Centro Sur Vol. 10 No. 3 - July - September – Revista Centro Sur - eISSN: 2600-5743

http://centrosureditorial.com/index.php/revista

Ethics and Legality in Artificial Intelligence-Based Applications: A Review and Commentary on European Data Protection Regulations

Ética y legalidad en Aplicaciones Basadas en Inteligencia Artificial. Revisión y comentarios de la normativa europea sobre la protección de datos

Fabian Marcelo Salinas
Professor, Catholic University of Cuenca, Law Program
Fabiansalinas@ucc.edu.ec
https://orcid.org/0009-0007-2958-0474

ABSTRACT

This research analyzes the tension between the development of Artificial Intelligence and the protection of personal data, comparing the European Union's regulatory framework with Ecuador's legal system. The results highlight the consolidation of "informational self-determination," which grants users absolute control over their data, including rights of access, rectification, and erasure. However, a critical technical conflict is identified due to the opacity of machine learning algorithms, which function as "black boxes" that are difficult to interpret and carry discriminatory biases inherited from historical data. Given this, data governance in sensitive sectors such as healthcare and education requires oversight by specialized delegates and bioethics committees. Finally, it is concluded that Ecuadorian legislation exhibits institutional shortcomings and legal fragmentation, making it insufficient to standardize its technologies in the international markets of Europe and the United States.

https://doi.org/10.37955/cs.v3i2.420
Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

RESUMEN

Esta investigación analiza la tensión entre el desarrollo de la Inteligencia Artificial y la protección de datos personales, comparando el marco normativo de la Unión Europea con el ordenamiento jurídico de Ecuador. Los resultados destacan la consolidación de la "autodeterminación informativa", que otorga al usuario el control absoluto sobre sus datos, incluyendo derechos de acceso, rectificación y supresión. Sin embargo, se identifica un conflicto técnico crítico debido a la opacidad de los algoritmos de aprendizaje automático, que funcionan como "cajas negras" difíciles de interpretar y arrastran sesgos discriminatorios heredados de datos históricos. Ante esto, la gobernanza de datos en sectores sensibles como la salud y la docencia exige la supervisión de delegados especializados y comités de bioética. Finalmente, se concluye que la legislación ecuatoriana presenta falencias institucionales y dispersión jurídica, resultando insuficiente para homologar sus tecnologías en los mercados internacionales de Europa y Estados Unidos.

Keywords / Palabras clave

Informational self-determination, Algorithmic bias, Data governance

Autodeterminación informativa, Sesgo algorítmico, Gobernanza de datos

Introduction

The Spanish Constitution was a pioneer in recognizing the fundamental right to personal data protection when it stipulated that “the law shall limit the use of information technology to guarantee the honor and personal and family privacy of citizens and the full exercise of their rights,” demonstrating a visionary stance on the current challenges facing a society based on data analysis. This law aims to establish the fundamental right of individuals to the protection of personal data; it applies to any partially or fully automated processing of personal data, as well as to the non-automated processing of personal data contained in or intended to be included in a file. The data protection principles include regulations on data accuracy, confidentiality, data processing based on the data subject’s consent, consent of minors, processing required by law, public interest, criminal data, and—within the special categories—it makes specific

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

mention of data processing in the field of health. Across all these areas, the law emphasizes that users must be aware of what their data will be used for and how it will be used; consent must be obtained from the data subject for its use; and the data subject may request that the data be corrected to ensure its accuracy (Office of the President, 2018).

Under this law, the user to whom this information refers has full control over what can be done with their data; all procedures must be completely transparent. Since the individual is aware of the purpose for which their information is being used, they may access the study being conducted with their data at any time to verify that it is being used correctly, exercising their right of access, rectification, erasure, restriction of processing, data portability, and objection. Users may decide to have their data completely deleted from any file or database of their choosing, or to suspend the use of their data, among other options. It is a significant achievement that the individuals to whom this information pertains are given a fundamental role in decisions regarding their data, thereby curbing the business of data trading and demanding the respect users of this information deserve—namely, the right to know and be aware of how their information will be used (from the Office of the President, 2018).

For those who work with this information, there are strictly restrictive guidelines; therefore, data analysts must thoroughly review the law to avoid committing serious violations. This law places a very heavy burden of responsibility on data analysts, so they must undergo special preparation and training to perform their work properly. This may, to some extent, limit the freedom previously enjoyed in analyzing and processing data, potentially prohibiting the use of certain algorithms that have been widely used, particularly in the profiling of individuals. This law highlights the importance of human interpretability in algorithm design (from the Office of the President, 2018; Goodman and Flaxman, 2017).

