CELE
Centro de Estudios en Libertad de Expresión

Artículo de investigación

74

Emerging Technologies and Human Rights from the Perspective of the Inter-American Legal Framework

Agustina Del Campo

June 2025

Agustina Del Campo, "Emerging Technologies and Human Rights from the Perspective of the Inter-American Legal Framework", Artículo de investigación No. 74 (ENG), Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2025)

UP
Universidad de Palermo

Facultad de Derecho

Centro de Estudios en Libertad de Expresión

Emerging Technologies and Human Rights from the Perspective of the Inter-American Legal Framework

Agustina Del Campo

Director

adelgampoiso@gmail.com

June 2025

I. I. Introduction and Scope of the Article

Emerging technologies are radically transforming contemporary societies and human activities. We are currently undergoing a period of profound scientific and technological change that breeds curiosity, optimism, hope, and concern. Perspectives on development and change range from "techno-solutionist" views—those that see technology as the answer to a wide array of serious social problems—to deep concern about the potential impact of these developments on the social fabric.

Emerging technologies are scientific and technical innovations under development that have the potential to significantly transform society, the economy, and human interaction. These technologies are characterized by their rapid evolution, their disruptive impact across various sectors, and the new ethical and regulatory challenges they present (OECD, 2018; UN, 2019). They include, among others, artificial intelligence (AI), robotics, 3D printing, the Internet of Things, and biotechnology.

This article aims to introduce the main challenges posed by emerging technologies and to highlight key human rights standards within the Inter-American Human Rights System (IAHRS) that can contribute to ongoing debates and inform responses. Without seeking to provide an exhaustive analysis, the text lays the groundwork for more in-depth future research by identifying critical areas of concern and the relevant legal instruments within the IAHRS. This paper builds on four prior essays commissioned as part of a Ford Foundation project implemented by the Inter-American Institute of Human Rights (IIHR) in 2023. These essays addressed regulatory challenges (spanning self-regulatory, normative, ethical, political, and legal dimensions) in relation to blockchain, artificial intelligence, neurotechnologies, and surveillance and facial recognition technologies. Rather than replicating or summarizing the findings of each of these essays, the purpose of this article is to interpret them through the lens of established human rights standards within the IAHRS, identifying solid normative benchmarks that may help guide concrete solutions and address the questions that remain open. Given the rapidly evolving nature of this field, identifying these unresolved questions is a critical task in itself.

In this regard, the article will introduce some of the most pressing human rights challenges within the context of the Inter-American Human Rights System (IAHRS), including:

- The right to privacy and the protection of personal data

- The right to freedom of expression
- The right to equality and non-discrimination
- The right to due process

These rights are protected by various instruments within the Inter-American Human Rights System (IAHRS), such as the American Convention on Human Rights (ACHR) and the case law of the Inter-American Court of Human Rights (IACtHR). The article will examine how these instruments can be interpreted in an evolving manner and applied in the context of emerging technologies.

II. The Importance of a Rights-Based Approach

In recent years, concerns about the ethical and legal challenges posed by the rapid development of new technologies have driven the gradual emergence of an international regulatory framework. Multilateral initiatives have also sought to address these issues comprehensively.

Various international mechanisms have emphasized the need to frame both technological development and its regulation within international human rights law, beginning with initiatives led by the United Nations (UN), including the World Summit on the Information Society (WSIS) and the establishment of the Internet Governance Forum[1].

Over the past decade, the United Nations has established several mechanisms, including the Special Rapporteur on the right to privacy in 2015[2]; the High-Level Panel on Digital Cooperation (2018)[3]; the B-Tech Project in 2019[4], aimed at advising States and businesses on the implementation of the UN Guiding Principles on Business and Human Rights; the Office of the Tech Envoy in 2022[5]; and the High-Level Advisory Body on Artificial Intelligence convened in 2023[6].

In November 2021, UNESCO's General Conference adopted the Recommendation on the Ethics of Artificial Intelligence to protect and promote human rights. The UN Human Rights Council has also addressed the risks associated with new technologies. In this regard, a 2021 report of the UN Human Rights Council Advisory Committee raised concerns about the discriminatory impact of emerging digital technologies and the threats they pose to individuals' mental autonomy.

---

[1] United Nations (n.d.). Internet Governance Forum (IGF). Retrieved from: https://publicadministration.desa.un.org/projects/internet-governance-forum-igf-2006-current

[2] United Nations Human Rights Council, OHCHR (2015). The Human Rights Council established the mandate of the Special Rapporteur on the right to privacy. Retrieved from: https://www.ohchr.org/en/press-releases/2015/03/human-rights-council-creates-mandate-special-rapporteur-right-privacy.

[3] United Nations (2018). High-level Panel on Digital Cooperation. Retrieved from: https://www.un.org/en/pdfs/HLP-on-Digital-Cooperation_Press-Release.pdf.

[4] Office of the United Nations High Commissioner for Human Rights (OHCHR) (2019). B-Tech Project. Retrieved from: https://www.ohchr.org/es/business/b-tech-project#:~:text=El%20Proyecto%20B%2DTech%20proporciona,la%20esfera%20de%20la%20tecnolog%C3%ADa.

[5] United Nations General Assembly (2020). Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation, A/74/821. Retrieved from: https://documents.un.org/doc/undoc/gen/n20/102/51/pdf/n2010251.pdf.

[6] United Nations (2023). High-level Advisory Body on Artificial Intelligence. Retrieved from: https://www.un.org/techenvoy/ai-advisory-body.

The Organisation for Economic Co-operation and Development (OECD) adopted the Principles on Artificial Intelligence, which provide guidance to governments, organizations, and individuals on prioritizing human interests and ensuring accountability in the design and governance of AI systems. In September 2024, within the framework of the Summit of the Future, world leaders convened by the United Nations adopted the Pact for the Future, which included the Global Digital Compact, committing to respect, protect, and promote rights in the digital space.[7] [8]

These documents argue, to varying degrees, for the need to protect and promote human rights in the digital environment. International human rights law constitutes a normative framework shared by all countries globally, designed and adopted to protect and promote the fundamental rights of individuals against state power. Although approaches to human rights may vary from country to country, the human rights narrative provides a common language, ideally suited to dealing with global, interjurisdictional, and often decentralized technologies such as the Internet. With over 75 years of development, it has strengthened democracies around the world, promoted liability and accountability for atrocities, and limited the abuse of power.

Despite persistent human rights challenges and an unprecedented democratic crisis, it remains important—one year after the 75th anniversary of the Universal Declaration of Human Rights—to reaffirm this framework as both desirable and achievable, and as a shared guide for the ongoing technological transformation.

i. Technical and policy approaches to emerging technologies

Emerging technologies are scientific and technical innovations that offer unprecedented potential, while in many cases, their risks remain unknown. Most experts agree that these technologies are still in an experimental phase. These innovations significantly transform the boundaries between virtual, physical, and biological spaces.

