BRIDGE WATCH REPORT

Digital Transition in Latin America

Jean Monnet Network Policy Debate Bridge Watch Project:
Values and Democracy in the EU and Latin America

2025

Mario Torres Jarrín
Naiara Posenato
Aline Beltrame de Moura
Nuno Cunha Rodrigues

BRIDGE WATCH
JEAN MONNET POLICY DEBATE

LACES
Latin American Center
of European Studies

Co-funded by
the European Union

BRIDGE WATCH REPORT

Digital Transition in Latin America

Jean Monnet Network Policy Debate Bridge Watch Project:
Values and Democracy in the EU and Latin America

Naiara Posenato
Mario Torres Jarrín
Aline Beltrame de Moura
Nuno Cunha Rodrigues

2025

BRIDGE WATCH
JEAN MONNET POLICY DEBATE

LACES
Latin American Center
of European Studies

Co-funded by
the European Union

This work is published under the responsibility of the Jean Monnet Network Policy Debate–Bridge Watch Project–Values and Democracy in the EU and Latin America (101126807). The opinions expressed and the arguments used in this work do not necessarily reflect the official views of the universities that are members of the Bridge Watch Project.

The support of the European Commission for the production of this publication does not constitute an endorsement of the content, which reflects solely the opinions of the authors, and the Commission cannot be held responsible for any use that may be made of the information contained therein.

Data Sheet:

Title: Bridge Watch Report - Digital Transition in Latin America

Subtitle: Jean Monnet Network Policy Debate Bridge Watch Project: Values and Democracy in the EU and Latin America

Edit by: Mario Torres Jarrín, Naiara Posenato, Aline Beltrame de Moura, Nuno Cunha Rodrigues

Publisher: AAFDL Editora, Lisboa

ISBN: 978-989-9312-30-2

Year: 2025

Follow BRIDGE Watch's publications and activities at:

https://eurolatinstudies.com/en/

https://www.facebook.com/eurolatinstudies/

https://www.instagram.com/eurolatinstudies/

https://br.linkedin.com/company/euro-latin-studies

Table of Contents

Acknowledgements

Local Coordinators

Martina Lourdes Rojo - Argentina
Juan David Alarcón Morales – Bolivia
Aline Beltrame de Moura - Brasil
Fabíola Wüst Zibetti – Chile
Walter Orlando Arévalo Ramírez – Colombia
Danilo Vicente Garcia Caceres – Ecuador
Manuel Becerra Ramirez – México
Roberto Ruiz Díaz Labrano - Paraguay
Ena Carnero Arroyo - Perú
Pablo Guerra Aragone - Uruguay

Ad Hoc Consultants

Giovanni Ziccardi

Permanent Consultant

Cátia Miriam

Local Consultants

Andres Lagarde Munin - Argentina
Axel Lodovico Molina - Argentina
Santiago Deluca - Argentina
Julio Ielpi Boyero - Argentina
Cesar Carlos Bohrt Urquizo - Bolívia
Cristina Mendes Bertoncini Corrêa - Brasil
Debora Bonat - Brasil
Ignacio Sánchez - Chile
Danielle Zaror - Chile
Daniela Olivares - Chile
Andrea Lucas - Chile
Alejandro Beltrán Torrado - Colombia
Desiré Nazenin Lopez Mondavi - Ecuador
Michelle Ochoa - Ecuador
Ana Georgina Alba Betancourt - México
Patrícia Stanley Zarza - Paraguay
Manuel Ángel Cipriano Pirgo - Perú
Graciela Romero Silvera - Uruguay

Introduction

The BRIDGE Watch Report "Digital Transition in Latin America" constitutes one of the main outcomes of the Jean Monnet Network Policy Debate Project – BRIDGE Watch – *Values and Democracy in the EU and Latin America* (101126807), co-funded by the Erasmus+ Programme of the European Commission and supported by the Latin American Center of European Studies (LACES). This project brings together a network of 14 universities from Europe and Latin America: Universidade de Lisboa (Portugal), Universidade Federal de Santa Catarina (Brazil), Universidad del Salvador (Argentina), Universidad Nacional Autónoma de Mexico, Universidad del Rosario (Colombia), Universidad de Sevilla (Spain), Università degli Studi di Milano (Italy), Universidad Mayor de San Andrés (Bolivia), Universidad Central del Ecuador, Universidad Nacional de Trujillo (Peru), Universidad de Chile, Universidad Nacional de Asunción (Paraguay), Universidad de la República (Uruguay), and Universidad Pontificia de Salamanca (Spain).

The BRIDGE Watch project aims to strengthen mutual understanding between the European Union and Latin America by promoting comparative study of their values, institutions, and public policies in strategic areas for sustainable development and democratic governance. Within this framework, the present report examines the current landscape and the key challenges of digital transformation in ten Latin American countries—Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Mexico, Paraguay, Peru, and Uruguay—identifying common trends, structural divides, and opportunities for bi-regional cooperation.

The analysis is structured around four thematic pillars:

I. Digital Transformation and Equitable Access to Technology

1. National policies for digital transition.
2. Digital Access and connectivity of the population.
3. Measures for digital sovereignty.
4. Inequalities in access to technology between urban and rural areas.
5. Public policies to reduce the digital divide.
6. Recognition of the right to access the Internet as a fundamental right.

II. Green Technology and the Digital Climate Transition

7. Regulations on technological sustainability.
8. Adoption of Green Tech practices.
9. Compliance with European environmental standards.

III. Ethics, Transparency, and Algorithmic Justice

10. Computer ethics in the technological and artificial intelligence fields.
11. Artificial intelligence in judicial and oversight systems.
12. International cooperation.
13. Corporate adaptation to the EU AI Act.
14. Ethical codes of conduct for AI-developing companies.
15. Integration of ethics into teaching and research on AI.
16. Regulations on algorithmic transparency.
17. Prevention of algorithmic discrimination and independent oversight.
18. Protection of private life and in the digital environment.

IV. Cybersecurity, Global Digital Trust, and International Cooperation

19. Use of AI against terrorism and criminality.
20. Digital surveillance and international human rights standards.

The methodology adopted draws on the comparative assessment approach developed by the European Commission in its Rule of Law Mechanism, adapting it to the particularities of the Latin American context. The study is based on national questionnaires completed by the project's local partners and reviewed through a double-check system that incorporated contributions from regional experts and specialized consultants. The information gathered reflects the normative, institutional, and case law developments in the countries analyzed up to July 2025.

The responses to the questionnaires were based on official information provided by national authorities, complemented by contributions from national and international non-governmental organizations, research groups, and specialized think tanks. To ensure robust analysis, rigorous quality criteria were applied, including factual accuracy, comprehensiveness, reliability, relevance, and the internal consistency of the collected data.

The digital transition in Latin America and the Caribbean (LAC) is advancing steadily, driven by the rise of emerging and disruptive technologies that are transforming the economy, society, and governance. This process has enabled the creation of innovation ecosystems and strengthened digital infrastructure, but it has also revealed deep inequalities in access, connectivity, and technological capabilities. In this context, the European Union (EU) and LAC countries recognize the urgent need to establish more robust bi-regional cooperation to promote an inclusive, sustainable, and people-centered digital transformation. The EU–LAC Digital Alliance, launched in 2023 under the Global Gateway strategy, serves as a key instrument for coordinating joint efforts across connectivity, data governance, cybersecurity, and innovation. Thus, the digital transition has become a strategic pillar for advancing sustainable development and social cohesion in both regions. In a global landscape marked by the growing power of Big Tech companies and the increasing challenges to digital sovereignty, this alliance represents a strategic opportunity to build ethical global technological governance grounded in human rights, transparency, and sustainability, thereby consolidating a fairer, more inclusive digital model.