This law enshrines the right to non-discrimination for users, and this poses a serious problem, since the use of algorithmic profiling is inherently discriminatory, categorizing individuals according to certain variables; and since the data contains information on inequality, exclusion, and other traces of discrimination, algorithms trained on this data will evidently also exhibit this bias. As for data transparency, it is currently extremely difficult to comply with this regulation, since some supervised machine learning algorithms use correlations or associations that go beyond statistical significance and

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

lack an explanation that can be understood by a human (Goodman and Flaxman, 2017).

The creation of this law can be likened to the implementation of bioethics committees for research involving human subjects, which require researchers to conduct their work with patients in mind and in accordance with the principles of beneficence, non-maleficence, autonomy, and justice (Office of the President, 2018; Lolas, 2008; UNESCO, 2009).

In addition to the special care that data analysts must exercise when working with personal information, it is considered necessary to appoint a data protection officer when the study is conducted by certain institutions, notably educational institutions offering instruction at any level. In the field of health, while healthcare facilities are required to maintain patients' medical records, healthcare professionals are exempt from this requirement, although they are legally obligated to maintain their own patients' medical records. Data processing in health research may utilize tools such as informed consent, provided that research involving patient data has been previously approved by a bioethics committee for research involving human subjects (Presidency of the Republic, 2018; He et al., 2019).

Challenges in Artificial Intelligence Regarding Compliance with Legislation

There is a clear need to redesign algorithms and data processing systems to ensure interpretability by those involved in data collection, from the analyst to the individual from whom the information originates. This opens up a new potential field of study within Artificial Intelligence, enabling the translation of information that has thus far been treated as "black boxes"—where it is neither relevant nor necessary to understand what is happening as long as the necessary connections are made to produce a successful output— all the way to "open" systems specifically designed for machine learning tasks involving personal data.

The processing of personal information presents a significant challenge if it is to be carried out by automated or semi-automated information-selection systems. The goal is to find a way to analyze attributes and their correlations that can eliminate attributes that may lead to discrimination against individuals based on race, gender, etc., as well as any information correlated with these attributes or from which a sensitive factor about the individual might be inferred. This

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

information processing is similar to what is required for data anonymization; this process must be carried out automatically and reviewed by a data protection officer, who examines the entire dataset before analysts or other relevant parties work with it and ensures compliance with established regulations.

The application of European data protection regulations is of global importance, as it requires individuals who develop applications using personal data—and who wish to market their product in Europe, conduct business with the European Union, or access data from individuals residing within the European Union—to comply with all guidelines established by this law, regardless of the regulations in their country of origin. Therefore, from a legal standpoint, countries must establish new data regulations to ensure compliance with the most important global standards (Europe, the United States, China), thereby eliminating any risk of noncompliance.

Ecuador's Legal Framework on Personal Data Protection

Following the massive personal data breach in September 2019, the Ministry of Telecommunications submitted a draft data protection law, the "Organic Law on the Protection of Personal Data," adapting the law to the current reality of a society based on the consumption and generation of personal data. To this end, Ecuador proposes the adaptation and adoption of the proposed declaration of principles on privacy and personal data protection in the Americas, along with accompanying legal regulations that govern and regulate the collection and processing of personal data. The points addressed in the proposed law include the legitimacy and lawfulness of data, an analysis of the purpose for which the data will be used, the relevance and minimization of personal data, the proportionality of processing, consent, confidentiality, quality, retention, security, and accountability regarding the data (Presidency of the Republic of Ecuador, 2019).

The Ecuadorian bill was an important step forward in data protection, but it has legal—rather than technical—shortcomings that affect its applicability within Ecuador's legal framework and render it insufficient for AI and Big Data projects to be commercialized or implemented in the European Union or the United States, as it does not adequately comply with all the regulations established by those jurisdictions (Enriquez Alvarez, 2017).

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

A foundation must be established to clarify how data is processed. Thus, the Organic Law on Transparency and Access to Public Information (LOTAIP), in Article 1, establishes that "Access to public information is a right of individuals guaranteed by the State." The provisions enshrined in this organic law enable several things, including: safeguarding personal information and promoting the democratization of society. Compliance with international conventions, among other elements that facilitate the transparency of processes regarding the handling of public data (National Congress, 2004) .

Furthermore, Article 6 of the LOTAIP establishes guidelines regarding confidential information. This is defined as information derived from the most personal and fundamental rights, as set forth in Articles 23 and 24 of the Constitution of Ecuador.

In addition to these provisions, Articles 5 and 6 of the LOTAIP define what constitutes public information and what constitutes private or confidential information. In the first case, information is considered public when any document, in any format, is held by public institutions and legal entities covered by this Law. As for confidential information, private information is defined as public information that is not subject to the principle of disclosure. The misuse of this information will result in appropriate legal action (National Congress, 2004) .