According to the report of the Advisory Committee of the United Nations Human Rights Council (2021), emerging technologies include:

"data distribution and automated decision-making, such as artificial intelligence, the Internet of things, blockchain technology and cloud computing, among others."[9] It also refers to "a breadth of responses on many different types of systems, including robotics, automation, wireless waves, predictive analytics and various types of information and communications technology (ICT) that are present at different stages of the datafication cycle."[10]

The World Economic Forum (WEF), in its report Top 10 Emerging Technologies of 2023, highlights that these technologies can be characterized by several features, including:

---

[7] United Nations General Assembly (2024). El Pacto del Futuro [Pact for the Future], Resolution adopted by the General Assembly on 22 September 2024, A/RES/79/1, Annex: Pacto Digital para el Futuro [Global Digital Compact], retrieved from https://documents.un.org/doc/undoc/gen/n24/272/25/pdf/n2427225.pdf.

[8] Ibid.

[9] United Nations (2021). Impactos, oportunidades y retos que pueden entrañar las tecnologías digitales nuevas y emergentes en relación con la promoción y la protección de los derechos humanos [Impacts, opportunities and challenges of new and emerging digital technologies for the promotion and protection of human rights], Human Rights Council Advisory Committee Report, A/HRC/47/52. Retrieved from: https://documents.un.org/doc/undoc/gen/n20/102/51/pdf/n2010251.pdf

[10] Ibid.

- ➢ Novelty: the technology is emerging and at an early stage of incipient development, not already widely used.
- ➢ Applicability: has the potential to be of significant use and benefit to societies and economies in the future; is not of only marginal concern.
- ➢ Depth: is being developed by more than one company and is the focus of increasing investment interest and excitement within the expert community; likely to have a significant impact in the next 3-5 years.
- ➢ Power: is potentially powerful and disruptive in altering established ways and industries[11].

We are currently in a moment characterized by the proliferation of regulatory frameworks for technology. The way in which technological development is framed varies depending on the sector, the country, or international institutions and actors. Multiple parallel initiatives are competing to establish themselves as models for the industry.[12] In addition to corporate self-regulation, which was once preferred by various actors within the framework of global technology governance, there are now regional, global, ethical, legal, political, and economic initiatives of diverse kinds.

a. General approach vs. approach to specific uses

The challenges posed by technological development have given rise to multiple areas of tension. A common trend in comparative law, and even in international law, appears to be to address emerging technologies in an overarching manner while also attending to the regulation, self-regulation, and co-regulation of specific technologies. Thus, in recent years, principles, guidelines, and regulations have emerged for specific technologies such as artificial intelligence or neurotechnologies. The aforementioned Recommendation on the Ethics of Artificial Intelligence of UNESCO, as well as the AI Principles of the Organisation for Economic Co-operation and Development (OECD), are examples of this. The development of principles and regulations on neurotechnologies appears to be following this trend. UNESCO has launched a new process to develop recommendations in this area, following the model that led to the AI recommendations.[13] At the regional level, the Inter-American Juridical Committee (CJI) of the Organization of American States approved in March 2023 the Inter-American Principles on Neuroscience, Neurotechnologies and Human Rights, emphasizing the need for specific regulation to protect the rights of children and adolescents, as well as persons with disabilities.

This general approach, centered on the type of technology, contrasts with the development of standards and principles focused on the specific uses of technologies and their integration into—and impact on—preexisting social practices, rather than on the technology itself. For example, facial recognition technologies are regulated considering their potential use for mass surveillance or law enforcement purposes. This is the perspective adopted, for instance, by the European Parliament when it prohibits, in principle, the use of facial recognition technologies in the 2023 Artificial Intelligence Act, while establishing exceptions for their use in specific cases (even though these exceptions have been strongly criticized for their vagueness or breadth).

---

[11] World Economic Forum (June, 2023), *Top 10 Emerging Technologies of 2023*, Retrieved from https://www.weforum.org/reports/top-10-emerging-technologies-of-2023

[12] United Nations High-level Advisory Body on Artificial Intelligence (2024). *Gobernanza de la IA en beneficio de la humanidad* [Governing AI for Humanity]. Retrieved from: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.

[13] UNESCO (s.f). *Ética y neurotecnologías. [Ethics and neurotechnologies]. Retrieved from:* https://www.unesco.org/es/ethics-neurotech.

In their essay "Sonría, usted está siendo vigilado" [Smile, You Are Being Watched], Carolina Botero and Juan de Brigard illustrate this approach by analyzing the use of technology in policing and its relationship to broader notions of security in society. The focus is not on the technology itself, but rather on its potential use by the state apparatus and on how these practices or technological developments are embedded within the broader history of crime prevention and prosecution, stereotypes, security, and related concerns. Chomczyk Penedo approaches the analysis of blockchain technology in a similar way, which differs (or may differ) across the four specific uses described in the article: identity registration systems, voting, real property registration systems, and the banking and financial system[14].

General instruments often establish overarching principles for specific technologies while also addressing challenges linked to their particular uses. The 2023 European Artificial Intelligence Act illustrates this approach by combining general rules on AI with the identification of high-risk applications, such as biometric systems.

Different regulatory approaches present both advantages and disadvantages. General principles—such as UNESCO's Recommendation on the Ethics of Artificial Intelligence or the Inter-American Principles on Neuroscience—offer a broad framework within which more specific principles can then be developed for each of their potential uses. However, one of the risks of a broader approach is the vagueness that often accompanies a general and wide-ranging text in terms of human rights. The development of such frameworks has, in some cases, also contributed to the perception of a "legal vacuum" surrounding certain technologies and their deployment. As Hinestroza Arenas[15] points out in the accompanying essay on neurorights, this type of approach may lead to demands for new rights or renegotiations regarding the content of existing rights. Use-based approaches tend to be more specific and allow for a more careful formulation of the elements necessary for the protection and promotion of human rights in the development, deployment, and implementation of new technologies across different contexts. Undoubtedly, these approaches are complementary.

b. Risk-based approaches vs. rights-based approaches

The experimental nature of emerging technologies, combined with the pace of their development, has raised significant questions about their impact on society and on the exercise and protection of human rights. A large part of this technological development is in the hands of the private sector, which operates under the United Nations Guiding Principles on Business and Human Rights (UNGPs). These non-binding principles promote a risk-based approach and are incorporated in most countries within the framework of corporate social responsibility.

The UN Principles were the result of years of negotiation and disagreements regarding the applicability and binding nature of human rights obligations in the private sector.[16] In essence, the Principles reaffirm the responsibility of States as the primary actors in the prevention, protection, and promotion of human rights, while setting out recommendations for companies to identify, assess, and mitigate the potential impacts of their activities on human rights. These recommendations should be implemented through mechanisms such as corporate due diligence and human rights impact assessments. The framework also clearly provides

[14] Chomczyk Penedo, A. (2023) *Tecnología blockchain: ¿es posible su uso respetando el derecho a la privacidad y otros derechos humanos?* Annex 4.

[15] Hinestroza-Arenas A. (2023) *Interfaces Ordenador-Cerebro: ¿es necesaria la protección de los neuro derechos para respetar los derechos humanos?* Annex 2.

[16] Alvarez Ugarte, R. (2020). *ICT and Human Rights: Towards a Conceptual framework of Human Rights Impact Assessments*. Retrieved from: https://www.palermo.edu/Archivos_content/2021/cele/papers/ICT-and-Human-Rights.pdf.

guidance for the information and communication technologies (ICT) sector, including infrastructure, protocols, and content intermediaries.

