personal data protection reveals both areas of synergy and critical points of conflict. Legal norms, such as the privacy by design principles or the expanded rights of the data subject in the GDPR, effectively embody the ethical imperatives of responsibility, transparency and respect for autonomy. At the same time, other aspects, such as the formalisation of consent, the ethical opacity of algorithms, or the vagueness of the concept of 'public interest', demonstrate a deep normative tension that cannot be resolved solely by positive law instruments. This underscores the key thesis of the study: achieving a fair and sustainable balance between the private and public interest is impossible without the full integration of ethics into the structure of legal regulation. Ethics should function not as an external moral guide, but as an equal component of the normative system, capable of shaping its legitimacy, contextual sensitivity and adaptability. Despite the positive examples of normative synergy between law and ethics, the digital environment gives rise to a number of systemic ethical risks that threaten fundamental values such as autonomy, dignity, and justice. Their identification is key to understanding the limitations of existing legal models and the need for a regulatory reorientation towards moral sensitivity. The table below presents a typical classification of such risks (Table 2).

The concept of ethical risk in the digital context is grounded in the theory of normative legitimacy, which integrates legal permissibility with the moral justifiability of action. The identified categories reflect not merely functional flaws in technology, but structural threats to the moral order of digital interaction. Their assessment serves a diagnostic function and constitutes a prerequisite for ethical-legal auditing. To summarise, none of the models examined provides a universal solution to the problem of striking a balance between privacy and the public interest. This necessitates a shift towards an integrated approach that combines legal certainty with ethical sensitivity.

4.2. Digital solidarity as the normative basis of an ethical and legal model

The analysis conducted highlights the need to deepen the conceptual foundation of the proposed model through the category of digital solidarity, which is presented in this article as a key element of its scientific novelty. Unlike the dominant approaches to personal data protection, which focus primarily on individual rights and the data subject's control mechanisms, the concept of digital solidarity proposes a shift in emphasis towards collective responsibility and the interdependence of participants in digital ecosystems. Digital solidarity can be defined as a normative principle that entails the fair distribution of risks, benefits and responsibilities arising from the processing of personal data within complex socio-technical environments. It is based on the premise that data processing almost never concerns a single individual exclusively, but has broader implications for other individuals, groups and society as a whole. Thus, digital solidarity complements the classical model of 'individual control over data' with a dimension of mutual responsibility.

In functional terms, digital solidarity is realised at several levels. At the interpersonal level, it involves an awareness that individual data-sharing practices can affect the rights and interests of others, particularly through the secondary use of information or algorithmic profiling. At the institutional level, it translates into a requirement for organisations to consider not only the formal legality of data

Table 2
The main manifestations of ethical degradation.

Type of risk	Description of the phenomenon	Consequences.
Algorithmic selection without transparency	Decisions are made on the basis of non-transparent algorithms that do not explain their logic and do not allow verification (black-box systems).	Undermining the right to an explanation, loss of trust, legal unaccountability
Profiling with psychographic features	Creation of digital behavioural models based on sensitive parameters such as emotions, beliefs, and social connections.	Manipulation of choice, interference with autonomy, marketing exploitation
Stigmatisation by behavioural characteristics	Formation of a 'reputation rating' based on online activity (social networks, purchases, search queries, etc.).	Digital discrimination, restriction of access to services, formation of a biased digital image
Delegated responsibility	Decisions are made automatically, but responsibility is shared between the developer, the platform, and the user.	The absence of ethical subjectivity, the inability to appeal or to hold accountable.
Information asymmetry	The user does not know what data about him or her is being processed, how, by whom and for what purpose.	Formalisation of consent, loss of control, psychological alienation

processing, but also the potential negative consequences for vulnerable groups, power imbalances and the risks of discrimination. At the transnational level, digital solidarity addresses issues of inequality in global data flows, including the phenomena of digital colonialism, unequal access to technology and differing protection standards.

It is fundamentally important that digital solidarity does not duplicate the principle of accountability enshrined in the GDPR, but rather offers a different kind of regulatory logic. Whilst accountability focuses on demonstrating compliance with formal legal requirements on the part of a specific data controller, digital solidarity goes beyond individual duty and introduces a collective dimension of responsibility, where the key factor is not merely compliance with the rules, but the fairness of the consequences for all parties involved. Thus, there is a shift from procedural legality to substantive legitimacy. In this context, the proposed concept helps to rethink the very nature of digital regulation: from individualised control to interconnected governance, from legal compliance to ethical responsibility, and from geographically limited jurisdiction to the global interdependence of digital processes (Table 3).