On the other hand, private information or information subject to the regulations of the Ecuadorian Institute of Intellectual Property (IEPI) shall be governed by the provisions set forth in the Organic Code on the Social Economy of Knowledge, Creativity, and Innovation. This Code emphasizes the creation of knowledge and how it will be transmitted and managed, with the aim of making efficient use of these resources. Article 39 of this law establishes universal, free, and secure access to knowledge in digital environments. This will be achieved through digital platforms and information technologies, prior to the declaration of copyright, and through the use of Creative Commons licenses that restrict its use and application (National Assembly of Ecuador, 2016) .

Similarly, based on the regulations set forth by the IEPI and specifically Article 81 thereof, the process for technology transfer is outlined. This process will be carried out to transfer knowledge, techniques, or technological processes that enable the development of products and services (National Assembly of Ecuador, 2016) . To this

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

end, contractual arrangements will be utilized, such as proof of concept, technological validation, and licensing, among others. From a legal standpoint, these must be properly substantiated.

It should also be noted that certain content will not be publicly accessible in a database. Intellectual property rights constitute an exception to the public domain; thus, to promote culture, artistic development, and technological advancement, one must adhere to principles of social responsibility, ethics, and morality, as well as to the laws established by both the Constitution and the Intellectual Property Law regarding data classified as private, state-owned, community-owned, or mixed.

However, it is important to note the moral rights that must be present in every project or work; these stem from Article 118 of the Intellectual Property Law. This article stipulates that unpublished works must be preserved and made public, with an emphasis on the creation of artificial intelligence, which will be closely linked to the moral principles established by the Constitution and the law. It should be noted that, although there is no explicit provision within Ecuador regarding the creation of artificial intelligence, this will be subject to the interpretation and scrutiny of the entities responsible for enforcing the law (National Assembly of Ecuador, 2016) .

Among other elements outlined in the law, issues such as data ownership and how such data is regulated under Ecuadorian law are clarified. Compared to the European Union's approach, there are still gaps in the development of information infrastructure, raising questions such as how, in the 21st century, data can be managed without compromising the integrity of a country, a region, a municipality, or an individual. To this end, the creation of Creative Commons—which is already being implemented on the internet—bases its structure on the legal framework provided by each country, region, and the global community (Vera, 2013) .

Judicial Safeguards

Art. 91.—The purpose of an action for access to public information is to guarantee access to such information when it has been expressly or tacitly denied, or when the information provided is incomplete or unreliable. Such an action may be filed even if the denial is based on the information's classification as secret, restricted, confidential, or any other classification. The restricted nature of the information must

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

be declared prior to the request by a competent authority and in accordance with the law. (VERBATIM).

Art. 92.—Every person, in their own right or as a representative authorized for that purpose, shall have the right to be informed of the existence of and to access documents, genetic data, databases or files containing personal information, and reports concerning themselves or their property that are held by public or private entities, whether in physical or electronic form. Likewise, they shall have the right to know how such information is used, its purpose, the origin and destination of personal information, and the retention period of the file or database. Those responsible for personal data banks or files may disclose the archived information with the authorization of the data subject or as authorized by law. The data subject may request from the data controller free access to the file, as well as the updating, correction, deletion, or erasure of the data. In the case of sensitive data—the storage of which must be authorized by law or by the data subject—the adoption of necessary security measures will be required. If your request is not addressed, you may bring the matter before a judge. The affected individual may file a lawsuit for damages incurred. (VERBATIM).

In accordance with our Constitution, these two articles constitute the legal framework governing the use of data and the right of all Ecuadorian citizens and foreign residents to access their data and publicly available information. To provide context for this issue, we will refer to JUDGMENT 001-14-PJO-CC, which is a (BINDING JUDICIAL PRECEDENT). This ruling serves as the basis when a natural or legal person asserts these constitutional rights through the courts.

In accordance with the eighth paragraph of Article 9 of the Law on Electronic Commerce, Signatures, and Data Messages, published in the Official Register, Supplement No. 557, dated April 17, 2002, “Personal data” refers to “data or information of a personal or intimate nature that is subject to protection under this law.”

In other legislation and in legal doctrine, access to public information is referred to as “improper habeas data.” Bruno Gaiero and Ignacio Soba, *La Regulación Procesal del Habeas Data* (The Procedural Regulation of Habeas Data), Editorial B de F, Buenos Aires, 2010, p. 48, describe the legal concept as follows: “Currently, there is a marked tendency to establish a special framework to facilitate this claim

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

(access to public information), generally referred to as 'improper habeas data.' Although habeas data was originally conceived as a guarantee of access to personal data, over time it began to be applied, by extension, to data held by the government for the purpose of clarifying the activities carried out by those in power. This is the crystallization of what came to be known as "improper habeas data." It is clear that, due to the similarity of the subject matter—as well as, , because of how blurred the line between what constitutes public information and what constitutes personal information can become—the two guarantees can be confused. However, the prerogatives or "legal positions" that can be derived from each right are undoubtedly distinct. While the right to public information is limited to mere access, the scope of action regarding personal information expands significantly."