The UNGPs have been in force since their adoption in 2011, with varying levels of adherence and compliance by the companies concerned.[17] The voluntary nature of compliance and the absence of effective monitoring mechanisms have led several states and international organizations to promote more direct forms of state regulation. These regulations partially replicate the language of the Guiding Principles and incorporate obligations to identify and monitor risks to human rights stemming from the development, deployment, and application of technologies such as AI. They also establish specific obligations regarding mitigation and remediation.[18]

The risk-based approach proposed by the UNGPs has been adopted by various legislative proposals and soft law instruments internationally[19], generating clear benefits but also significant challenges. Among its advantages, this approach helps overcome the information asymmetry that characterizes this field, where the private sector has more and better tools to assess the impact of its services on society. It also gives effect to the principle of "immediacy," insofar as it creates obligations for those best positioned to know, prevent, and remedy harm.

Among the challenges, however, this approach delegates to the private sector the identification and mitigation of risks that are often unclear and lack concrete definitions, and it creates mitigation obligations that, in many cases, inevitably result in limitations on the exercise of certain rights, such as privacy or freedom of expression. Furthermore, in many instances, the articulation of risk-based obligations extends beyond the human rights framework to encompass all kinds of risks, some legally recognized as such and others not. The separation between risks and the legal framework where they are defined and conceptualized creates significant breadth and discretion, both for the company tasked with identifying, mitigating, and remedying them, and for the state supervisory body responsible for verifying compliance and assessing whether corporate conduct conforms to the applicable norms.[20]

c. *Ethics and Human Rights*

There is a growing tension between ethical guidelines and binding legal instruments in the field of emerging technologies and human rights. On the one hand, instruments such as UNESCO's Recommendation on the Ethics of Artificial Intelligence provide non-binding ethical guidance. On the other hand, international

---

[17] United Nations (2011). *Principios Rectores sobre Derechos Humanos y Empresas* [Guiding Principles on Business and Human Rights]. Retrieved from: https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf.

[18] Del Campo, A., Zara N., and Alvarez Ugarte R., *Are Risks the New Rights: the perils of the risks approach in tech regulation, (forthcoming)* Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5161173.

[19] Regulation (EU) 2022/2065, Digital Services Act https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022R2065; Regulation (EU) 2024/1689, Artificial Intelligence Act https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L_202401689 ; UNESCO, Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multistakeholder Approach, 2023, https://unesdoc.unesco.org/ark:/48223/pf0000387360 ; UNESCO, Recomendación sobre la ética de la inteligencia artificial [Recommendation on the Ethics of Artificial Intelligence], 2022, https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa; Organization of American States (OAS), Office of the Special Rapporteur for Freedom of Expression, Inclusión digital y gobernanza de contenidos en internet [Digital inclusion and content governance on the Internet], CIDH/RELE/INF. 28/24, 2024, https://www.oas.org/es/cidh/expresion/informes/Inclusion_digital_esp.pdf.

[20] Del Campo, A., Zara N., and Alvarez Ugarte R., *Are Risks the New Rights: the perils of the risks approach in tech regulation, (forthcoming)* Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5161173.

human rights treaties, such as the American Convention on Human Rights, establish binding legal obligations for states.

This tension raises several questions: How do these different types of instruments relate to one another? In the event of a conflict, which should prevail? Although there is a connection between ethics and law, the enforceability and monitoring of both spheres differ significantly. How can soft law (including ethical guidelines) influence the interpretation and application of human rights treaties in the context of new technologies? Are existing legal frameworks equipped to address the challenges posed by emerging technologies? The joint development of ethical, moral, and legal principles may dilute the concrete obligations established by existing international law. This paper proposes identifying areas where the law already provides precise rules that do not require adaptation and others where further development and specificity are needed.

III. Opportunities and challenges for the application of Inter-American standards in the development of emerging technologies

The incorporation of emerging technologies into everyday life has a significant impact on the social, political, and economic development of countries. It is advisable to analyze these technologies from a human rights perspective, since, although they encompass a wide range of technical and scientific advances, they directly affect the exercise and protection of human rights. The Inter-American Human Rights System (IAHRS) provides a robust framework for addressing the challenges posed by emerging technologies.

i. Freedom of expression

The 2009 Joint Declaration of the Special Rapporteurs[21] already referred to the importance of freedom of expression, including on the Internet. The first thematic report of the United Nations to directly address the issue of human rights and technology was Frank La Rue's 2011 report.[22] The Inter-American Commission on Human Rights (IACHR) has recognized that new information and communication technologies have facilitated freedom of expression and access to information. However, it has also warned of the risks that these technologies may pose to other rights (Office of the Special Rapporteur for Freedom of Expression, IACHR) Libertad de expresión e internet [Freedom of Expression and the Internet,], OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13, 2013).

The right to freedom of expression is enshrined in Article 13 of the American Convention on Human Rights (ACHR). The wording of Article 13 differs in part from that of Article 19 of the International Covenant on Civil and Political Rights and Article 10 of the European Convention on Human Rights. It is the only one of the three that explicitly prohibits prior censorship and indirect restrictions by the state.

Article 13(2) of the American Convention on Human Rights expressly provides that the exercise of freedom of expression

Shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: (a) respect for the rights or reputations of others; or (b) the protection of national security, public order or public health or morals. According to the Inter-American Commission on Human Rights (IACHR), prior censorship "(...) occurs when, through the

[21] Inter-American Commission on Human Rights (IACHR) (2011). Declaración Conjunta sobre Libertad de Expresión e Internet [Joint Declaration on Freedom of Expression and the Internet]. Retrieved from: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849.

[22] La Rue, F. (2011) *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, (A/HRC/17/27) 2011 Retrieved from: https://digitallibrary.un.org/record/706200?ln=en&v=pdf.

exercise of public authority, measures are adopted to prevent in advance the free circulation of information, ideas, opinions, or news, by any procedure that conditions expression or the dissemination of information on prior state control, for example, by prohibiting publications or seizing them, or any other procedure aimed at achieving the same end.[23]"

The Inter-American Commission on Human Rights (IACHR) has held that prior censorship is the archetypal form of extreme and radical violation of freedom of expression, as it entails its suppression.

Freedom of expression is the rule, and any restriction on it must be exceptional, imposed through subsequent liability established by law, and must be proportionate and necessary.[24] These subsequent liabilities must not be discriminatory or produce discriminatory effects.[25]

Much of the technological development of recent years directly or indirectly affects the exercise of freedom of expression or has applications that may impact it. Artificial intelligence has enabled the automated moderation of content on the Internet, curating online content in real time, filtering and blocking certain materials, and monitoring expression on an unprecedented scale. In addition, generative AI has revolutionized the production of written and audiovisual content, expanding possibilities in terms of creation, replication, forgery, layering, and related practices. This development, as Aguerre notes in the accompanying essay, has prompted immediate responses from the private sector, governments, civil society, and academia globally due to the opportunities and risks it presents.[26] On the one hand, the availability of AI entails radical changes in efficiency and speed in content production and threatens to distort various aspects of the current labor landscape. On the other hand, the rapid pace of its development, combined with limited knowledge and technical capacity to audit these technologies, also raises concerns regarding due process, equality, and non-discrimination, including in their application to freedom of expression standards.