Taken together, the BRIDGE Watch report, "The Digital Transition in Latin America," constitutes a methodologically solid and comparatively coherent tool that offers a comprehensive overview of the current state, progress, and challenges of digital transformation in the region. The report examines its interaction with bi-regional integration processes, national public policies, and the global dynamics of technological governance to identify best practices, foster dialogue between the European Union and Latin American countries, and formulate strategic recommendations to consolidate a model of digital cooperation that is inclusive, sustainable, and people-centered.

Nonetheless, its findings provide an analytical framework that will enable the European Commission to assess the promotion and protection of human rights in the region's key countries, guiding its political, commercial, and diplomatic relations with Latin America and fostering the dissemination of the European Union's fundamental values. This process of cooperation and mutual learning seeks to strengthen democratic governance, the protection of human rights, and the consolidation of legal and institutional frameworks that are more transparent, effective, and consistent with a model of technological governance grounded in human rights principles, democracy, the rule of law, equity, and sustainability.

Lisbon, December 2025.

Mario Torres Jarrín, European Institute of International Studies, Sweeden
Naiara Posenato, Università degli Studi di Milano, Italy
Aline Beltrame de Moura, Universidade Federal de Santa Catarina, Brazil
Nuno Cunha Rodrigues, Universidade de Lisboa, Portugal

Pilar I

Digital Transformation and Equitable Access to Technology

Section 1. National policies for digital transition

Has your government adopted specific regulations and/or political strategies to ensure the digital transition in your country? (For example: policies to support digital literacy, etc.)

Summary

All the countries surveyed have adopted specific regulations, strategies, and policies to facilitate the digital transition, covering digital literacy, connectivity, digital government, and the knowledge economy.

In Latin America, countries have advanced through diverse national strategies aimed at digital transformation, technological literacy, and the modernization of the State, though at varying paces and with varying approaches depending on their institutional contexts.

In Argentina, key initiatives include the *Digital Agenda 2030*; the educational programs *Conectar Igualdad* (Connect Equality) and *Prender Conectados* (Switch on Connected Learning); the *Juana Manso* digital literacy platform; the State Modernization Plan; the Knowledge Economy Promotion Law; *Argentina Programa 4.0*; and the National Cybersecurity Strategy 2023–2027. Complementarily, Bolivia has promoted the *Bolivia Digital Agenda 2021–2025*, the Telecommunications Law of 2020, the National Digital Literacy Plan, and the launch of the *Túpac Katari* satellite, intended to expand connectivity in rural areas.

In Brazil, digital government policies focus on administrative efficiency and public innovation, notably the *Federal Digital Government Strategy 2024–2027*, as well as laws and decrees that encourage de-bureaucratization, digital education, and sectoral programs such as *Justiça 4.0*. Chile, for its part, has developed long-term strategies since 2004, combining educational programs, digital transformation laws, and the National Artificial Intelligence Policy, culminating in the *Chile Digital 2025* initiative.

In Colombia, the combination of public policies such as *Vive Digital* (Live Digital), administrative simplification laws, and the *National Digital Strategy 2023–2026* reflects a comprehensive approach linking connectivity, education, and institutional modernization. Ecuador has given high priority to literacy and digital transformation through *Plan Ecuador Digital* and the Regulation of the Digital and Audiovisual Transformation Law, focusing on inclusion and the strengthening of technological capacities.

In Mexico, the *National Digital Strategy 2021–2024* is complemented by literacy and connectivity programs, as well as digital government laws aimed at building a more transparent and innovative public administration. Paraguay structures its policies around four strategic pillars: digital government, digital economy, connectivity, and institutional strengthening, while Peru combines laws, decrees, and programs aimed at digital trust and cybersecurity.

Finally, Uruguay maintains one of the most consolidated agendas in the region with its *Digital Agenda 2019–2028*, centered on digital citizenship, technological resilience, and the development of regulatory frameworks on artificial intelligence and cybersecurity.

All these governmental initiatives reflect a regional effort to ensure digital inclusion, improve State efficiency, promote technological education, and strengthen the knowledge economy, positioning the region to face the challenges and opportunities of global digital transformation.

Recommendations

1. Expand and guarantee digital access: ensure nationwide Internet coverage and the availability of technologies, including in rural and vulnerable areas, to reduce connectivity gaps.
2. Strengthen digital literacy and technological education: implement educational programs and continuous training platforms, and promote the inclusion of disadvantaged groups and foster gender equality in digital skills.
3. Coordinate national policies and strategies: articulate digital government plans, knowledge-economy initiatives, and technological transformation strategies to achieve an integrated and coherent approach that maximizes impact across the population.
4. Promote technological innovation and sustainability: advance laws and regulations that encourage innovation, administrative efficiency, and the adoption of sustainable technologies, including international standards in Green Tech and digital transformation.

Section 2. Digital access and connectivity of the population

What are the main barriers (including economic, educational, and cultural) to the widespread adoption of new information technologies, high-speed Internet connections, and artificial intelligence in your country? What percentage of the population in your country, according to the most recent statistical data, has access to broadband connectivity?

Summary

Across the countries studied, both common and country-specific barriers can be identified that hinder the widespread adoption of new technologies, high-speed connectivity, and artificial intelligence. Unequal infrastructure remains one of the main obstacles, as many rural and remote areas lack reliable fixed or mobile high-speed networks. In Argentina, some provinces reach only 32% broadband coverage, while in Bolivia, Peru, and Ecuador, mountainous or jungle terrain significantly restricts the expansion of fiber-optic networks and other services.

The urban–rural and regional divide further exacerbates these challenges. In Brazil, although more than 90% of households have Internet access, only 81% of rural areas have connectivity, compared to 94% in urban areas. This disparity is also present in other countries, where access and service quality depend heavily on geographic location and population density, thereby limiting equitable development of digital capacities.

Economic and educational factors represent another significant barrier to be considered. The cost of devices, subscriptions, and maintenance restricts adoption among low-income households, while the lack of digital literacy, technological skills, and familiarity with artificial intelligence environments prevents connectivity from translating into effective, productive use of digital tools.

In terms of broadband coverage, percentages vary across countries and data sources, including private, public, and international surveys. Argentina, Brazil, Mexico, and Chile are among the countries whose populations show the highest broadband coverage and access rates.

Recommendations

1. Equitable expansion of connectivity infrastructure: invest in high-speed fixed and mobile networks in rural, remote, and geographically complex areas, ensuring nationwide coverage and reducing the urban–rural divide.
2. Strengthening digital literacy and training: implement technological education programs that build digital skills and familiarity with artificial intelligence, prioritizing vulnerable communities and regions with lower access.
3. Affordable and accessible technologies: establish support mechanisms, financing schemes, or differentiated tariffs for devices, data plans, and maintenance, ensuring that low-income households can connect and make effective use of technology.
4. Regional monitoring and coordination of digital policies: create systems to track connectivity and the effective use of technologies, promoting coordination between public and private actors to design policies tailored to local needs and reduce digital inequalities.