4.3. Criteria for ethical-legal balance

In the context of the regulatory contradictions and moral ambiguity of modern personal data processing practices identified in the previous chapters, there is an urgent need to create a clear ethical and legal framework for assessing the permissibility of interference in the personal sphere (Nissenbaum, 2004). The proposed system of criteria is the result of a synthesis of positive law, ethical philosophy, judicial practice and interdisciplinary reflection aimed at integrating legal norms with moral imperatives. The five criteria set out in this section form the operational basis for the study's response to the problem outlined above. It is intended not only to formalise the grounds for data processing, but also to give it legitimacy in terms of dignity, autonomy, fairness and transparency - the basic values of a democratic digital order. Each criterion relates to a specific aspect of the balance between privacy and public interests, which the existing regulatory framework leaves insufficiently defined in legal terms. Together, they form a structured filtering mechanism designed to answer the following question at each stage of the data processing assessment: does this practice strike a balance between the rights of the data subject and the legitimate needs of society that is not only formally justified but also well-founded?

The theoretical basis of the proposed criteria is an integrative approach that combines normative certainty with ethical sensitivity. The starting point is the fundamental rights, in particular the right to respect for private life, provided for in Article 8 of the European Convention on Human Rights (ECHR, 1950) and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The development of the criteria takes into account the characteristic conflicts identified in analytical and judicial practice, in particular the tension between individual autonomy and national security (S. and Marper v. the United Kingdom, 2008), the right to be forgotten and freedom of expression (M.L. and W.W. v. Germany, 2018), and between employee privacy and employer control (Bărbulescu v. Romania, 2017). The sources of specification are the key provisions of the GDPR (Regulation (EU) 2016/679), ECtHR precedents, ethical concepts of autonomy, accountability, fairness and transparency, as well as international ethical guidelines on AI and digital technologies (IEEE, 2023; EU AI Act, 2024).

The first of these criteria is the legitimacy of the purpose, which requires that each action to process personal data is not only formally lawful, but also value-based. The purpose must be specific, socially significant and consistent with fundamental human rights. Although Articles 5 and 6 of the GDPR declare the principles of limiting the purpose and lawfulness of processing (GDPR, 2016; GDPR-Info, 2025), without ethical scrutiny, the concept of 'public interest' can be used to legitimise excessive interference. This is especially true in the practice of mass collection of biometric data, as shown in the case of S. and Marper v. the United Kingdom, where the ECtHR recognised that even a public purpose must have a moral limit (European Court of Human Rights, 2008).

The second criterion, proportionality of the intervention, requires ensuring an optimal balance between the achievement of the goal and the extent of the restriction of the data subject's rights. Any processing should be the minimum necessary in terms of volume, nature and duration (GDPR-Text.com, 2025). Legally, this principle is enshrined in Article 5(1)(c) of the GDPR, and its ethical significance is to prevent excessive interference in the private sphere. Proportionality acts as a deterrent in areas where societal objectives are often used to justify total surveillance or profiling. The ECtHR judgment in *Bărbulescu v. Romania* clearly demonstrates the importance of taking this proportionality into account in labour relations, especially when it comes to monitoring digital communications without proper warning (European Court of Human Rights, 2017; Global Freedom of Expression, 2023).

The third criterion, transparency and clarity of information processes, implies that data subjects must clearly understand what data is being processed, for what purpose, by whom and how. The transparency provided for in Articles 5(1)(a) and 12-14 of the GDPR should be implemented through plain language, explainability of algorithms and prevention of information asymmetry (ICO, 2025; GDPR Summary, 2025). In an ethical context, this criterion is aimed at recognising the data subject not merely as a recipient of policies,

Table 3
The difference between the accountability principle (GDPR) and digital solidarity.