Likewise, disparities in access to these technologies and in their governance have been identified as threats to the sustainable development of countries that remain excluded from their benefits. Only a limited number of companies and/or countries worldwide are capable of developing effective AI systems, even at an experimental stage. According to the High-level Advisory Body on Artificial Intelligence of the United Nations, in its report Governing AI for Humanity, only a few countries have participated in drafting key AI governance instruments, and many have not participated in any, despite being directly or indirectly affected by these technologies.[27] Likewise, biometric technology applied in the public sphere also poses threats to the

---

[23] Organization of American States (OAS), Inter-American Commission on Human Rights (IACHR) (2019), *Informe Anual de la Comisión Interamericana de Derechos Humanos 2009*, *Informe de la Relatoría Especial para la libertad de expresión* [Annual Report of the Inter-American Commission on Human Rights 2009, Report of the Office of the Special Rapporteur for Freedom of Expression] (OEA/Ser. L/V/II., December 30, 2009, p. 272.) See also Inter-American Court of Human Rights, *Case Palamara Iribarne Vs. Chile*, 2005, Series C No. 135, para. 68. Retrieved from: https://www.corteidh.or.cr/docs/casos/articulos/seriec_135_esp.pdf

[24] Organization of American States (OAS), Inter-American Commission on Human Rights (IACHR) (2015), *Informe Anual de la Comisión Interamericana de Derechos Humanos*, *Informe Anual de la Relatoría Especial para la Libertad de Expresión*, (OEA/Ser.L/V/II., Doc. 48/15, December 31, 2015, Para. 25). [Original in Spanish.]

[25] Organization of American States (OAS), Inter-American Commission on Human Rights (IACHR) (2019), *Informe Anual de la Comisión Interamericana de Derechos Humanos 2009*, *Informe de la Relatoría Especial para la libertad de expresión* [Annual Report of the Inter-American Commission on Human Rights 2009, Report of the Office of the Special Rapporteur for Freedom of Expression] (OEA/Ser. L/V/II., December 30, 2009, p. 251.)

[26] Aguerre, C. (2023) *Inteligencia Artificial, Innovación y Derechos Humanos. Notas para una marcha cautelosa en América Latina*. Annex 1.

[27] United Nations High-level Advisory Body on Artificial Intelligence (2024), *Gobernanza de la IA en Beneficio de la Humanidad* [Governing AI for Humanity], p. 9 Retrieved from: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.

rights to anonymity and protest, in addition to the risks to privacy and due process that will be addressed below.

Similarly, the Internet of Things enables surveillance that extends into the most private and intimate domains of individuals' lives. Neurotechnologies, as highlighted by the Inter-American Juridical Committee (CJI), pose risks to freedom of expression and opinion insofar as they create opportunities for manipulation and interference with individual will and dignity. The Inter-American Juridical Committee (CJI), in line with Principle 7 of the Inter-American Principles on Neuroscience, Neurotechnologies and Human Rights, underscores the importance of protecting individuals' neurocognitive integrity. It emphasizes the need to prevent illegitimate or harmful uses of neurotechnologies, particularly where they may be used to interfere with brain activity or to restrict the exercise of human rights. It further stresses that access to a person's mental activity must never compromise freedom of thought and conscience, nor render these dependent on third parties, as this would undermine rights, security, and personal autonomy.[28]

Threats to freedom of expression arise from both the public and the private sectors. With regard to the state, technology enables an unprecedented level of scrutiny and surveillance, providing countries around the world with tools for monitoring and observing public discourse on a scale never seen before, thereby threatening freedom of expression and association, among other rights. In addition, the current capacity to systematize information enables intelligence gathering from open sources, which remains largely underregulated across different regions of the world, including the Inter-American region.[29] With the widespread diffusion of the Internet and its mass adoption, states have also engaged in practices that have, in many cases, proven counterproductive and problematic from a freedom of expression perspective, including campaigns to stigmatize and persecute minorities and dissidents, state-sponsored disinformation, and abusive practices in the conduct of online electoral campaigns, among others.

From the private sector perspective, what once appeared to be fully decentralized and neutral has, over time, become increasingly concentrated in the hands of a limited number of specific companies. This has led to certain practices, such as the moderation and curation of content on the Internet, having a disproportionate impact on the freedom of expression of an ever-growing group of users and content producers, including journalists, civil society actors, artists, and influencers. Social media platforms and other online intermediaries have become key "gatekeepers" of online freedom of expression. Their content moderation policies, often implemented through AI algorithms, can exert a significant influence on public discourse, and the failure of companies to adhere to clear and human rights–respecting criteria may undermine the strength of the public debate required in a democratic society.[30] Moreover, the private regulation of online speech is shaped by various technologies, including surveillance and monitoring tools, automation, and artificial intelligence.

On the other hand, the dominance of a small number of technology companies over the main online communication channels raises concerns about diversity and pluralism in public discourse. The Office of the

---

[28] See, in this regard, Principio 7 de la Declaración de Principios Interamericanos en Materia de Neurociencias, Neuro tecnologías y Derechos Humanos [Principle 7 of the Inter-American Declaration of Principles on Neuroscience, Neurotechnologies and Human Rights].

[29] Bertoni, E. (2023) *Las prácticas OSINT, ¿son amigas o enemigas de los derechos humanos?*, CELE. Retrieved from: https://www.palermo.edu/Archivos_content/2023/cele/papers/231115-Bertoni-reporte-inicial-OSINT.pdf., Zara N. (2023). *Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay*, CELE, Retrieved from: https://www.palermo.edu/Archivos_content/2023/cele/papers/233008-reporte-regional-OSINT.pdf.

[30] United Nations (2011), *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión* [Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression] (A/HRC/38/35). Retrieved from: https://digitallibrary.un.org/record/706200?ln=en&v=pdf

Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) has held that concentration of media ownership is a practice that undermines the plurality of voices and hinders the diverse expression of different sectors of society. Concentration on the Internet poses new challenges, one of which is how to define concentration itself. What criteria should be used to determine market dominance? And, if so, which market is at issue? Given the cross-jurisdictional nature of the Internet, not all states are equally positioned to regulate a global and decentralized market such as the one the Internet entails. The European Union has recently adopted the Digital Markets Act, and the implementation process will likely yield lessons learned and best practices both for the Union and other countries with smaller markets or more limited regulatory capacities.

The wording of Article 13 of the American Convention on Human Rights, together with the principles developed in Inter-American jurisprudence on freedom of expression, makes it possible to formulate preliminary statements applicable to these and to other technologies that affect or may affect this right. A first assertion, following what has been established above, is that freedom of expression is protected regardless of the medium used to exercise it, and that the right applies to protected expression in any format. States have an obligation to refrain from arbitrarily interfering with its exercise.[31] In other words, online and offline expressions are protected, whether generated organically or artificially, and whether true or false.