Art. 66.—The following rights of individuals are recognized and guaranteed: paragraph 19. The right to the protection of personal data, which includes access to and control over such information and data, as well as their corresponding protection. The collection, storage, processing, distribution, or dissemination of such data or information shall require the authorization of the data subject or a statutory mandate.

The right to the protection of personal data is complex in nature and encompasses various dimensions related to "personal" information. This concept is articulated in legal doctrine by Óscar Puccinelli, who states the following: "The 'right to data protection' is understood as the sum of principles, rights, and guarantees established in favor of individuals who may be harmed by the processing of personal data pertaining to them."

As the author rightly notes, the right to data protection—and specifically, its element known as "informational self-determination"—is instrumental in nature, subordinate to the protection of other constitutional rights that may be affected when personal data is used, such as privacy, honor, psychological integrity, etc.,

Oscar Puccinelli, *Habeas Data in Indo-Ibero-America*, Temis, Bogotá, 1999, p. 68.

Informational self-determination entails the right of every person to exercise control over personal information concerning them, vis-à-vis any public or private entity. This right was first invoked by the Federal

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

Constitutional Court of Germany in its ruling on the Census Act of December 15, 1983, which empowers individuals to decide and consent, freely and with full knowledge of the facts, to the use of their personal data by third parties in the context of automated data processing.

Sustainable urban planning has established itself as a fundamental strategy in Latin America to address challenges associated with the accelerated growth of cities, disorderly urban sprawl, territorial inequality, and increasing exposure to natural hazards (UN-Habitat, 2022). In this context, territorial planning is a key tool for promoting balanced development, improving the population's quality of life, and ensuring the efficient and sustainable use of available resources.

Sustainable urban planning has established itself as a fundamental strategy in Latin America, a region where over 80% of the population resides in urban centers. However, implementing these frameworks requires navigating a complex reality marked by deep socioeconomic inequalities and rapid, often informal, peripheral growth.

Traditional planning models frequently clash with the spontaneous expansion of informal settlements, where vulnerable communities lack critical access to clean water, basic sanitation, and reliable public transit. Additionally, Latin American cities face escalating climate vulnerabilities—ranging from landslides in steep Andean terrain to severe flooding in coastal hubs—making urban resilience a matter of immediate survival rather than a theoretical ideal.

To address these pressing challenges, current regional strategies are increasingly incorporating contemporary models such as Transit-Oriented Development (TOD) and nature-based solutions to mitigate urban sprawl and protect endangered ecosystems. Local governments are working to align municipal master plans with global mandates, such as the New Urban Agenda and SDG 11.

Yet, a persistent implementation gap remains. While many countries have highly progressive national land-use legislation, local municipalities often lack the administrative, financial, and enforcement capabilities needed to curb aggressive real estate speculation and regulate land use effectively. Ultimately, sustainable urban planning in Latin America is evolving beyond simple aesthetic zoning toward a model of participatory governance, aiming to bridge the stark divide between the formal and informal city.

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

In Ecuador, territorial planning is regulated by the Constitution of the Republic of Ecuador (2008), the Organic Code of Territorial Organization, Autonomy, and Decentralization (COOTAD, 2010), and the Organic Law on Territorial Planning, Land Use, and Management (LOOTUGS, 2016). These instruments establish the powers of the Decentralized Autonomous Governments and the necessary mechanisms for the planning, management, and regulation of land use through tools such as the Development and Territorial Planning Plan (PDOT) and the Land Use and Management Plan (PUGS) (Constitution of the Republic of Ecuador, 2008; COOTAD, 2010; LOOTUGS, 2016).

Within this framework, the canton of Latacunga is a relevant case study due to its importance as an urban center in the province of Cotopaxi and its historical exposure to volcanic threats associated with the Cotopaxi volcano. This situation poses significant challenges for territorial planning and risk management. Therefore, this paper analyzes the relationship between the current regulatory framework and the application of land-use planning instruments in Latacunga, with the aim of identifying their contribution to sustainable development and the reduction of territorial vulnerability.