Criteria	Accountability principle (GDPR)	Digital solidarity (the developed model)
Normative logic	Compliance	Equity of outcomes
Responsible party	Data controller	All ecosystem participants
Nature of responsibility	Individual	Collective
Main focus	Legal compliance	Ethical and social legitimacy
Scope	Primarily jurisdictional	Transnational
Assessment	Formal	Substantive

but as an active participant in the process, capable of making informed decisions. In the environment of automated systems, this means the requirement for explainable AI, i.e. the ability of algorithms to explain the logic of their decisions (IBM, 2023; Nannini et al., 2024).

The next criterion is accountability and responsibility, which requires that each data processor, controller, processor, developer or algorithm operator - not only comply with the rules, but also be able to demonstrate compliance and, in case of harm, bear legal and moral responsibility. What is at stake is not reactive ex post responsibility, but a proactive normative culture in which responsibility is embedded within organisational ethics. This principle is enshrined in Article 5(2) of the GDPR as the principle of accountability, which requires not only compliance but also the ability to demonstrate compliance (GDPR, 2016; GDPR Summary, 2025). Article 24 of the GDPR expands upon this provision by obliging the controller to implement technical and organisational measures that ensure and demonstrate that the processing is in accordance with the Regulation. (GDPRhub, 2025; ICO, 2025).

The model is completed by the criterion of data subject participation, which brings the individual out of the passive state of a processing object and into the position of an active participant in digital interaction. Its ethical basis is respect for autonomy, and its legal basis is the rights enshrined in Articles 15–22 of the GDPR. This includes the right of access (Article 15), rectification (Article 16), erasure (Article 17), restriction of processing (Article 18), portability (Article 20) and objection to processing (Article 21), as well as protection against automated decisions (Article 22) (EDPB, 2023; GDPRhub, 2025). Only when these rights are truly upheld can individuals control their digital lives, resist interference that goes against their will, and ensure that digital practices are consistent with their own values.

The proposed criteria should not be applied in isolation, but as a comprehensive filtering and evaluation system. They serve not only as a legal verification tool, but also as an analytical tool for ethical auditing of digital solutions, policies and infrastructures. They make it possible to overcome the superficial logic of formal compliance by replacing it with a substantive assessment of moral adequacy and legal appropriateness. This constitutes their methodological advantage as guiding principles for the development of ethically sensitive legislation and resilient, trust-based digital environments. The developed system of criteria is not only an analytical tool, but also a fundamental component of an integrated ethical and legal model that allows conceptualising fair regulation of digital relations in the era of algorithmic governance. It serves as a bridge between norm and value, between procedure and legitimacy, affirming the idea that no digital intervention is acceptable without moral responsibility for its consequences.

At first glance, the criteria included in the proposed framework may appear to reflect established principles found in existing legal and ethical instruments. However, the novelty of this study lies not in the introduction of entirely new normative categories, but in the systematic integration and operationalisation of these principles within a single assessment model. Unlike the GDPR, which establishes predominantly procedural and compliance-oriented requirements, the proposed system of criteria is designed to assess the substantive legitimacy of data processing practices. It shifts the analytical focus from whether a particular practice formally complies with legal norms to whether it can be justified from an ethical and social perspective. Furthermore, unlike ethical guidelines developed at European level, which often remain declarative and principle-based, this framework translates these principles into a structured set of interrelated criteria that can be applied consistently and comparably. The originality of the model lies in its integrative and operational nature: it combines legal norms and ethical considerations, transforms abstract principles into assessment tools, and provides a coherent framework for evaluating complex data management practices in various contexts.

The proposed ethical and legal model should be considered within the context of existing approaches to data governance and digital ethics. Unlike traditional regulatory frameworks, which focus primarily on compliance with formal rules, this model introduces a structured mechanism for assessing the substantive legitimacy of data processing practices. In this sense, it extends rather than replaces doctrinal approaches by incorporating ethical criteria into the assessment process. Compared to ethical and philosophical models, which often emphasise abstract principles such as autonomy or justice, the proposed framework offers a higher degree of operationalisation. It transforms these principles into a system of evaluation criteria that can be applied in specific regulatory and political contexts. This overcomes a key limitation of existing ethical approaches, namely their lack of practical applicability. At the same time, the model differs from new approaches to algorithmic governance, which typically focus on technical solutions such as explainability or reducing bias. Whilst these contributions are important, they often remain fragmented and insufficiently linked to the broader legal and regulatory framework. The proposed model seeks to overcome this fragmentation by integrating technical, legal and ethical dimensions into a single evaluation framework.