However, technological advances have generated new debates related to freedom of expression. For example, discussions have emerged around copyright—particularly in relation to AI-generated content—as well as the potential harms such content may cause, including disinformation, discrimination, stigmatization, or even defamation. In addressing these issues, Inter-American principles and case law make it possible to assert that whenever the State restricts freedom of expression, it must do so in accordance with a law, in a clear manner, and following procedures established by law. Such law must pursue a legitimate objective, and be necessary and proportionate. The manner in which issues arising from technological development are addressed —and their application or implications for the exercise of rights recognized by law—will depend on each state. In no case, except for the explicit exceptions established by the American Convention on Human Rights, may States order or indirectly promote prior censorship. This is reflected in multiple instruments developed within the Inter-American Human Rights System (IAHRS), including the report on freedom of expression and electoral disinformation commissioned by the Organization of American States General Assembly to the Office of the Special Rapporteur for Freedom of Expression (2018).[32]

In addition, according to the Regional Observatory on Freedom of Expression of the Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), technological development has reopened debates on freedom of expression that seemed to have been settled until the 2010s. Among them are debates surrounding the right to be forgotten, defamation on the Internet, discriminatory speech, and harmful—but not illegal—speech. There is a trend toward reopening legislative debates aimed at modifying well-established standards in the case law of the Inter-American system, often justified by the speed,

---

[31] This position was expressed by the special rapporteurs of the United Nations, the Organization for Security and Co-operation in Europe (OSCE), the Organization of American States (OAS), and the African Commission on Human and Peoples' Rights (ACHPR) (2017), who warned that "general prohibitions on the dissemination of information based on vague and ambiguous concepts, including 'false news' ('fake news') or 'non-objective information', are incompatible with international standards on restrictions to freedom of expression." UN, OSCE, OAS, ACHPR Declaración Conjunta Sobre Libertad De Expresión Y "Noticias Falsas" ("Fake News"), Desinformación Y Propaganda, 2017, para. 2a.

[32] Organization of American States (OAS), Office of the Special Rapporteur for Freedom of Expression (2019), Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales [Guide to Guaranteeing Freedom of Expression in the Face of Deliberate Disinformation in Electoral Contexts], OEA/Ser.D/XV.22, 2019, https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf.

permanence, and volume of content available on the Internet.[33] A similar pattern can be observed in other regions of the world, including Africa, Europe, and Asia. While in many cases legislatures succeed in conducting healthy debates and reject solutions that are contrary to freedom of expression, particularly after the COVID-19 pandemic and amid the democratic crisis affecting various regions for decades, a number of laws have nevertheless been adopted that run counter to well-established human rights standards.

States not only have obligations to respect human rights, but also—consistent with Articles 1, 2, and 13 of the American Convention on Human Rights—have obligations to ensure rights without discrimination and to adapt their domestic legal systems to the Convention. The obligation to respect entails negative obligations on the part of the State, that is, obligations of non-interference. By contrast, the responsibility to guarantee human rights entails positive obligations, including the adoption of laws that guarantee the effective exercise of the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, through any medium. This obligation has recently been emphasized by various national and international bodies, such as UNESCO.

In 2023, UNESCO adopted the Guidelines for the Governance of Digital Platforms to guide States in developing regulatory safeguards.[34] UNESCO's work appears to have been largely inspired by the pioneering European regulation in this area: the Digital Services Act. This law, adopted in 2022, is the first specifically devoted to the governance of social media platforms and search engines, particularly to exert some degree of oversight over the private sector engaged in the curation, hosting, and promotion of third-party content (primarily search engines and social media, but also some e-commerce platforms). Adopted by the European Parliament and partly implemented by the European Commission in collaboration with various Member States, the law proposes a risk-based approach to platforms and identifies, in Article 34, a set of risks that platforms must assess, report, and mitigate. The instrument also establishes certain obligations, such as due process, notice, and the right of appeal, which companies engaged in content moderation must henceforth take into account in relation to their users. It further includes transparency obligations regarding terms and conditions of service, as well as requirements to regularly report on their practices and statistics concerning the implementation of their signal detection systems. These obligations are to be welcomed.

At the same time, however, these frameworks also entail relatively vague obligations regarding lawful content. The Digital Services Act, like the UNESCO Guidelines, adopts a risk-based approach to technology, identifying not only risks to human rights but also other risks potentially harmful permissible expressions that threaten civic space or democracy, as well as women and girls, and children and adolescents, among others. The latter risks pose particularly difficult challenges if European law were to serve as a possible model for domestic legislation in the Inter-American region. Differences in the formulation and scope of freedom of expression across both systems will undoubtedly be a source of contention, especially when interpreting the absolute prohibition of censorship under the Inter-American framework and the provisions concerning indirect restrictions.[35]

---

[33] Del Campo, A. (2023), *Volume, Speed, and Accessibility as Autonomous Harms: Can Modern Legal Systems Deal With Harmful but Legal Content? en New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*. Carnegie Endowment for International Peace. Retrieved from: https://carnegie-production-assets.s3.amazonaws.com/static/files/Feldstein_et_al_-_DDN_spread-UPDATED2.pdf.

[34] UNESCO. (2023) *Directrices para la gobernanza de las plataformas digitales: salvaguardar la libertad de expresión y el acceso a la información con un enfoque de múltiples partes interesada* [Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multistakeholder Approach]. Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000387360.

[35] Del Campo, A., Zara N., and Alvarez Ugarte R., *Are Risks the New Rights: the perils of the risks approach in tech regulation, (forthcoming)* Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5161173.

ii. Privacy

Privacy, enshrined in Article 11 of the American Convention on Human Rights (ACHR), faces new challenges in the digital age. This right is also recognized in the International Covenant on Civil and Political Rights,[36] the Universal Declaration of Human Rights,[37] and, from a comparative perspective, in Article 8 of the European Convention on Human Rights.[38]

The notion of private life "encompasses aspects of an individual's physical and social identity, including the right to personal autonomy, personal development, and the right to establish and develop relationships with other human beings and with the outside world.[39]" In Escher et al. v. Brazil (2009), the Inter-American Court of Human Rights held that "Article 11 of the Convention prohibits any arbitrary or abusive interference with the private life of individuals,"[40] and further noted that the right to privacy extends to digital information.

According to the Inter-American Commission on Human Rights (IACHR), the right to privacy protects at least four key legal interests: (i) freedom from arbitrary interference by the State or third parties; (ii) the right to autonomy in accordance with each individual's life plan; (iii) the right to prevent the disclosure of activities within the private sphere, including the circulation of information obtained therein without the individual's consent; and (iv) the right to one's own image.[41] The Inter-American Court of Human Rights has held that the right to privacy "encompasses the way in which the individual sees himself and how he chooses to project himself to others, and is an indispensable condition for the free development of personality.[42]"

Privacy is an enabling right that underpins the enjoyment of other rights and the free development of individuals' personality and identity, as well as their capacity to participate in political, economic, social, and cultural life.

---

[36] United Nations General Assembly (1966). *Pacto Internacional de Derechos Civiles y Políticos*. [International Covenant on Civil and Political Rights, Treaty] Series, vol. 999, p. 171, Retrieved from: https://www.refworld.org/legal/agreements/unga/1966/en/17703,

[37] United Nations General Assembly (1948), *Declaración Universal de los Derechos Humanos* [Universal Declaration of Human Rights], 217 A (III), Retrieved from: https://www.refworld.og/legal/resolution/unga/1948/en/11563.

[38] Council of Europe (1950), *Convenio Europeo de Derechos Humanos*, *modificado por los Protocolos Nos. 11, 14 y 15* [European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15] (ETS No. 005, November 4, 1950). Retrieved from: https://www.refworld.org/legal/agreements/coe/1950/en/18688]: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[39] Inter-American Court of Human Rights (2012), *Artavia Murillo y otros ("Fecundación in vitro") vs. Costa Rica* (Series C N. 257, para. 143) Retrieved from: https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf.