Section 3. Measures for digital sovereignty

Has your government adopted regulatory or policy measures to ensure "national digital sovereignty"? (For example: reinforced protection for local companies and start-ups, the creation of an internal telematic network, the elimination of dependency on Chinese and American technology companies, etc.)

Summary

Across Latin America, the adoption of measures to ensure national digital sovereignty reveals a heterogeneous landscape among the countries surveyed. Argentina, Bolivia, Brazil, Mexico, Peru, and Uruguay have implemented concrete policies, regulations, and strategies to protect national companies and start-ups and to reduce technological dependency on foreign providers, prioritizing areas such as State and private-sector digital security and autonomy.

In contrast, Chile, Colombia, and Paraguay have not yet established specific digital sovereignty measures, according to available information. The absence of formal policies in these countries underscores the need to develop strategic planning and regulations to protect national technological interests and ensure autonomous, secure development.

Ecuador, for its part, is currently pursuing legislative initiatives to create a regulatory framework to promote digital sovereignty, although large-scale implementation measures have not yet been adopted.

Overall, the data provided show that, although several countries have made significant progress in protecting digital autonomy, others need to accelerate the development of strategic policies to ensure that digital transformation advances in a sovereign, secure, and sustainable manner, reducing external technological dependency—which remains a vulnerability for all countries.

Recommendations

1. Develop comprehensive regulatory frameworks for digital sovereignty: promote laws and public policies that define principles, objectives, and mechanisms to guarantee technological autonomy, data protection, and critical digital infrastructure, adapted to each country's context.

2. Foster innovation and strengthen the national technological ecosystem: support national companies, universities, and start-ups through tax incentives, public financing, and innovation programs, in order to reduce dependence on foreign providers and reinforce national productive capacity in the digital sphere.

3. Promote sovereign and secure digital infrastructure: invest in national data networks, data-storage centers (data centers), and state-owned or mixed cloud services, ensuring information security and the operational continuity of the State.

4. Strengthen regional cooperation on digital sovereignty: promote alliances among Latin American countries to share best practices, develop common cybersecurity standards, and negotiate jointly with major international technological actors.

5. Incorporate education and training on technological sovereignty: design educational and professional training programs that promote knowledge of digital sovereignty, cybersecurity, and technological innovation, ensuring the development of national capacities and a critical, participatory digital citizenship.

Section 4. Inequalities in access to technologies between urban and rural areas

According to the most recent data, what are the primary differences in access to technology between urban and rural areas in your country?

Summary

Across the countries analyzed, significant inequalities persist between urban and rural areas in access to digital technologies, connectivity, and broadband Internet services. On average, between 66% and 94% of the urban population have stable access to the Internet and technological devices, while in rural areas these figures drop sharply, reaching only 30% to 40%. These divides reflect structural inequalities linked to limited infrastructure, the high costs of implementation and maintenance in low-density areas, and the geographical challenges of mountainous, jungle, or hard-to-reach regions. In addition, lower digital literacy and lower income levels in rural areas further restrict the effective use of available technologies. This limits educational, employment, and civic-participation opportunities, perpetuating cycles of inequality.

Closing this divide requires integrated policies that combine investment in infrastructure, digital inclusion programs, support for device acquisition, and digital skills training, ensuring an equitable technological transformation across urban and rural territories.

Recommendations

1. Expand rural digital infrastructure: promote public and private investments to deploy connectivity networks in rural and remote areas, prioritizing sustainable technologies—such as wireless or satellite networks—that reduce installation and maintenance costs in hard-to-reach territories.
2. Implement digital inclusion and literacy programs: develop national policies that promote training in basic and advanced digital skills, targeting rural communities, women, and the young population to ensure the effective and productive use of available technologies.
3. Promote economic incentives and technological support: establish financial assistance programs for device acquisition and subscribing to Internet connections and maintenance services, especially for low-income households, rural cooperatives, and small businesses.

Section 5. Public policies to reduce the digital divide

What public policies (laws, regulations, funding mechanisms, and technological initiatives) have been implemented to reduce the digital divide in your country and in specific regions of your country, and in what way?

Summary

Across all the countries surveyed, various public policies have been implemented to reduce the digital divide, although results remain uneven. These initiatives include regulatory frameworks, connectivity programs, subsidies, and technological projects aimed at improving Internet access, strengthening digital literacy, and promoting technological inclusion.

Among the most notable measures are national connectivity plans—such as *Conectar Igualdad* (Equal Connectivity Program) in Argentina, Bolivia Digital, Brazil's Federal Digital Government Strategy, Chile Digital 2025, and *Vive Digital* (Live Digital) in Colombia—which promote the expansion of broadband networks and the installation of free access points in educational and community institutions. Likewise, several countries have allocated public funds and established partnerships with the private sector to expand fiber-optic coverage and 4G and 5G mobile networks, particularly in rural areas.

However, despite these efforts, significant disparities between urban and rural areas persist due to limited infrastructure, geographic dispersion, high service costs, and the lack of financial sustainability of long-term projects. Governments continue to face the challenge of combining technological infrastructure, affordable pricing policies, and digital skills training programs to achieve effective, equitable technological inclusion across the region.

Recommendations

1. Develop regional strategies for digital inclusion: promote cooperation among Latin American countries to share best practices, coordinate investments in cross-border digital infrastructure, and establish common standards that ensure equitable and sustainable connectivity.
2. Strengthen infrastructure in rural and hard-to-reach areas: increase public and private investment in expanding fiber-optic networks, satellite systems, and wireless technologies, prioritizing rural, border, and isolated communities in order to guarantee high-quality coverage throughout the territory.
3. Ensure financial sustainability and affordable pricing: create stable financing mechanisms, targeted subsidies, and regulatory frameworks that foster competition, reduce service costs, and ensure universal access to the Internet as an essential public good.
4. Promote public–private partnerships: establish strategic agreements among governments, technology companies, universities, and local organizations to support innovation projects,

infrastructure maintenance, and the development of inclusive and sustainable digital services.

Section 6. Recognition of the right of access to the Internet as a fundamental right

Does your government or your Constitution recognize the "right of access to the Internet" as a fundamental right? If so, under what terms, principles, or legal provisions?

Summary

Most of the countries surveyed recognize access to the Internet as an essential condition for the exercise of fundamental rights, even though it is not expressly included in their constitutions as an autonomous right. In general, Internet access is linked to the rights to information, communication, education, freedom of expression, and citizen participation, underscoring its role in social inclusion and democratic development.

Recognition is primarily implemented through laws and public policies on telecommunications or access to information. In Argentina and Mexico, Internet access is defined as an essential public service or a service of general interest, obliging the State to ensure its availability and affordability. In Brazil, principles such as net neutrality, privacy, and universal access are established, while in Uruguay, access to the Internet is classified as a universal public service. Colombia, Peru, and Ecuador incorporate digital access into their inclusion and technological development strategies, linking it to the rights to education and civic engagement. Chile, by contrast, is one of the few countries that has amended its Constitution to explicitly recognize the right of access to the Internet as a guiding principle for public policy.

Although most countries view it primarily as a derivative component of the right to information rather than an independent fundamental right, there is regional consensus on the principles of universality, equity, affordability, and non-discrimination.