In order for the proposed model to function not only as a conceptual framework but also as a practical tool, it is necessary to define specific protocols for its application across the following categories: supervisory bodies and regulators, digital platform operators, companies and technology developers, each of which interacts with the model at different stages of the data processing lifecycle and requires specific operational guidelines. For data protection authorities, the model can be operationalised as a structured regulatory audit protocol that complements existing compliance review mechanisms. The specific procedure involves the following steps. In the first step, the authority applies the criterion of legitimacy of purpose as a first-level filter: if the stated purpose of processing is not specific, socially significant and compatible with fundamental rights, further assessment is inappropriate. Hence, the practice must be rejected regardless of the extent to which it technically complies with formal requirements.

In the second step, the proportionality test is applied to determine the minimum necessary amount of data: the regulator must require the controller to provide documentary evidence explaining why a smaller volume or less sensitive categories of data would not suffice to achieve the stated objective. In the third step, transparency and accountability are assessed through an analysis of the system's documentation: is the algorithm explainable to a degree sufficient to challenge a specific decision; has a chain of responsibility been established between the developer, the operator and the controller? The fourth step verifies the reality of the data subject's participation: not only the formal existence of mechanisms for exercising rights, but also their accessibility, comprehensibility and effectiveness in practice. The result of the audit is not a binary compliant/non-compliant assessment, but a graded conclusion highlighting specific areas where the practice is formally lawful but substantively problematic, which provides grounds for issuing

mandatory instructions for rectification, rather than merely financial penalties. In the context of cross-border data flows, supervisory authorities can use the model as a tool for mutual recognition: two authorities from different jurisdictions, when assessing the same practice against common criteria, arrive at comparable results even in the absence of formal regulatory convergence. This is significant for authorities in countries seeking an adequacy decision from the European Commission, particularly for Ukraine in the context of harmonisation with the EU acquis.

For large platforms that process data from millions of users, the model can be integrated into internal data management processes as a tool for ethical stress-testing of new features and products prior to their launch. The specific protocol involves the following stages. During the product design phase, the responsible team conducts a structured analysis based on five criteria, documenting the responses to each in a standardised assessment form. The criterion of legitimacy of purpose requires an answer to the question: does the new feature serve a genuine user need, or is it primarily a mechanism for collecting additional data under the guise of convenience? The proportionality criterion requires a comparative analysis: were less intrusive alternatives considered, and why were they rejected? The transparency criterion requires preliminary testing for comprehensibility: can the average user, after reading the data processing notice, explain in their own words what will happen to their information?

During the internal approval stage, the assessment is submitted to an independent ethics officer or an accountability committee, which has the authority to block the launch or request further revisions. During the post-launch monitoring phase, the platform is required to track not only technical compliance metrics but also indicators of substantive legitimacy: the frequency of appeals against automated decisions, metrics on the exercise of the right to erasure, and the level of complaints regarding unclear information. The identification of systemic deviations constitutes grounds for suspending the function and conducting a re-assessment. A separate recommendation for platforms is the introduction of a public register of ethical legitimacy assessments, similar to the DPIA registers that are already mandatory in some jurisdictions. The public nature of the assessments serves a dual purpose: it provides external pressure for accountability and establishes a precedent for the industry as a whole.

For organisations developing AI-based systems or processing personal data as part of their business processes, the model can be integrated into internal compliance standards as an extended counterpart to the DPIA, calling it an Ethical-Legal Legitimacy Impact Assessment (ELPIA). The difference from a standard DPIA lies in the fact that a DPIA assesses risks to data subjects' rights within the existing legal framework, whereas an ELPIA additionally assesses whether the practice is substantively justified even if it formally complies with the law. The specific form of the ELPIA should include: a documented justification of the legitimacy of the purpose, referring not only to the legal basis for processing but also to the social significance of the purpose; a comparative analysis of proportionality, including a list of alternatives considered and rejected; the results of transparency testing on a representative group of users; an accountability chain diagram with clear personal assignments of responsibility at each stage of processing; an assessment of the effectiveness of data subject participation mechanisms, with documentation of the results of pilot testing. The ELPIA must be carried out prior to the system's launch, reviewed in the event of significant changes to the processing logic, and retained as part of corporate documentation, with access granted to regulators upon their request.