[40] Inter-American Court of Human Rights. (2009). *Caso Escher y otros vs. Brasil* (Series C No. 200, para. 113). [Original in Spanish.] Retrieved from https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp.pdf

[41] Office of the Special Rapporteur for Freedom of Expression (IACHR), Internet y Derechos Humanos [Internet and Human Rights], 2013, Para. 131, citing Inter-American Commission on Human Rights. Reports No. 82 /10. Case No. 12.524. Fontevecchia y D'Amico. Argentina. July 13, 2010. Para. 91, et seq. and Inter-American Court of Human Rights, Artavia Murillo y otros vs. Costa Rica (2012), para. 143.

[42] Inter-American Court of Human Rights (2012), *Artavia Murillo y otros ("Fecundación in vitro") vs. Costa Rica* (Series C N. 257, para. 143) [Original in Spanish]. Retrieved from: https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf.

Thus, "violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association.[43]" In particular, it is important to emphasize that privacy is an essential right in a democratic society, as it enables individuals to form and express their opinions freely and to participate in public debate without fear of reprisals. Furthermore, in Fontevecchia y D'Amicco vs. Argentina, the Inter-American Court of Human Rights held that the State has the obligation to guarantee the right to private life through positive actions, which may, in certain cases, entail the adoption of measures aimed at ensuring that right by protecting it from interference by public authorities as well as by private persons or institutions, including the media.[44]

The protection of personal data forms part of the right to privacy, and this has been reflected in the various instruments of the Inter-American Human Rights System (IAHRS) addressing this issue, including those of the Inter-American Juridical Committee (CJI), the Inter-American Commission on Human Rights, and the Inter-American Court of Human Rights. Furthermore, the UN General Assembly, in its Resolution 68/167 on "The Right to Privacy in the Digital Age" (2014), emphasized that "the same rights that people have offline must also be protected online," including the right to privacy, and expressed concern about "the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights.[45]" The large-scale collection and processing of personal data by technology companies and governments pose serious challenges to the right to privacy.

State use of mass surveillance technologies, driven by advances in artificial intelligence and data processing and by tools that enable the recording and indexing of facial features in databases, poses a significant threat to privacy and to the broader exercise of human rights. These practices may have a chilling effect on the exercise of other fundamental rights, such as freedom of expression and association, and pose a challenge in the context of security and national defense measures, where States often justify surveillance as necessary for the protection of public order and public safety.

The evolution of technology, innovation, and digitalization, on the other hand, has given rise to new activities and business models that increasingly depend on the processing of large volumes of personal data in new and complex ways. As noted in a recent report by the UN Special Rapporteur on the right to privacy, "certain technological developments may pose new challenges for the implementation of data protection and privacy laws and can cause significant negative effects, such as discriminatory and biased outcomes for individuals, or affect their ability to exercise their data protection and privacy rights.[46]" The large-scale datafication of everyday life through digital platforms has created an ecosystem in which every interaction

---

[43] United Nations Human Rights Council (2017), Resolution 34/7. Retrieved from: https://ap.ohchr.org/documents/s/HRC/resolutions/A_HRC_RES_7_34.pdf

[44] Inter-American Court of Human Rights (2011). *Case Fontevecchia y D'Amico vs. Argentina*. (Series C No. 238. Para. 49.) [Original in Spanish.] Retrieved from: https://www.corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf

[45] United Nations General Assembly (2013) *Resolución 68/167, "El derecho a la privacidad en la era digita*l"[The right to privacy in the digital age]. Retrieved from: https://documents.un.org/doc/undoc/gen/n13/449/50/pdf/n1344950.pdf

[46] United Nations Human Rights Council (2023), *Informe de la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères, Mecanismos legales de salvaguarda para la protección de datos personales y la privacidad en la era digital, [Report of the Special Rapporteur on the right to privacy, Ana Brian Nougrères, Legal safeguards for personal data protection and privacy in the digital age] A/HRC/55/46*, para. 9, Retrieved from: https://docs.un.org/en/A/HRC/55/46

generates data that can be collected, analyzed, systematized, and monetized.[47] The scale and depth of data collection raise fundamental questions about informed consent and the control that individuals have over their personal information.

Beyond more traditional concerns—such as mass or targeted surveillance, whether public or private—data-driven systems introduce additional complexities. By generating new forms of interaction, these systems can themselves shape, affect, or even promote the exercise of human rights. This is the case with big data analytics, artificial intelligence, and machine learning systems. Access to large volumes of data is, ultimately, what enables the development of these technologies, which are unevenly distributed across the world.[48] Within this framework, certain paradoxes begin to emerge: the less stringent personal data protection laws are, the greater the capacity for innovation and development of AI technologies, but the weaker the protections against potential violations of the right to privacy. Conversely, the stricter data protection laws become, the more costly it is to develop such technologies, generating inequalities in access, fewer incentives to overcome potential gaps in the data used to train these systems, which in turn leads to discrimination, stigmatization, overgeneralization, and exclusion.

On the other hand, these systems make it possible to infer sensitive information from seemingly innocuous data. Principle 3 of the Inter-American Principles on Neuroscience, Neurotechnologies and Human Rights, adopted by the Inter-American Juridical Committee (IJC) highlights neural data as highly sensitive personal data. Principle 4 clearly identifies the need to frame the processing of neural data within the framework of informed consent as developed in data protection theory. Depending on their uses and applications, these technologies can reveal, predict, infer, or even, based on the information processed, influence a person's sexual orientation, political opinions, health status, or future behavior without their knowledge or explicit consent.

The recognition and expansion of what may be considered highly sensitive personal data in the digital age is particularly important, especially in light of the need—evident in many countries of the region—to adopt or update existing data protection laws. As Hinestroza-Arenas aptly argues in her essay, there may be new issues to address in the development of rights under emerging technologies, but it is essential to build upon the existing normative framework. Otherwise, the continued effectiveness of already recognized rights is at risk, and debates regarding their scope and definition are reopened.

While it is true that all interactions on the Internet and with new technologies generate and rely on data, the mere protection and regulation of personal data use does not exhaust the necessary human rights analyses required to achieve technological development that respects human rights. The logic of data protection is, to a greater or lesser extent, a private-law logic, approaching personal data from the perspective of will, property, and consent. This logic is limited in addressing issues of public interest and may even be insufficient to ensure an adequate and proportionate balance in the exercise of rights. As Botero and De Brieger argue, the datafication of legal discourse may distort the more complex issues arising from technological development and its diverse uses by both the public and private sectors.