Materials and Methods

This research is framed within a qualitative, documentary-analytical design. It is based on the systematic review, critical interpretation, and comparison of regulatory frameworks, constitutional texts, draft legislation, and specialized scientific literature addressing the intersection between ethics, legality, and the development of technologies based on Artificial Intelligence (AI) and big data. The methodological approach adopted does not seek to quantify variables, but rather to gain a deep understanding of the phenomenon of “informational self-determination” and the technical and legal limitations faced by contemporary legislation, with a comparative emphasis on the regulatory framework of the European Union and the legal system of the Republic of Ecuador.

To ensure the validity and rigor of the findings, the units of analysis were strictly defined and categorized as follows:

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

A. International and European Regulations

European Union Regulations: Analysis of guidelines regarding the protection of personal data in automated environments, aimed at ensuring algorithmic transparency and the right to an explanation.

Universal Declarations: Incorporation of the principles of UNESCO's Universal Declaration on Bioethics and Human Rights, used as a regulatory analogy for data governance.

B. Ecuadorian Regulations and Case Law

Constitution of the Republic of Ecuador: Specifically, Article 66, paragraph 19, which recognizes the fundamental right to the protection of personal data; as well as Articles 91 and 92 on the judicial guarantees of Access to Public Information and Habeas Data.

Organic Laws and Codes: Review of the Organic Law on Transparency and Access to Public Information (LOTAIP), the Organic Code on the Social Economy of Knowledge, Creativity, and Innovation, and the Law on Electronic Commerce, Signatures, and Data Messages.

Bills and Judicial Doctrine: Evaluation of the Draft Organic Law on Personal Data Protection submitted by the Ministry of Telecommunications in September 2019, and analysis of the binding precedent established by Ruling 001-14-PJO-CC of the Constitutional Court of Ecuador.

Heuristics and Document Selection. An exhaustive search and selection of official documents and indexed articles was conducted using key descriptors such as "ethics in AI," "data protection," "habeas data," "algorithmic profiling," and "informational self-determination." Priority was given to sources that linked the limitations of machine learning algorithms to the fulfillment of fundamental rights.

Legal Hermeneutics and Interpretation. In this stage, the hermeneutic method was applied to unravel the meaning and scope of written norms. The fundamental principles of data protection under European law (accuracy, confidentiality, explicit consent, processing limitation, and portability) were analyzed in light of the realities of "black box" technologies that hinder human interpretability. Likewise, the doctrinal construct of informational self-determination—which originated in German case law (the 1983 Census Act ruling)—and its reception in Latin American legal doctrine were analyzed.

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

Comparative and Technical Analysis. The robustness of global regulatory frameworks was compared with the Ecuadorian legal ecosystem. The legal shortcomings of the 2019 Ecuadorian proposal were critically examined in light of the requirements of the European and U.S. markets. In turn, the concepts of public, confidential, and private information defined in the LOTAIP were contrasted with the rights of exclusion derived from intellectual property and the use of open licenses such as Creative Commons.

Critical Synthesis and Categorization. Finally, the information was processed, coded, and structured into three essential thematic areas that guide the research discussion:

The role of the data analyst and the challenges of algorithmic bias: Assessment of the legal liability of data scientists and the dilemma of indirect discrimination introduced by training data that reflects historical inequities.

Procedural safeguards against automated processing: Operational distinction between the right of access to public information (improper habeas data) and the right to personal data protection (pure habeas data).

Data governance in specialized fields: Ethical and methodological implications of using sensitive data in the fields of health, medical research, and education.

Since the research addresses the legal framework of ethics and privacy, the methodological design strictly adheres to principles of scientific integrity. Direct informed consent from human subjects was not required due to the strictly documentary nature of the primary data. The validity of the study is ensured through the triangulation of sources: the direct comparison of constitutional texts, current organic laws, and publications by experts in information and computer law.

Results

The documentary analysis and hermeneutic interpretation of regulatory and doctrinal texts made it possible to structure the findings around the tension between technological innovation driven by Artificial Intelligence (AI) and the ethical-legal frameworks designed to safeguard individuals' fundamental rights. The results have been organized according to regulatory asymmetries, the

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

challenges of algorithmic opacity, and the state of legislation in the Ecuadorian context compared to European standards.

The New Paradigm of Informational Self-Determination and User Control

One of the most significant findings concerns the evolution of the right to personal data protection, whose modern legal origins can be traced to the Spanish Constitution, which was a pioneer in recognizing the need to restrict the use of information technology to protect honor and family and personal privacy. This approach has evolved conceptually toward "informational self-determination," a doctrinal construct established through the case law of the German Federal Constitutional Court in its ruling on the 1983 Census Act.

The research demonstrates that informational self-determination is not a static right, but rather an instrumental and complex power that grants individuals full control over their personal data vis-à-vis public or private entities. This control is exercised through a set of procedural rights that transform the relationship between citizens and the entities that process their information:

Explicit Consent and Awareness of Purpose: The user must be fully aware of what data is being collected and for what specific purposes it will be processed. Any collection, processing, or distribution of data requires the explicit authorization of the data subject or a direct mandate from the law.