Recommendations

1. Constitutionally recognize access to the Internet as a fundamental right: advance toward the explicit incorporation of Internet access into national constitutions, ensuring its recognition as an autonomous right linked to the full exercise of other fundamental rights such as education, information, and citizen participation.
2. Strengthen regulatory and legal frameworks: update and harmonize telecommunications and digital services laws to consolidate Internet access as an essential or universal public service, establishing clear obligations for the State and private operators regarding coverage, quality, and affordability.

3. Promote equity-driven policies to reduce the digital divide: develop strategies that guarantee equitable Internet access in rural and hard-to-reach areas, prioritizing investment in infrastructure, financial support measures, and digital inclusion programs.

4. Guarantee the principles of neutrality, privacy, and non-discrimination: the policies should safeguard net neutrality, protect users' personal data, and ensure a digital environment free from censorship and discrimination, thereby strengthening public trust in technology use.

5. Promote regional cooperation and public-sector innovation: foster Latin American cooperation frameworks to share best practices, enhance technological interoperability, and develop sovereign digital solutions that reinforce regional technological autonomy.

Pillar II

Green Technology and Digital Climate Transition

Section 7. Regulations on technological sustainability

What regulations on technological sustainability are in force in your country, and what aspects do they regulate?

Summary

There are several regulations and public policies aimed at promoting technological sustainability, although their scope and degree of implementation vary across countries. Broadly speaking, these regulatory frameworks focus on three main areas: the environmental management of electronic waste, energy efficiency in the use of digital technologies, and the promotion of a circular economy within the technological sector.

Brazil and Chile have the most robust regulatory frameworks, primarily in the area of waste from electrical and electronic equipment, imposing obligations on producers and distributors to collect, recycle, and dispose of devices in an environmentally responsible manner. In Mexico and Argentina, technological sustainability policies are integrated into broader digital transformation and green transition strategies, encouraging energy efficiency and green innovation in the technology industry. Colombia, Ecuador, and Peru have adopted regulations to reduce the digital carbon footprint and promote the use of clean energy in data centers and telecommunications networks. Paraguay and Uruguay have advanced policies that encourage sustainable digitalization of the State and the responsible use of information technologies. Although technological sustainability is not yet fully consolidated in national legislation, the region is moving toward a more comprehensive approach that integrates digital innovation, environmental responsibility, and sustainable development.

Recommendations

1. Consolidate regional regulatory frameworks on technological sustainability: strengthen and harmonize national regulations in order to create a common Latin American framework on technological sustainability. This includes the comprehensive management of electronic waste, energy efficiency, and the transition toward a circular economy within the technological sector.

2. Promote economic incentives and green innovation: introduce fiscal and financial incentives for companies and start-ups that develop clean technologies, reduce their environmental footprint, or incorporate sustainable practices into their digital processes. These measures also involve encouraging research into renewable energy solutions suitable for data centers, telecommunications networks, and digital public services.

3. Integrate technological sustainability into digital transformation policies: embed environmental sustainability criteria into national digitalization and e-government strategies, prioritizing efficient resource use, reduced energy consumption, and training in sustainable digital practices.

Section 8. Adoption of Green Tech practices

What technological sectors in your country have adopted Green Tech practices, and through which modalities, investments, and associated costs?

Summary

The adoption of Green Tech practices has expanded significantly across the region, driven by energy-transition policies, corporate sustainability strategies, and international commitments to climate action. Mexico stands out for its investments in solar energy; Ecuador and Peru for rural renewable initiatives; Colombia for electric mobility; Brazil and Argentina for biofuels and wind power; Bolivia for solar energy; Chile for green hydrogen; Paraguay for hydropower; and Uruguay for achieving a fully renewable energy matrix. Nonetheless, levels of investment and implementation still vary according to the economic and technological capacity of each country surveyed.

The energy sector leads the green transition. Brazil, Chile, and Mexico are investing heavily in renewable energy—particularly solar, wind, and green hydrogen—to diversify their energy mix and reduce emissions. Argentina, Uruguay, and Colombia promote energy-efficiency and distributed-generation projects through public–private partnerships.

In agriculture and manufacturing, countries such as Peru and Ecuador have incorporated sustainable digital technologies to optimize water use, reduce waste, and foster circular-economy practices. The automotive sectors in Mexico, Brazil, and Argentina are advancing electric mobility through tax incentives, charging infrastructure, and local production of electric vehicles.

Similarly, the construction sector is advancing with sustainable building standards and energy-efficiency regulations, while telecommunications and banking increasingly implement carbon-footprint reduction strategies and green finance instruments. In the transport sector, several cities in Chile, Colombia, and Uruguay are integrating electric bus fleets and developing sustainable public-transport systems.

Although initial investments in Green Tech entail high upfront costs—particularly in energy infrastructure and transportation—governments recognize their long-term economic and environmental returns. The Latin American region is steadily moving toward a cleaner and more resilient economy, integrating technological sustainability as a core pillar of competitiveness and development.

Recommendations

1. Establish green financing frameworks and fiscal incentives: adopt long-term sustainable policies that encourage public and private investment in clean technologies. This includes creating national green-innovation funds, expanding fiscal incentives for renewable energy projects, electric mobility, and energy efficiency, as well as issuing green bonds and climate-finance instruments. It also involves promoting the financial sector's engagement

in channeling capital toward initiatives that support sustainable energy and the digital transition.

2. Promote sustainable technological integration in strategic sectors: foster sustainable digitalization, efficient management of natural resources, and circular-economy practices, ensuring that green technologies help drive employment, competitiveness, and emissions reduction.
3. Strengthen regional cooperation and technology transfer: developing a regional green-innovation framework would help reduce costs, attract foreign investment, and enable coordinated progress toward a low-carbon, resilient, and environmentally responsible economy.

Section 9. Compliance with European environmental standards

Do the technology companies in your country comply, to the best of your knowledge, with European environmental standards?

Summary

Yes, in general, companies comply with European environmental standards, especially those with an international presence or integrated into global supply chains. These firms have adopted environmental management policies, energy-efficiency measures, electronic-waste management systems, and emissions-reduction practices aligned with regulations such as the European Waste Electrical and Electronic Equipment Directive and international standards such as ISO.

Compliance with these standards responds not only to international legal requirements but also to the demands of consumers and business partners who prioritize sustainability. Sectors such as telecommunications, hardware manufacturing, renewable energy, and data centers have implemented recycling processes, energy-efficient practices, and the use of clean energy.

Although challenges persist among small and medium-sized enterprises (SMEs) and smaller local companies, the overall trend is positive, with a growing commitment to circular-economy practices, carbon-footprint reduction, and sustainable technological innovation, progressively aligning with European environmental criteria.

Recommendations

1. Encourage SMEs and companies to adopt sustainable practices: provide financial support, green credits, and technical assistance to enable smaller-scale companies to meet European environmental standards, including energy efficiency, electronic waste management, and international certifications.

2. Strengthen environmental oversight and monitoring: develop public supervision mechanisms to verify compliance with environmental regulations across all technological sectors, ensuring transparency and continuity in sustainable practices.
3. Promote the transition toward sustainable production and green and digital innovation: advance green and digital policies that stimulate recycling, the reuse of electronic components, and the adoption of clean and smart technologies throughout the production chain, fostering resource efficiency, sustainable innovation, and a comprehensive reduction of the carbon footprint.
4. Facilitate international cooperation and technological transfer: establish partnerships with European companies, agencies, and programs to update standards, share best practices, access clean technologies, and strengthen staff training in environmental management and energy efficiency.