With regard to biometrics, for example, the authors argue that "This conception of the face as data, and, by extension, of biometric data as identical to other sensitive data, not only dehumanizes what is arguably our most distinctive identifying feature—by turning it into a tradable asset and dissociating it from the individual to whom that face belongs—but also confines the question of the limits that should be imposed

[47] Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.
[48] United Nations High-level Advisory Body on Artificial Intelligence (2024), *Gobernanza de la Inteligencia Artificial en beneficio de la Humanidad: Informe final* [Governing AI for Humanity: Final Report]. Retrieved from: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.

on this technology to the domain of personal data protection. In this case, as in many others where the social implications of datafication are particularly pressing, a legalistic approach is insufficient to understand the phenomenon and to effectively protect us from its negative consequences, since legal categories are incapable of capturing reality in all its nuances and implications."[49] The integration of biometric technologies into identification and authentication systems poses new risks for privacy. The collection and storage of biometric data, which are unique and immutable, increases the risk of identity theft and misuse of personal information. The Inter-American Juridical Committee has expressed concern about these risks.[50] For example, the deployment of cameras equipped with real-time facial recognition technology enables the tracking and tagging of individuals, thereby granting authorities the capacity to maintain detailed records of the movements of large numbers of people, potentially categorizing them according to various characteristics.[51]

State responsibility for the rights to privacy and data protection in the digital age entails not only refraining from violating these rights, but also adopting positive measures to ensure their effective enjoyment. This implies not only the establishment of appropriate legal frameworks, but also the implementation of policies and practices that safeguard privacy.[52]

Within the Inter-American system, specific standards have been developed to protect individuals from direct interference by the State in the exercise of the right to privacy. These include the requirement that any interference be prescribed by law and be necessary and proportionate. Mass surveillance is generally considered disproportionate, and although it may be justified in certain circumstances, such measures must comply with standards of proportionality, be subject to ongoing review to determine their continued necessity, and not disproportionately affect other rights, including the right to anonymity, freedom of association and assembly, and freedom of expression.

Measures adopted for the individual surveillance of a person must be subject to judicial oversight, ensuring due process, the guarantees of a natural, independent, and impartial judge, and the right to an effective remedy. The right of defense includes the right to be notified of measures affecting one's person and privacy, subject only to narrowly construed exceptions that meet the tests of necessity and proportionality. These standards make it possible, at least in principle, to establish minimum safeguards even for emerging technologies when they are used by the State. Moreover, with regard to the duty to guarantee, they also outline basic criteria that regulations must follow, including obligations of communication and transparency, the protection of personal data, and rights of access, rectification, erasure, and objection, where applicable. In addition, they allow for the inference of certain obligations and powers of the State vis-à-vis the private sector. On the one hand, States must allow users to be informed when their data are requested by public authorities, and may require private sector companies to expressly notify in which cases

[49] Botero, C and De Brigard, J, (2023). "Sonría, Ud está siendo filmado", Annex 3. [Original in Spanish].

[50] Organization of American States (OAS), Inter-American Juridical Committee (2021), *Principios actualizados sobre la privacidad y la protección de datos personales* [Updated Principles on Privacy and Personal Data Protection] (CJI/RES. 266, 2021), Retrieved from: https://www.oas.org/es/sla/cji/docs/CJI-RES_266_ESP.pdf

[51] United Nations Human Rights Council. (2019). Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión [Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression] (A/HRC/41/35, para. 12), Retrieved from: https://digitallibrary.un.org/record/3814512?ln=en

[52] Inter-American Juridical Committee (2023), *Declaración de Principios Interamericanos en Materia de Neurociencias, Neurotecnologías y Derechos Humanos* [Inter-American Declaration of Principles on Neuroscience, Neurotechnologies and Human Rights] (CJI/RES. 281 (CII-O/23) corr.1, March 9, 2023). Retrieved from: https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf.

data are being collected, how they are processed, for what purposes, and to report any security incidents affecting databases that may compromise their security or privacy.

iii. Equality and Non-Discrimination

Equality and non-discrimination are fundamental principles of international human rights law. Articles 1.1 and 24 of the American Convention on Human Rights establish the rights to equality and non-discrimination. Article 1.1 provides for the obligation to respect and ensure the exercise of human rights "without discrimination of any kind on grounds of race, colour, sex, language, religion, political or other opinion, national or social origin, economic status, birth, or any other social condition."[53] Article 24 establishes that "All persons are equal before the law. Consequently, they are entitled, without discrimination, to equal protection of the law."[54] The Inter-American Court of Human Rights has further held that each of the rights enshrined in the Convention must be respected and guaranteed without any discrimination.[55] The obligation to respect requires that the State refrain from discriminating, whether directly or indirectly; and the obligation to guarantee requires that it adopt measures to protect persons under its jurisdiction from arbitrary discrimination.[56] Moreover, this obligation entails the proactive adoption of measures to remedy preexisting situations of discrimination.[57]

In this regard, the adoption of artificial intelligence systems in areas such as education, employment, and public services may exacerbate existing structural inequalities and generate new forms of social exclusion. For example, automated decision-making algorithms may indirectly discriminate against individuals on grounds of gender, race, or socioeconomic status, thereby affecting the right to work and the right to education on equal terms. Likewise, the digital divide and the lack of access to emerging technologies limit the effective enjoyment of economic, social, cultural, and environmental rights (ESCER), particularly in rural, Indigenous, or otherwise vulnerable communities. States must adopt proactive measures to ensure that the development and deployment of AI do not perpetuate or amplify historical patterns of discrimination and instead contribute to the progressive realization of economic, social, cultural, and environmental rights.

Furthermore, the Office of the Special Rapporteur for Freedom of Expression (SRFOE) stated in its report Standards for a Free, Open and Inclusive Internet (2016) that "The rights to equality and nondiscrimination inform the guiding principles that must shape public policy on matters concerning the Internet, as well as each one of the human rights discussed in this report. The obligation to guarantee those rights will require, where appropriate, the adoption of specific positive measures in light of the demands of each right."[58]

---

[53] Organization of American States (OAS) (1969) *Convención Americana sobre Derechos Humanos* [American Convention on Human Rights], Article 1.1. Retrieved from: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

[54] Ibid, Article 24.

[55] Inter-American Court of Human Rights, *Case Apitz Barbera y otros ("Corte Primera de lo Contencioso Administrativo") vs. Venezuela*. Judgment of August 5, 2008, Preliminary Objections, Merits, Reparations and Costs, Series C, No. 182., para. 209.

[56] Inter-American Court of Human Rights. *Case Yatama vs. Nicaragua*. Judgment of June 23, 2005, Preliminary Objections, Merits, Reparations and Costs, Series C, No. 127.

[57] Inter-American Commission on Human Rights (IACHR) (2009), *Informe Anual 2008* [Annual Report 2008]. Report of the Office of the Special Rapporteur for Freedom of Expression, Chapter III (Inter-American Legal Framework of the Right to Freedom of Expression), OEA/Ser. L / V / II.134. Doc 5 rev., 1, February 25, 2009), Para. 230, retrieved from: http://www.cidh.oas.org/annualrep/2008sp/indice2008.htm

[58] Office of the Special Rapporteur for Freedom of Expression (SRFOE) (2016), *Estándares para una Internet libre, abierta e incluyente* [Standards for a Free, Open and Inclusive Internet], retrieved from: https://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf.