Right to Rectification and Maintenance of Accuracy: Users have the unequivocal right to demand that their data be corrected or updated to ensure its accuracy within any storage system.

Right to erasure and portability: The regulations under review empower individuals to autonomously decide to completely delete their information from specific databases or to revoke the previously granted permission to use such data.

This paradigm shift represents a structural milestone in the contemporary digital economy, as it directly impacts the market and trade in big data. By transferring decision-making power to the data subject, corporations and developers are compelled to establish fully transparent processes.

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

Technical and Liability Challenges for Analysts in AI Environments

The results reveal a critical gap between the requirements imposed by the regulatory framework and the technical feasibility of implementing them in advanced machine learning models. The legislation introduces restrictive guidelines and an unprecedented burden of legal and ethical responsibility on data scientists and analysts. This legal pressure requires professionals to undergo continuous specialized training to avoid committing serious legal violations during the design of automated systems.

However, this regulatory rigidity imposes substantial barriers to free technical development, limiting the analytical flexibility that existed before these regulations took effect. The analysis identifies three critical technical problems in the use of contemporary algorithms:

The Problem of Inherently Discriminatory Profiling

Legal frameworks explicitly prohibit discrimination in automated processing. However, the analysis shows that algorithmic profiling algorithms are inherently discriminatory due to their very functional nature, which consists of categorizing and segmenting individuals based on specific variables. Since the historical datasets used to train AI contain deep-rooted biases, inequities, and patterns of social exclusion, the resulting algorithms mathematically reproduce and amplify these discriminatory biases.

The Opacity of "Black Boxes" vs. the Right to an Explanation

Regulations require that algorithmic co-design take into account human interpretability and users' right to receive a comprehensible explanation of the automated decisions that affect them. The study demonstrates the extreme technical complexity of meeting this requirement with current supervised machine learning models. These models operate through complex associations and correlations that defy traditional statistical understanding, lacking a linear logic that can be translated into language comprehensible to a human being. The common practice in AI of prioritizing successful data outputs without understanding the internal processing (black boxes) directly conflicts with legal transparency requirements.

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

The Need for Automated Mitigation Systems

Given these limitations, the results suggest that the future development of AI must be reoriented toward the creation of "open" systems and the co-design of algorithms capable of processing data ethically. This involves developing automation tools that detect and remove from training datasets those sensitive attributes (race, gender, etc.) or correlated variables from which any factor of discrimination or vulnerability might be inferred. This process of automated filtering and anonymization must be complemented by human oversight exercised by a Data Protection Officer before analysts are granted access to the final dataset. To provide a structured overview of the findings, the following table summarizes the operational characteristics, protected rights, shortcomings, and ethical implications identified in the various legal instruments and frameworks analyzed.

Table 1. *Analysis of Results.*

Regulatory Framework / Instrument	Main Approach and Guaranteed Rights	Technical or Legal Limitations and Shortcomings	Impact on AI Development and Applied Ethics
European Data Protection Regulations (General Data Protection Regulation)	Guarantees the user's absolute control over their data. Recognizes the rights of access, rectification, erasure, restriction of processing, data portability, and objection. Requires algorithmic transparency and the right to receive a clear explanation of automated decisions.	It presents a significant challenge for practical application when dealing with supervised machine learning models featuring "black box" structures that lack direct human interpretability.	It restricts the prior freedom to process data. It potentially prohibits the use of traditional mass profiling algorithms due to their inherently discriminatory bias. It functions in a manner analogous to medical bioethics committees.
Constitution of the Republic of Ecuador (Arts.	It recognizes the fundamental right to personal data protection. It	It creates procedural confusion within the	It makes the use of big data subject to the express authorization of the data subject or a legal mandate.

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

66, no. 19, 91, and 92)	establishes the judicial safeguards of pure *Habeas Data* (to access, update, correct, or delete personal information) and Access to Public Information (improper *Habeas Data*).	judicial framework due to the fine line between information that is public in nature and that which is strictly confidential or personal.	It provides a solid legal basis for claims for damages arising from unlawful processing.
Draft Organic Law on Personal Data Protection (Ecuador, 2019)	Adaptation of international principles following massive data breaches. It regulates the principles of legitimacy, lawfulness, specified purpose, relevance, data minimization, proportionality, confidentiality, and security.	It has legal and institutional shortcomings rather than technical ones, which limits its practical applicability within the national legal system and prevents its international recognition.	It is insufficient to allow local developments in AI and *Big* Data to be exported, commercialized, or formally validated in the markets of the European Union or the United States.
Organic Code on the Social Economy of Knowledge (Ecuador - IEPI)	t regulates technology ransfer and the efficient nanagement of nowledge through ontractual agreements. t guarantees universal nd secure access in igital environments hrough the use of open icenses such as *Creative Commons*.	Intellectual property rights serve as an exception to the public domain. There are no explicit guidelines regarding authorship or moral rights for works generated autonomously by artificial intelligence.	It subjects technological developments and algorithms to the restrictive interpretation of intellectual property regulators, under constitutional principles of morality and social responsibility.