Pillar III

Ethics, Transparency, and Algorithmic Justice

Section 10. Computer ethics in the technological and artificial intelligence fields

What ethical principles govern the development and use of AI in your country?

Summary

In most of the countries surveyed, the development and use of artificial intelligence is not yet specifically regulated. Therefore, no national laws exist that directly address all of its ethical and legal dimensions. However, governments and national bodies rely on ethical principles promoted by international organizations—particularly those issued by the OECD and UNESCO—which highlight values such as transparency, fairness, responsibility, inclusion, and respect for human rights.

On the other hand, existing legal frameworks on data protection, access to public information, and information security serve as guidelines for the responsible implementation of AI. These principles seek to ensure that AI systems respect privacy, promote fairness, avoid discriminatory algorithmic bias, and foster accountability in their design and use. It is also important to note that, despite advances in digitalization and green technologies, regulatory divides persist in key areas such as personal data protection, artificial intelligence, cybersecurity, and electronic-waste management. The adoption of international and national ethical standards provides a solid foundation for moving toward more comprehensive and coherent regulatory frameworks in the future, ensuring technological development that is safe, responsible, and aligned with human rights.

Recommendations

1. Develop national regulatory frameworks specific to artificial intelligence: promote the adoption of national laws and regulations that address all ethical, legal, and social aspects of artificial intelligence, aligned with international principles. The EU AI Act may serve as a reference for incorporating risk classification criteria, establishing transparency obligations, and implementing AI impact assessment systems.
2. Training and international cooperation on the ethical governance of artificial intelligence: implement training programs for public officials, developers, companies, and civil society, focused on the ethical governance of artificial intelligence.
3. Strengthen regional and international cooperation on artificial intelligence: promote alliances and networks among countries to share best practices and establish oversight mechanisms that ensure the effective implementation of ethical and regulatory principles.

Section 11. Artificial intelligence in the judicial and oversight systems

How is artificial intelligence used within the courts and the bodies responsible for oversight and accountability? What initiatives and regulatory frameworks currently exist regarding datasets?

Summary

In the countries surveyed, the use of artificial intelligence in courts and oversight bodies is emerging as a tool to streamline judicial processes, enhance transparency, and improve decision-making efficiency. However, implementation remains incipient and is largely limited to pilot projects or support systems rather than autonomous decision-making mechanisms.

In Brazil, the *Victor* project uses AI algorithms to analyze large volumes of judicial files, identify litigation patterns, and optimize case allocation within the judiciary. In Argentina, the *Prometea* project assists judges in drafting rulings and suggesting relevant precedents, improving document management and reducing processing times. Mexico has developed *Julia*, a judicial support system that classifies case files and provides recommendations on administrative procedures, thereby improving efficiency in courts and oversight bodies. In Peru, the *Curia* project is used to manage large amounts of procedural information, detect inconsistencies, and support internal audits. Other Latin American countries, such as Colombia, Chile, and Uruguay, have also begun exploring the use of artificial intelligence for fiscal audits, oversight of public procurement, and analysis of corruption reports to detect irregularities and reduce fraud risks.

Regarding datasets, most countries lack AI-specific regulations, but principles on personal data protection, anonymization, and information security are applied in accordance with national laws and internationally inspired standards. Efforts focus on ensuring data quality, traceability, and reliability, while promoting transparency and accountability in the use of algorithms.

Recommendations

1. Establish regulatory frameworks for judicial and administrative artificial intelligence: adopt specific laws and regulations that define the limits and responsibilities in the use of AI systems in courts and oversight bodies, ensuring that algorithms comply with principles of transparency, fairness, ethics, and human and fundamental rights.

2. Ensure the quality and responsible management of datasets: implement policies that guarantee the traceability, anonymization, integrity, and security of the data used by AI systems, with clear standards for the collection, storage, and updating of procedural and administrative information.

3. Promote training in ethical and technological governance: develop programs tailored for judges, prosecutors, auditors, and administrative staff on the responsible use of AI, ethical

governance of algorithms, and oversight of automated systems, thereby strengthening institutional trust and efficiency.

4. Support pilot projects and regional cooperation: promote the implementation of AI pilot projects such as *Victor*, *Prometea*, *Julia*, and *Curia*, assessing their impacts and lessons learned; and foster the exchange of experiences and best practices among Latin American countries to standardize methodologies and reinforce regional capacities in artificial intelligence applied to justice and accountability bodies.

Section 12. International cooperation

Are there cooperation agreements between the EU and your country on AI regulation? If so, what areas do they cover?

Summary

In the countries surveyed, there are currently no formal cooperation agreements with the European Union specifically focused on the regulation of artificial intelligence. However, existing data-protection frameworks provide a solid foundation for strengthening bi-regional cooperation and establishing shared principles and standards that could guide future AI regulations ethically and securely. Although many governments express interest in aligning their policies with international standards—such as the ethical principles of the OECD and UNESCO—no bilateral, bi-regional, or multilateral agreements have yet been established that directly regulate the implementation of artificial intelligence in line with the European framework, including the EU AI Act.

Nevertheless, there is an indirect form of alignment through the adoption of international best practices and recommendations promoted by the European Union in global forums on the ethical governance of artificial intelligence, transparency, data protection, and algorithmic security. Some national institutions have initiated comparative studies and technical working groups to examine how the provisions of the EU AI Act could be incorporated into future regulatory frameworks, although these initiatives remain exploratory.

Finally, although there is clear interest in regulatory convergence with the European Union, no formal cooperation agreements on artificial intelligence regulation are currently in place. The region continues to rely on international standards and domestic regulations to guide ethics, transparency, and data protection in AI systems. At the same time, the formalization of strategic partnerships with the European Union remains pending.

Recommendations

1. Initiate bilateral and bi-regional dialogues with the European Union: establish working groups and cooperation frameworks to explore the incorporation of EU AI Act standards,

fostering regulatory convergence and the exchange of best practices in ethical governance, transparency, and data protection.

2. Strengthen institutional capacities and develop comparative studies: build technical and legal capacities to interpret and adapt European provisions to local contexts. This includes comparative studies, staff training on international regulations, and the creation of protocols for the responsible implementation of artificial intelligence.

3. Promote regional cooperation frameworks: advance regional agreements that incorporate European ethical and regulatory standards into local AI policies. Regional cooperation would help harmonize criteria, facilitate technological transfer, improve system interoperability, and advance a more robust, coordinated regulatory approach across the region.

Section 13. Corporate adaptation to the EU AI Act

To what extent do national companies operating in Europe need to comply with the EU's AI regulations?

Summary

In the countries surveyed, all companies that operate or commercialize products and services in the European Union are required to comply with the EU's regulatory framework on artificial intelligence—primarily the EU AI Act—as well as with the data-protection and transparency standards established by the European Union. This adaptation requires companies to implement risk-management systems, assess and mitigate potential algorithmic biases, ensure data traceability, and guarantee the explainability of AI models for users and regulatory authorities.

Companies must also comply with specific documentation, certification, and audit requirements depending on the classification of their AI systems, with particular emphasis on those categorized as high-risk, such as systems used in health, justice, education, or financial services. This entails investments in technology, staff training, and adjustments to internal processes related to both AI development and deployment. Moreover, alignment with EU regulations has encouraged the adoption of ethical and sustainability best practices in AI projects, strengthening trust among clients, business partners, and investors. Ultimately, the obligation to comply with the European Union's rules drives companies to raise their standards of governance, transparency, and accountability in the use of artificial intelligence.