Legislators and public policy bodies. For bodies responsible for legislative regulation or the formulation of digital policy, the model can serve as a regulatory benchmark as a standard against which the quality of new regulatory initiatives is assessed. A specific recommendation is to introduce a mandatory test of ethical and legal legitimacy for draft legislation concerning the processing of personal data or the use of AI systems in the public sector. Such a test should address five questions corresponding to the model's criteria: is the purpose of the regulatory measure sufficiently specific and socially justified; are the proposed data processing mechanisms the minimum necessary to achieve this objective; does the draft legislation provide for a clear procedure for informing citizens; are clear mechanisms for institutional accountability in place; are effective tools for participation and the protection of the rights of individuals whose data is subject to regulation ensured. For Ukraine, this recommendation is particularly relevant in the context of drafting a new version of the Law “On the Protection of Personal Data”. The proposed test could be enshrined as a mandatory regulatory analysis procedure within the framework of regulatory impact assessments.

It is important to emphasise that the model does not assume ideal conditions for implementation and is designed to operate in a real-world environment characterised by institutional constraints, information asymmetry, and technological changes that outpace regulatory capabilities. In this sense, it functions as a graduated assessment system, allowing for the distinction between practices that are formally lawful but ethically problematic; partially compliant; and fully legitimate, thereby ensuring adaptability and applicability across different legal systems and at different levels of regulatory development.

5. Conclusions

In today's globalised digital environment, the right to privacy is increasingly at the centre of tensions between individual autonomy and public interest. The study's contribution to addressing this issue is threefold. Firstly, it demonstrates that the balance between privacy and public interests cannot be adequately assessed within a purely legal framework, as the concept of public interests lacks a consistent ethical threshold. Secondly, it introduces the concept of digital solidarity as a normative principle that rethinks the balance as a collective rather than a purely individual issue, shifting the analytical focus from bilateral claims to rights to systemic accountability within data ecosystems. Thirdly, it translates these conceptual advances into a structured five-criteria model that provides practical recommendations for regulatory analysis, ethical auditing and legislative reform, addressing the gap between formal compliance and substantive legitimacy, which defines the central problem of the study. Existing legal regimes, while showing progress in the normative regulation of personal data circulation, remain largely reactive and formalised, falling short of adequately addressing the moral complexity of digital transformations. The central thesis of the study is affirmed in its full significance: effective protection of personal data is possible only through the genuine integration of the ethical dimension into the structure of legal regulation - an

approach that entails not the parallel coexistence of ethics and law, but their conceptual unity.

In the course of the study, three models of ethical–legal regulation were classified, typical ethical conflicts arising in judicial practice (in particular, that of the ECtHR) were identified, and zones of synergy and tension between legal provisions and moral imperatives were analysed. The main result was the development of an integrated system of criteria for the admissibility of interference in the sphere of personal data, which combine legal certainty with ethical legitimacy. These include: legitimacy of purpose, proportionality, transparency, accountability and participation of the data subject.

The original contribution of this work lies in bridging the traditional gap between legal and ethical analysis. Unlike studies that treat ethics as a factor external to law or as post facto criticism, a conceptually sound integrated model is proposed in which ethical reflection acts as a co-founder of normative legitimacy. The formulated system of criteria is not only an analytical tool, but also a regulatory framework for the practical assessment of digital solutions, capable of shifting the focus of modern personal data regulation from formal compliance to substantive moral responsibility. The methodological value of the study lies in its interdisciplinary nature: the combination of legal doctrine, ethical theory, philosophy of technology, and analysis of judicial practice has allowed for a deeper understanding of contemporary risks and ways to address them.

The practical significance of the study allows us to formulate a number of specific recommendations for different categories of stakeholders. For Ukraine, the proposed model can serve as a basis for revising regulatory policy, in particular at the level of the Law of Ukraine 'On the Protection of Personal Data' (Verkhovna Rada of Ukraine, 2010), strengthening ethical and legal responsibility, and harmonising regulatory practice with international requirements in the field of digital privacy. For legislators and politicians, it is advisable to incorporate the proposed criteria into national legislation, update legal approaches based on ethical risk assessment, and harmonise international data protection regimes through the introduction of a unified value base. The transition to proactive regulation focused on 'ethics by design' will allow to stay ahead of threats instead of reacting to them belatedly.