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

The Ecuadorian Context: Limited Progress and International Discrepancies

A detailed analysis of Ecuador's legal situation reveals a scenario of regulatory reaction to information security crises, characterized by the existence of scattered and disjointed regulations compared to unified global frameworks. The proposed Organic Law on Personal Data Protection, spearheaded by the Ministry of Telecommunications in September 2019 following a massive data breach in the country, sought to adapt the local legal framework to a consumer society and the massive generation of personal data. To this end, it proposed adopting the privacy principles set forth in the Declaration of the Americas, structuring key pillars around proportionality, confidentiality, and the minimization of collected data.

However, the results conclusively demonstrate that this regulatory effort suffers from structural legal shortcomings that drastically limit its applicability and impact. When compared to robust foreign regulations (such as those in Europe or the United States), Ecuadorian legislation exhibits technical gaps and operational loopholes that prevent local technology- and AI-based companies from competing globally. Software products and big data architectures developed under this local framework fail to reliably meet the standards required for international trade or cross-border data exchange with the European Union. This creates an urgent need to overhaul domestic regulations to align them with the world's three major regulatory blocs—Europe, the United States, and China—thereby mitigating the risk of technological trade exclusion.

Furthermore, Ecuador's legal ecosystem is characterized by fragmented criteria regarding the management of technical knowledge. The Organic Law on Transparency and Access to Public Information (LOTAIP) draws the formal boundaries between the right to access documents held by state institutions (public information) and data derived from strictly personal rights that are not subject to the principle of public disclosure (confidential information).

However, when the analyzed information or the developed algorithm falls within the scope of intellectual property, the legal framework shifts to the Organic Code on the Social Economy of Knowledge, Creativity, and Innovation. This body of law introduces essential concepts such as "proof of concept" and "technological validation" to

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

contractually regulate the transfer of technological processes aimed at creating commercial products and services. It also promotes open access on digital platforms by using Creative Commons licenses to define creators' rights regarding restrictions and usage.

Despite these tools, the findings reveal that Ecuadorian law does not include explicit regulations governing intellectual products generated automatically by artificial intelligence. This complete lack of positive law leaves the resolution of conflicts to the exclusive interpretation and judgment of the judges and administrative bodies that administer the country's laws, which introduces a high degree of legal uncertainty for investments and research in the field of data science.

Sectoral Data Governance and Ethical Analogies

A cross-cutting methodological finding of this research is the identification of an operational convergence between data governance in Artificial Intelligence and the historical structuring of medical bioethics and human research committees. The introduction of strict regulations on the processing of personal data mirrors the logic of the principles of beneficence, non-maleficence, autonomy, and justice, forcing software designers to structure their algorithms with the rights of users and data subjects as a top priority.

This bioethical approach takes on critical importance in data governance within sectors of high social sensitivity, such as education and public health:

Educational Environments and Delegation of Responsibilities: Research reveals that data analysis within educational institutions and schools at any level requires the formal appointment of a Data Protection Officer. This role is indispensable due to the risks posed by automated profiling of student performance or the behavior of minors on learning platforms.

Healthcare Management and Medical Research: In the healthcare sector, the findings reveal a duality in information archiving responsibilities. While healthcare institutions and facilities are strictly required by law to securely maintain their patients' medical records, individual medical professionals enjoy certain operational exceptions regarding the direct management of such records, without prejudice to their general obligation of confidentiality.

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

Surgical Use of AI in Medicine: For the practical implementation of machine learning and AI tools applied to predictive or diagnostic medicine, the research highlights the need to employ strict informed consent mechanisms. Such consent, along with the technical protocols for clinical data collection, must receive prior and explicit approval from a duly accredited bioethics committee for research involving human subjects before any computational processing of patient data is authorized.

Finally, the results demonstrate that the two legal safeguards enshrined in the Ecuadorian Constitution—Access to Public Information and Habeas Data—exhibit profound operational differences that are often conflated in judicial practice due to the similarity of the subject matter. While Access to Public Information (improper habeas data) is strictly limited to allowing mere access to information held by the State to ensure transparency in the actions of government officials, pure Habeas Data (regulated by Article 92 of the Constitution) significantly expands the scope of citizens' rights. The latter entitles the data subject not only to learn of the existence of their data or the use, origin, destination, and validity of their personal information in public or private records, but also to demand the updating, correction, or free deletion of such information, or the adoption of advanced security measures in the case of sensitive data, thereby strengthening the legal foundation for informational self-determination in the region.