Recommendations

1. Promote specialized training in AI governance: advance training programs for staff in technology companies on risk management, data traceability, bias mitigation, and algorithmic explainability, ensuring effective compliance with the EU AI Act.

2. Stimulate investment in responsible technological infrastructure: promote financing lines and fiscal incentives that facilitate the implementation of artificial intelligence systems

aligned with European standards, including internal audits, certifications, and improvements in data security.

3. Establish national guidance for regulatory alignment: develop reference frameworks and protocols to assist companies in meeting the documentation, certification, and risk-management obligations required by the European Union, particularly for high-risk systems.
4. Foster the adoption of ethical and sustainable best practices by encouraging the integration of ethical principles, sustainability, and transparency into AI projects, thereby strengthening the trust of users, clients, investors, and international regulatory bodies.
5. Promote business cooperation and mutual learning: stimulate spaces for sharing experiences, conduct joint audits, and foster collaboration between national companies and Big Tech firms to improve the implementation of European regulations and strengthen regional competitiveness in artificial intelligence.

Section 14. Ethical codes of conduct for AI-developing companies

Are there ethical codes of conduct for AI-developing companies in your country? If so, what are the main issues they address?

Summary

At present, there is no single, formal, and mandatory ethical code of conduct specifically for companies developing artificial intelligence solutions. However, the ethical framework for these activities is increasingly and more robustly shaped through governmental guidelines, evolving legislation, and international standards. These efforts aim to establish principles that guide the responsible and safe development, implementation, and oversight of artificial intelligence systems.

Much of the ethical guidance is based on personal data protection laws, access-to-information regulations, and information security standards, as well as on international agreements and recommendations issued by organizations such as the OECD, UNESCO, and the International Telecommunication Union. The core principles underscored include transparency in algorithmic functioning, fairness and non-discrimination in outcomes, companies' ethical responsibility for automated decisions, the traceability of AI processes, and the privacy of the data used. Emphasis is also placed on accountability and the explainability of systems, enabling users and authorities to understand, audit, and supervise their decisions.

Although no single mandatory code exists, many companies have adopted internal AI-ethics policies aligned with these guidelines, fostering trust among clients, business partners, and investors. The goal is for corporate ethical responsibility to become a central pillar in the development of artificial intelligence solutions, complementing national legislation and existing international standards.

Recommendations

1. Develop a national ethical code of conduct harmonized with regional standards: establish a legal framework that sets clear ethical principles for all companies developing artificial intelligence solutions, incorporating transparency, fairness, corporate accountability, data protection, and algorithmic traceability. This code should be aligned with regional standards and international best practices, facilitating cooperation and interoperability with European frameworks.

2. Establish national mechanisms for ethical monitoring and auditing of AI, with regional coordination: implement supervision systems, certification procedures, and periodic national-level audits to assess compliance with the ethical code and applicable legislation. At the same time, it would be advisable to establish regional coordination to share results, audit protocols, and common standards, reinforcing transparency and accountability in artificial intelligence systems.

3. Promote national, regional, and interregional EU–LAC forums on AI ethics: create spaces for dialogue among governments, companies, and international organizations at the national and regional levels, as well as with the European Union, to facilitate the exchange of information, experiences, best practices, and ethical standards. These interregional forums will strengthen EU–LAC cooperation by promoting coherent global ethical governance frameworks consistent with international standards.

Section 15. Integration of ethics into teaching and research on AI

Do universities and research centers in your country integrate ethical principles into the teaching of AI? If so, in what ways and for what purpose?

Summary

The integration of ethical principles into the teaching of artificial intelligence in universities and research centers is developing slowly but progressively, although no uniform or mandatory model currently exists. Most higher education institutions in the region recognize the importance of training professionals capable of designing, implementing, and overseeing AI systems responsibly, taking into account their social, economic, and legal impacts. Some universities have introduced specific courses on artificial intelligence, and the ethics of AI is becoming an increasingly common topic of academic inquiry; however, dedicated degree programs in this field are not yet in place. What does exist are general ethics courses, and those that address AI-related ethics tend to focus on fairness, transparency, data privacy, corporate responsibility, and algorithmic explainability.

There is also an ongoing debate regarding the depth and mandatory nature of ethics training within AI curricula, as well as the need for stronger coordination among universities, research institutions, governments, and international organizations. This discussion aims to define more systematic and coherent strategies to ensure that future AI developers act with social responsibility and adhere to robust ethical principles.

Recommendations

1. Integrate ethical AI governance into university curricula: ministries of education and universities should incorporate mandatory modules on AI ethics across degree programs in engineering, data science, law, and related fields, with a focus on human rights, fairness, privacy, and technological sustainability.
2. Strengthen cooperation among academia, governments, and international organizations: promote partnerships to develop curricular frameworks and joint research projects on AI ethics and governance, aligned with international standards.
3. Establish faculty training and certification programs in technological ethics: implement capacity-building programs for professors and researchers to integrate ethical dilemmas related to AI into teaching practices, fostering continuous learning and interdisciplinary research.
4. Create regional and bi-regional academic observatories on ethical AI governance: encourage the establishment of university networks and observatories to monitor progress in AI ethics education and promote the exchange of best practices across countries.

Section 16. Regulations on algorithmic transparency

Are there regulations on the transparency of the algorithms used in AI systems in your country? If so, what do they establish?

Summary

In most of the countries surveyed, there are no specific regulations that govern the transparency of the algorithms used in AI systems. However, several governments have begun discussing and promoting initiatives to ensure traceability, explainability, and accountability in the use of these technologies. At present, algorithmic transparency is addressed indirectly through general laws on personal data protection, access to public information, consumer protection, and digital government frameworks, which require the disclosure of automated criteria or processes when they affect citizens' rights.

Chile, Colombia, Paraguay, and Uruguay are the countries reporting concrete advances. Chile, for example, incorporated principles of transparency and explainability into its National AI Policy (2021), promoting the development of AI systems that are understandable to users. In Colombia, the National AI Strategy establishes the obligation to ensure auditability and accountability in automated systems. Uruguay, through its E-Government Agency, has issued guidelines on the responsible and transparent use of algorithms in the public sector, while Paraguay is developing regulatory initiatives to ensure the traceability of algorithmic decisions.

From a broader perspective, although specific regulations are still not predominant, regional trends point toward the creation of legal frameworks that require transparency in the algorithms used in AI systems and reinforce algorithmic accountability, thereby strengthening public trust and safeguarding human and fundamental rights in their implementation.

Recommendations

1. Develop national regulatory frameworks for algorithmic transparency and explainability: establish laws governing the transparent use of AI algorithms, requiring the disclosure of decision-making criteria, data traceability, and audit mechanisms.
2. Create specialized bodies for algorithmic oversight: establish technical entities or national committees to evaluate the functioning of AI systems across the public and private sectors, ensuring accountability, bias detection, and correction of irregularities. These bodies should include participation from academia, civil society, and experts in digital ethics.
3. Promote regional and interregional cooperation on best practices: foster collaboration among Latin American countries and between the EU and LAC to exchange regulatory experiences, audit methodologies, and training on algorithmic governance. The creation of permanent EU–LAC forums on AI ethics and transparency will help advance toward common standards that ensure the responsible, fair, and verifiable use of algorithms in the region.