For the academic community, an open avenue for further research remains the study of the evolving dynamics between law and ethics in the context of developments in artificial intelligence, biometric technologies, and automated decision-making systems. It is particularly important to develop methodologies for ethical auditing of digital practices and to integrate these approaches into educational programmes in law, IT and philosophy. For technology developers and business structures, the application of the principles of 'Privacy by Design' and 'Ethics by Design' should become not an option, but a standard for responsible technological development. The development of an internal culture of accountability, transparency and respect for user dignity should be seen as a means of obtaining not only regulatory approval but also a social licence to operate.

Further research should focus on developing mechanisms for the practical application of the proposed criteria across various sectors, including healthcare, finance, education and intellectual infrastructure. Particular attention should be paid to the contextual adaptation of ethical principles in different legal and cultural environments, as well as to the development of methodologies for the ethical auditing of digital systems. In the context of the growing complexity of global data ecosystems, the integration of ethical considerations into legal regulation appears to be a necessary condition for enhancing the legitimacy, sustainability and public perception of digital governance systems. The proposed model does not replace existing legal mechanisms, but is intended to complement them by introducing an additional level of evaluative sensitivity to issues of justice, accountability and collective impact.

CRediT authorship contribution statement

Veronika Horielova: Funding acquisition, Formal analysis, Data curation, Conceptualization. **Olena Derevianko:** Resources, Project administration, Methodology, Investigation. **Oleksii Yanushevskyi:** Writing – review & editing, Visualization, Validation, Software. **Maksym Lysak:** Writing – original draft, Visualization, Formal analysis, Conceptualization.

Ethical approval

All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Availability of data and materials

Data will be available on request.

Consent to participate

Informed consent was obtained from all individual participants included in the study.

Consent for publication

All individual participants agreed to be included in the study.

Funding

No funds, grants, or other support was received.

Conflicts of interest

The authors declare they have no financial and competing interests.

Data availability

No data was used for the research described in the article.

References

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Sergio, G., Molina, D., Benjamins, R., Chatila, R., Herrera, F., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Banks, J. (2025). Cookie fatigue and the erosion of informed consent. *Journal of Digital Ethics, 12*(1), 45–59.

Beauchamp, T. L., & Childress, J. F. (2001). *Principles of biomedical ethics*. Oxford: Oxford University Press.

Bloomberg Law. (2022). China's personal information protection law: Key compliance insights. https://www.bloomberglaw.com.

Bloomberg Law. (2025). California privacy Rights Act: Enforcement and compliance trends. https://www.bloomberglaw.com.

California Privacy Protection Agency. (2025). CPRA regulations and guidance. https://cppa.ca.gov.

Cao, J., & Meng, T. (2025). Ethics and governance of artificial intelligence in digital China: Evidence from online survey and social media data. *Chinese Journal of Sociology, 11*(1), 58–89. https://doi.org/10.1177/2057150X241313085

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. https://www.ipc.on.cam.

Cheung, A., & Chen, Y. (2021). Data governance in China: Between security and development. *China Information, 35*(1), 3–25. https://doi.org/10.1177/0920203X20976610

Chorzempa, M., Triolo, P., & Sacks, S. (2018). *China's social credit system: A mark of progress or a threat to privacy?* Peterson Institute for International Economics. https://www.piie.com.

De Hert, P., & Gutwirth, S. (2020). Data protection in the age of intelligent machines. *Computer Law & Security Review, 36*(4), 105–120.

De Hert, P., & Papakonstantinou, V. (2022). The ethical dimension of EU data protection reform. *European Journal of Law and Technology, 13*(1), 1–25.

Digichina. (2021). *Translation of China's Personal Information Protection Law (PIPL)*. https://digichina.stanford.edu.

Dittmar, E. C., Sposato, M., & Vargas Portillo, J. P. (2025). Interpreting intelligence: Organizational meaning-making processes in AI-enabled leadership development. *Journal of Information, Communication and Ethics in Society*, 1–14. https://doi.org/10.1108/JICES-05-2025-0112

ECHR. (1950). *European convention on human rights*. https://www.echr.coe.int.