Conclusions

A detailed analysis of the regulatory, ethical, and technical frameworks addressed in this literature review allows us to draw the following conclusions:

The fundamental right to personal data protection has evolved from a traditional guarantee of privacy to the complex concept of informational self-determination, which grants citizens absolute, informed, and transparent control over the purpose, access, correction, and complete deletion of their personal information in any analytical environment.

There is a critical and insurmountable gap between the regulatory requirements of international law (particularly European law) and the current technical feasibility of Artificial Intelligence; advanced supervised machine learning models operate as inherently

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

discriminatory and opaque "black boxes," which hinders the effective fulfillment of the user's right to receive an understandable and unbiased explanation.

The design, co-design, and implementation of Artificial Intelligence and Big Data systems necessitate a shift in the analytical paradigm, moving away from the traditional approach— —that focuses solely on the success of outputs toward open systems that automate the anonymization and removal of sensitive attributes under the strict oversight of a Data Protection Officer.

The governance of mass data processing shares an essential functional parallel with medical bioethics committees, demonstrating that in sectors of high social vulnerability—such as healthcare and education—the application of algorithms and the use of medical records must be subject to the principles of autonomy, justice, beneficence, and the rigorous use of duly monitored informed consent.

In the Ecuadorian context, the current regulatory ecosystem exhibits serious technical gaps and institutional shortcomings that limit its applicability and prevent the standardization of its technological developments in international markets such as the European or U.S. markets; Furthermore, the lack of explicit guidelines on AI-driven automated creation within the Organic Code of the Social Economy of Knowledge subjects this field to latent legal uncertainty and discretionary interpretation.

The jurisdictional guarantees enshrined in the Ecuadorian Constitution make a clear distinction between Access to Public Information (improper habeas data), which focuses on the transparency of government administration, and Habeas Data (in the strict sense), which stands as the ideal instrument for exercising cost-free control over the use, validity, updating, and deletion of personal and sensitive data.

References

National Assembly of Ecuador. (2016). Organic Code on the Social Economy of Knowledge, Creativity, and Innovation. *Official Register*, *IV*(899), 113. [suspicious link removed]

National Congress. (2004). Organic Law on Transparency and Access to Public Information. LOTAIP, 1–10. https://doi.org/10.1111/jfr3.12162

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743

Office of the President, M. (2018). *Organic Law 3/2018, of December 5, on the Protection of Personal Data and the Guarantee of Digital Rights* (Technical Information). https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Enriquez Alvarez, L. (2017). Paradigms of Personal Data Protection in Ecuador. Analysis of the Draft Organic Law on the Protection of the Rights to Privacy and Confidentiality Regarding Personal Data. *Law Review*, 43–61. http://www.fundamedios.org/wp-content/uploads/2016/09/proyecto-ley-de-datos.pdf

Goodman, B., and Flaxman, S. (2017). European Union Regulations on Algorithmic Decision-Making and the Right to Explanation. *AI Magazine*, *38*(3), 50–57. https://doi.org/10.1609/aimag.v38i3.2741

He, J., Baxter, S. L., Xu, J., Xu, J., Zhou, X., and Zhang, K. (2019). The practical implementation of artificial intelligence technologies in medicine. **Nature Medicine**, *25*(1), 30–36. https://doi.org/10.1038/s41591-018-0307-0

Lolas, F. (2008). Bioethics and animal research. A personal perspective and a note on the contribution of Fritz Jahr (Vol. 41; Technical Report).

Presidency of the Republic of Ecuador. (2019). *Organic Law on the Protection of Personal Data* (Technical Information). https://www.nmslaw.com.ec/

Puccinelli, O. (1999). *Habeas Data in Indo-Ibero-America*. Temis.

UNESCO. (2009). Universal Declaration on Bioethics and Human Rights. *Bioètica & debat: Open Forum of the Borja Institute of Bioethics*, *15*(55), 8–14. http://portal.unesco.org/es/ev.php-URL_ID=31058&URL_DO=DO_TOPIC&URL_SECTION=201.html

Vera, A. (2013). *Practical Guide to Creative Commons Licenses*. CENT-UJI. http://cent.uji.es/pub/sites/cent/files/Guia-Creative-Commons-by-Alejandro-Vera-Palencia-by-nc-sa-es-3.0.pdf

Received April 01, 2026 / Approved June 13, 2026 Pages: 34–55
eISSN: 2600-5743