Section 17. Prevention of algorithmic discrimination and independent oversight

Are there measures in place in your country to prevent algorithmic-driven discrimination, as well as independent bodies responsible for overseeing equality and algorithmic transparency?

Summary

Across the ten countries surveyed, there is a growing concern about discrimination arising from algorithmic systems and about the need for effective oversight mechanisms. However, no homogeneous regional framework exists. Only a few governments have taken concrete steps toward dedicated measures and supervisory structures. At the same time, most countries continue to rely on general legal provisions—such as constitutional guarantees, data protection laws, access-to-information rules, consumer protection, and competition law—that provide only limited and indirect regulation of artificial intelligence systems and emerging technologies.

Chile, Colombia, Paraguay, and Uruguay report concrete initiatives (policies, guidelines, or technical bodies) to ensure algorithmic traceability, auditing, and fairness. Ecuador, Peru, and

Argentina are making progress through sector-specific guidelines or legislative proposals that incorporate risk assessment and transparency obligations, particularly in the public sector. Brazil, Mexico, and Bolivia apply constitutional principles, data protection frameworks, and digital governance norms to address algorithmic risks, yet lack a dedicated, independent national body to monitor algorithmic fairness continuously.

Although general legal references—such as non-discrimination, data protection, and access to justice—allow for intervention in cases of bias, independent and specialized oversight remains incipient across most of the region. To strengthen protection, it is essential to establish independent technical units, mandatory algorithmic auditing requirements, and accessible redress mechanisms for individuals affected by automated discrimination.

Recommendations

1. Establish legal frameworks on algorithmic fairness: adopt specific regulations that ensure transparency and non-discrimination in artificial intelligence systems, aligned with international standards and the EU AI Act.
2. Create independent oversight bodies: establish autonomous entities responsible for auditing and monitoring algorithmic fairness and transparency across the public and private sectors.
3. Implement mandatory AI audits: require periodic assessments to identify biases and ensure that automated decision-making processes comply with human rights standards.
4. Promote ethical and technical training by providing capacity-building for public officials, developers, and auditors on responsible data management, fairness, and algorithmic bias mitigation.

Section 18. Protection of private life and privacy in the digital environment

Does the legislation in your country provide for measures to ensure the protection of family and/or private life in the digital environment? If so, what provisions are in place and what is their focus?

Summary

In most of the countries surveyed, national legislation includes measures to safeguard private and family life, as well as privacy in the digital environment, except in Ecuador, Paraguay, and Peru, where no specific frameworks, detailed regulations, or protocols have yet been adopted.

Overall, Argentina, Brazil, Chile, Colombia, Mexico, Uruguay, and Bolivia rely on personal data protection laws, constitutional provisions, and digital rights regulations that recognize privacy as a fundamental right. These norms impose obligations on public and private entities that process personal information, including requirements for informed consent, a legitimate purpose, data security, and individuals' rights to access, rectify, and delete their personal data. In some countries, such as Brazil and Mexico, specialized data protection authorities oversee compliance and may impose sanctions in case of violations.

Several countries also incorporate provisions on the ethical use of emerging technologies and automated data processing, placing particular emphasis on protecting minors, privacy in digital environments, and cybersecurity. The prevailing approach across the region seeks to ensure a balance between technological innovation and the safeguarding of fundamental rights, thereby promoting digital trust. Nevertheless, significant challenges remain in terms of effective implementation, inter-institutional coordination, and regulatory adaptation to rapid developments in artificial intelligence and large-scale data processing.

Recommendations

1. Promote regional harmonization and international cooperation: encourage the adoption of regional legal frameworks and EU–LAC cooperation agreements that ensure common standards for privacy and the ethical processing of personal data, taking the EU General Data Protection Regulation (GDPR) as a reference point. Such convergence facilitates regulatory interoperability, the secure exchange of information, and the equitable protection of digital rights.

2. Strengthen national data protection authorities: consolidate independent bodies with sufficient technical, legal, and financial capacities to oversee compliance with privacy legislation, impose effective sanctions, and advise public and private institutions on the ethical and secure use of personal data, particularly in light of advances in artificial intelligence-based technologies.

3. Update legal frameworks and promote digital literacy by revising existing legislation to incorporate principles for the responsible use of artificial intelligence, biometrics, digital surveillance, and cybersecurity. In parallel, implement digital literacy programs at all educational levels—primary, secondary, and tertiary—as well as initiatives targeting the general public and the public sector, aimed at strengthening knowledge of privacy, secure information management, and the protection of fundamental rights in digital environments.

Pillar IV

Cybersecurity, Global Digital Trust, and International Cooperation

Section 19. Use of AI in the fight against terrorism and criminality

Do the authorities in your country use AI to combat terrorism and criminality? If so, what guidelines, programs, and methods are applied?

Summary

Across all surveyed countries, authorities have begun using artificial intelligence systems to prevent and combat cyber-related offences, recognizing their potential to analyze large volumes of data and detect patterns of illicit activity in digital environments. Current applications include identifying financial fraud, cybercrime, attacks on critical infrastructure, and the dissemination of illegal content on networks and digital platforms. However, AI is not being used to combat terrorism.

The methods employed involve predictive data analytics, anomaly-detection algorithms, information-mining tools for online networks, and early-warning systems for cyber incidents. Machine-learning tools are also used to monitor suspicious behavior and prioritize response actions by competent authorities.

Although the adoption of AI-based tools is widespread, countries rely primarily on cybersecurity, data protection, and fundamental rights legislation to guide these practices, ensuring the legality, proportionality, and traceability of interventions. In several cases, internal operational protocols have been developed to provide guidance on oversight, auditing, and risk-mitigation measures, notably concerning bias or algorithmic errors.

Recommendations

1. Establish regulatory frameworks for the use of artificial intelligence in cybersecurity: develop national guidelines that define the limits, responsibilities, and operational protocols for the use of AI systems in the prevention of cyber-related offences, ensuring the protection of fundamental rights and the traceability of all actions.

2. Implement continuous auditing and oversight mechanisms: create internal and external mechanisms to periodically assess the performance, transparency, and fairness of the algorithms used by the authorities, including mechanisms to mitigate bias and correct errors in real time.

3. Strengthen the training and professionalization of specialized teams: provide technical personnel and security officials with training on the ethical and effective use of AI-based tools—including predictive analytics, anomaly detection, and information-mining techniques—ensuring responsible and reliable implementation.

4. Promote regional and international cybersecurity cooperation: encourage agreements for secure information exchange, the sharing of best practices, and the adoption of common

protocols among countries in the region and with the European Union, thereby facilitating the detection of cross-border threats and the development of joint technological solutions.

Section 20. Digital surveillance and international human rights standards

Do the digital surveillance regulations in your country comply with international human rights standards?

Summary

No existen leyes nacionales específicas sobre vigilancia digital, las autoridades se guían principalmente por tratados y normas internacionales de derechos humanos, así como por principios consagrados en convenios internacionales sobre privacidad, libertad de expresión y protección de datos. Estos marcos sirven como referencia para diseñar protocolos y regulaciones nacionales que buscan garantizar que las actividades de vigilancia digital respeten los derechos fundamentales. There are no specific national laws regulating digital surveillance, and authorities primarily rely on international human rights treaties and standards, as well as principles enshrined in international instruments on privacy, freedom of expression, and data protection. These frameworks serve as reference points for designing national protocols and regulations intended to ensure that digital surveillance activities respect fundamental rights.