Eke, D., & Stahl, B. (2024). Ethics in the governance of data and digital technology: An analysis of European Data Regulations and Policies. *DISO, 3*, 11. https://doi.org/10.1007/s44206-024-00101-6

European Commission. (2016). *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/.

European Court of Human Rights. (2008). S. and Marper v. the United Kingdom, Application nos. 30562/04 and 30566/04. https://hudoc.echr.coe.int.

European Court of Human Rights. (2017). Bărbulescu v. Romania, Application no. 61496/08. https://hudoc.echr.coe.int.

European Court of Human Rights. (2018). M.L. and W.W. v. Germany, Application nos. 60798/10 and 65599/10. https://hudoc.echr.coe.int.

European Data Protection Board (EDPB). (2023). *Guidelines on data subject rights under GDPR*. https://edpb.europa.eu.

GDPR-Text.com. (2025). *GDPR full text and commentary*. https://gdpr-text.com.

GDPRhub. (2025). Article 24 GDPR: Responsibility of the controller. https://gdprhub.eu.

Global Freedom of Expression. (2023). Bărbulescu v. Romania case summary. https://globalfreedomofexpression.columbia.edu.

Global Privacy Laws. (2025). Overview of South Korea's PIPA. https://globalprivacylaws.com.

Guenduez, A. A., Walker, N., & Demircioglu, M. A. (2025). Digital ethics: Global trends and divergent paths. *Government Information Quarterly, 42*(3), Article 102050. https://doi.org/10.1016/j.giq.2025.102050

IAPP. (2020). Brazil's LGPD: Key provisions and compliance strategies. https://iapp.org.

IBM Cost of a Data Breach Report. (2025). https://www.ibm.com/de-de/reports/data-breach.

ICO. (2025). Accountability and governance under the UK GDPR. https://ico.org.uk.

Internet Society Foundation. (2024). Ethical concerns in China's social credit system. https://www.internetsociety.org.

Kerasidou, A., & Kerasidou, C. (2023). Data-driven research and healthcare: Public trust, data governance and the NHS. *BMC Medical Ethics, 24*, 51. https://doi.org/10.1186/s12910-023-00922-z

Kloiber, D. (2021). The right to data protection: A comparative study. *Legal Bulletin, 3*.

Kolah, A. (2024). The multifaceted challenges and opportunities inherent in data protection and privacy regulation. *Data Protection Journal, 11*(1), 15–32.

Kuner, C., Bygrave, L. A., & Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

Law.asia. (2022). *Data protection trends in Asia-Pacific*. https://law.asia.

Murrell, G. (2018). Surveillance and privacy in China's digital governance. *Asian Journal of Law and Society, 5*(1), 89–104.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Stanford Law Review, 79*(1), 119–157.

PDPC. (2023). Singapore's Personal Data Protection Act (PDPA). https://www.pdpc.gov.sg.

Privacy Matters. (2025). China's data localization requirements under PIPL. https://privacymatters.org.

Qiu, Y., & Hu, Z. (2025). Progress and recommendations in data ethics governance: A transnational analysis based on data ethics frameworks. *Humanities and Social Sciences Communications, 12*, 1354. https://doi.org/10.1057/s41599-025-05664-4

RUSI. (2025). Cybersecurity and state surveillance: Comparative analysis. https://rusi.org.

Sampson, T. (2021). The ethics of consent in digital environments. *Journal of Information Ethics, 30*(2), 101–118.

Shamov, O. (2025). AI and copyright: From a doctrinal crisis to a hybrid model of collective licensing. *Legal Horizons, 26*(3), 68–76. https://doi.org/10.54477/LH.25192353.2025.3

Sposato, M., Dittmar, E. C., & Vargas Portillo, J. P. (2026). Navigating the dark side of AI in service ecosystems: An ethical leadership framework for risk mitigation. *Service Industries Journal*. https://doi.org/10.1080/02642069.2026.2643384

StratCom. (2021). China's social credit system: Strategic implications. https://stratcomcoe.org.

UNCTAD. (2025). UNCTAD Digital Economy Report 2024. https://unctad.org/publication/digital-economy-report-2024.

Verkhovna Rada of Ukraine. (2010). *Law of Ukraine "On Personal Data Protection" no. 2297-VI of June 1, 2010*. Official Portal of the Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2297-17.