No obstante, los gobiernos reconocen que la aplicación práctica de estos estándares enfrenta múltiples desafíos. La implementación efectiva no siempre se cumple, y en algunos casos la vigilancia digital puede exceder los límites previstos por los tratados internacionales, generando riesgos para la privacidad, la confidencialidad de losas comunicaciones y la protección de información sensible. Entre los principales obstáculos se encuentran la falta de mecanismos de supervisión independientes, recursos técnicos limitados y capacitación insuficiente del personal encargado de las operaciones de vigilancia. However, governments acknowledge that the practical application of these standards faces multiple challenges. Effective implementation is not always achieved, and in some cases digital surveillance practices may exceed the limits established under international treaties, creating risks to privacy, the confidentiality of communications, and the protection of sensitive information. Key obstacles include the lack of independent oversight mechanisms, limited technical resources, and insufficient training of personnel responsible for surveillance operations.

Para la región, el desafío central es asegurar que la seguridad y la prevención de delitos no comprometan los derechos humanos. Esto requiere fortalecer la supervisión independiente, la rendición de cuentas y la transparencia, así como promover la formación y la cultura de respeto a los derechos humanos en todas las operaciones de vigilancia digital, garantizando que, la normativa internacional se traduzca en práctica efectiva. For the region, the central challenge is to ensure that security and crime prevention do not compromise human rights. This requires strengthening independent oversight, accountability, and transparency, as well as promoting training and a culture of respect for human rights across all digital surveillance operations, ensuring that international norms are effectively translated into practice.

Recommendations

1. Establish specific national legal frameworks for digital surveillance: create laws that comprehensively regulate digital surveillance, incorporating international human rights standards on privacy, freedom of expression, and data protection, ensuring their applicability and effective enforcement.
2. Strengthen independent oversight mechanisms: establish autonomous supervisory bodies to monitor digital surveillance activities, assess their compliance with regulations, and ensure accountability in cases of potential abuses or rights violations.
3. Specialized training and capacity-building for personnel: develop continuous training programs for operators and officials responsible for digital surveillance, focused on human rights protection, ethical data management, and compliance with international protocols.
4. Transparency and accountability in surveillance processes: promote the publication of periodic reports on the use of digital surveillance technologies, including statistics, risk assessments, and corrective measures, fostering public trust and citizen oversight.
5. Integration of international standards into operational practice: ensure that digital surveillance protocols and procedures effectively translate international treaties and conventions into concrete actions, incorporating safeguards that minimize risks to privacy, communication confidentiality, and the protection of sensitive information.

Conclusion

The digital transition in the countries surveyed constitutes a complex, multifaceted process that combines technological expansion with a profound social, economic, and institutional transformation. This phenomenon goes beyond the mere adoption of new digital tools. It entails reconfiguring productive structures, redefining educational and labor models, and the need to build regulatory frameworks capable of protecting human rights and fundamental freedoms in digital environments. In this context, digitalization represents both an unprecedented opportunity for sustainable development and social inclusion, and a structural challenge that requires coordinated action at the regional, bi-regional (EU–LAC), and international levels.

The ten countries analyzed show significant progress in the incorporation of emerging and disruptive technologies, including, but not limited to, artificial intelligence (AI), big data, blockchain, intelligent automation, and the Internet of Things. These innovations are being applied across diverse sectors—including public administration, education, health, agriculture, and financial services—contributing to greater efficiency, transparency, and competitiveness in productive activities. In particular, the expansion of AI is enabling improvements in decision-making processes, while the use of massive datasets is generating new models for predictive analysis and evidence-based management. However, despite these advances, structural inequalities continue to limit both the scope and the sustainability of the digital transformation process. Divides in connectivity, access to technological infrastructure, digital-skills development, system interoperability, and the protection of digital rights remain deep and heterogeneous. In many countries, rural areas continue to lag behind in access to high-speed networks, hindering their ability to benefit from the opportunities that digitalization offers for agricultural production, distance education, and telemedicine. Likewise, gender inequality in access to and use of technology persists as a barrier to women's full participation in the digital economy.

These divides are not only technological, but also social and political. The lack of digital literacy and technological skills among broad segments of the population limits societies' ability to integrate inclusively into the new digital paradigm. Moreover, the absence of regulatory frameworks on data protection, privacy, intellectual property, and cybersecurity creates vulnerabilities that may be exploited by malicious actors or by dominant companies with considerable market power.

In this context, bi-regional cooperation between the European Union and Latin America and the Caribbean (EU–LAC) acquires strategic relevance. The EU–LAC Digital Alliance, framed within the Global Gateway initiative, is an essential instrument for coordinating joint efforts across key areas such as connectivity, ethical governance of artificial intelligence, sustainable technological innovation, digital skills development, and cybersecurity. This approach seeks not only to harness the opportunities of digital development but also to promote a people-centered transformation model grounded in shared values such as democracy, human rights, the rule of law, sustainability, and equity.

Cooperation between the two regions enables progress toward regulatory frameworks and global technological governance rooted in the protection of human rights, algorithmic transparency, data privacy, and environmental sustainability. EU–LAC cooperation emerges as a necessary counterbalance to the growing concentration of power held by Big Tech companies and to loosely regulated models of digital governance that may endanger States' technological sovereignty.

Within this broader context, the following potential areas of EU–LAC cooperation are identified:

1. Connectivity, telecommunications, and technological innovation: expand digital infrastructures — including fiber-optic networks, 5G, and satellite systems — to reduce territorial divides and promote digital inclusion, while fostering innovation labs, incubators, and acceleration programs that connect start-ups, universities, and companies, promoting strategic sectors such as biotechnology, clean energy, digital health, and agri-tech, strengthening knowledge economy and regional competitiveness, and ensuring regulatory frameworks that guaranteeing net neutrality, fair competition, and environmental sustainability.
2. EU–LAC cooperation on tech diplomacy and global technological governance: tech diplomacy enables sustained dialogue among States, institutions, academia, civil society, and Big Tech to address algorithmic transparency, privacy, cybersecurity, and the ethical use of artificial intelligence. Joint regulatory frameworks foster global standards on technological ethics, digital rights, and interoperability, strengthening trust, sustainability, and the participation of both regions in international digital governance.
3. Cybersecurity and data protection: develop joint digital-security protocols, harmonize data-protection regulations (based on the GDPR), and train specialized talent, thereby strengthening digital trust and facilitating secure cross-border information exchange.
4. Education, digital skills, and ethical governance: strengthen digital-literacy programmes and advanced training in artificial intelligence, cybersecurity, and technological ethics, promoting knowledge transfer and the exchange of best practices between the European Union and Latin America and the Caribbean countries to support the development of specialized talent, foster digital inclusion, and consolidate an ethical, inclusive, responsible, and sustainable technological governance model.

Taken together, this report seeks to strengthen bi-regional dialogue between the European Union and Latin America around the construction of an ethical, sustainable, and inclusive digital transition. By offering comparative analysis and proposals for strategic cooperation, it aims to support the development of evidence-based public policies to reduce digital divides, protect rights, and promote responsible innovation. The consolidation of a shared ethical framework for global technological governance between both regions represents not only an opportunity for development but also a concrete expression of the shared values of democracy, equity, sustainability, and respect for human dignity that have historically guided EU–LAC relations.