In the field of technology, both the Office of the Special Rapporteur for Freedom of Expression and other international bodies have long emphasized the need to protect and ensure the rights to equality and non-discrimination in access to technology and in the exercise of human rights through technological means, such as the Internet. The SRFOE has stated that "The obligation of equality and nondiscrimination also entails the State's obligation to guarantee the exercise of individual human rights on the Internet under equal conditions. Articles 1.1 and 24 govern both "online" and "offline," and individuals have the right to exercise their rights to assembly, association, freedom of expression, access to information, freedom of religion, and so on, without discrimination. The Internet is an essential tool for vulnerable communities and communities historically subjected to discrimination to obtain information, assert grievances, make their voices heard, participate actively in public debate, and help shape public policies designed to redress their situation."[59] Furthermore, the Convention on the Rights of Persons with Disabilities (CRPD) provides that "States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, [...] to information and communications, including information and communications technologies"[60] [...] "including the Internet."[61] [And] "To promote the design, development, production and distribution of accessible information and communications technologies and systems at an early stage, so that these technologies and systems become accessible at minimum cost."[62]

While emerging technologies have the potential to promote equality in certain respects, they may also reinforce and amplify existing social biases, thereby perpetuating discrimination.[63] Inequalities in access to the Internet and digital technologies may exacerbate existing disparities in the exercise of human rights online. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has emphasized that States have a positive obligation to promote or facilitate the right to freedom of expression and the means necessary to exercise this right, including the Internet.[64]

Regarding policies on access to the Internet and other technologies, the Inter-American Commission has stated that "The guarantee of nondiscrimination includes the State's obligation to address the specific Internet access needs that some particularly vulnerable groups may have. The Office of the Special Rapporteur further noted that "regulatory mechanisms need to be established – including pricing regimens, universal service requirements and licensing agreements – to foment broad access to the Internet, including for vulnerable sectors of society and the most isolated rural areas. For these purposes, all necessary efforts should be made to provide direct support to facilitate access, for example, as mentioned before, through programs to distribute affordable computers and the creation of community information technology centers and other points of public access."[65] Along the same lines, the report subsequently addresses the need to

[59] Ibid.

[60] Convention on the Rights of Persons with Disabilities (CRPD), Article 9.1, retrieved from: http://www.un.org/esa/socdev/enable/documents/tccconvs.pdf

[61] Convention on the Rights of Persons with Disabilities (CRPD), Article 21, retrieved from: http://www.un.org/esa/socdev/enable/documents/tccconvs.pdf

[62] Convention on the Rights of Persons with Disabilities (CRPD), Article 9, retrieved from: http://www.un.org/esa/socdev/enable/documents/tccconvs.pdf

[63] Geneva International Center for Justice, Digital Rights: The Impact of AI and Emerging Technologies on Human Rights, June 17, 2024.

[64] United Nations (2011), Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, [Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue] A/HRC/17/27, 2017.

[65] Office of the Special Rapporteur for Freedom of Expression (SRFOE) (2016), *Estándares para una Internet libre, abierta e incluyente* [Standards for a Free, Open and Inclusive Internet]. Retrieved from: https://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf.

combat discrimination against women and children, persons with disabilities, and historically excluded or otherwise vulnerable groups, and to adopt concrete measures to prevent it. The Pact for the Future and the Global Digital Compact highlight the need for, and the commitment of, signatory States to work to bridge the digital divide and thereby advance the Sustainable Development Goals.[66] Inequality in access to the Internet—and now in access to[67] and the development of emerging technologies—poses significant challenges to closing this gap and threatens global peace and stability.[68]

On the other hand, the deployment of experimental emerging technologies has demonstrated their potential impact on education, culture, work, and access to human rights and other rights and their enjoyment. "Notwithstanding widespread perceptions of emerging digital technologies as neutral and objective in their operation, race and ethnicity shape access to and enjoyment of human rights in all of the fields in which these technologies are now pervasive."[69] As highlighted by the Inter-American Juridical Committee, neurotechnologies, when applied without the necessary safeguards and limits, pose a risk, particularly for children and adolescents, persons lacking legal capacity, and other vulnerable groups.

Artificial intelligence and machine learning systems may perpetuate or exacerbate existing patterns of discrimination, contributing to phenomena such as hate speech and disinformation. Artificial intelligence applied to biometrics is also shaped by factors that contribute to discrimination and bias. AI relies on available data, which in many cases lack adequate representativeness across different population groups. The increasing use of facial recognition systems and surveillance technologies to monitor and manage specific population groups has raised a number of significant human rights concerns, including the right to privacy, freedom of peaceful assembly and association, freedom of expression, and freedom of movement.[70] The automated or non-automated creation of personal profiles enabled by biometric technologies may, in many cases, disproportionately reinforce racial, gender, or religious biases that affect the exercise and promotion of human rights.[71]

The concrete impacts, however, depend in many cases on how these technologies are used and by whom. Thus, the use of biometrics and AI in public spaces by law enforcement agents, as described by Botero and

---

[66] United Nations General Assembly (2024). El Pacto del Futuro [Pact for the Future], Resolution A/RES/79/1 (22 September 2024), Annex: Pacto Digital para el Futuro [Global Digital Compact], retrieved from https://documents.un.org/doc/undoc/gen/n24/272/25/pdf/n2427225.pdf.

[67] United Nations General Assembly (2024). El Pacto del Futuro [Pact for the Future], Resolution A/RES/79/1 (22 September 2024), Annex: Pacto Digital para el Futuro [Global Digital Compact], retrieved from https://documents.un.org/doc/undoc/gen/n24/272/25/pdf/n2427225.pdf.

[68] United Nations High-level Advisory Body on Artificial Intelligence (2024). Gobernanza de la IA en beneficio de la humanidad [Governing AI for Humanity] p. 9 https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.

[69] United Nations Human Rights Council (2020), Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, La discriminación racial y las tecnologías digitales emergentes: un análisis de los derechos humanos, [Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance: Racial discrimination and emerging digital technologies: a human rights analysis] A/HRC/44/57, para. 5.

[70] United Nations Committee on the Elimination of Racial Discrimination (CERD) (2020), Recomendación General No. 36[General Recommendation No. 36] (2020), para. 35.

[71] The Committee on the Elimination of Racial Discrimination has recognized that specific groups, such as migrants, refugees and asylum seekers, persons of African descent, Indigenous peoples, and national and ethnic minorities, are the most vulnerable to racial profiling. CERD/C/CAN/CO/21-23, paras. 15 and 16 a) - d); and CERD/C/ITA/CO/19-20, paras. 27 and 28

De Brigard, is different than the application of AI to judicial decision-making or to decisions concerning social security benefits. The Committee on the Elimination of Racial Discrimination has noted that "there is a real risk of algorithmic bias when artificial intelligence is used in decision-making in the context of law enforcement. Algorithmic profiling raises serious concerns, and the consequences with regard to the rights of the victims could be very serious.[72]"

The private sector also engages in uses that may raise significant concerns in this area and may affect the rights to freedom of expression, culture, education, and work, among others.[73] The aforementioned report of the United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance states "But technology is never neutral – it reflects the values and interests of those who influence its design and use, and is fundamentally shaped by the same structures of inequality that operate in society" (A/HRC/44/57, para. 7). Technological development is largely driven by a thriving private sector, generally concentrated in developed countries.[74] These developments are sometimes deployed in information and knowledge platforms, such as social media, search engines, or online games, and at other times they are used for other types of applications, including scientific, educational, health, financial, and banking contexts. Often, the private sector even provides services to the state itself. Accordingly, the design of these technologies must also be attentive to relevant human rights standards. It has been observed that "If bias is embedded in design choices, an algorithm can contribute to biased outcomes, even if the data fed into the algorithm are perfectly representative."[75]

For example, a 2019 report by the National Institute of Standards and Technology (NIST) states that the accuracy of facial recognition software tools in identifying individuals of different sexes, ages, and racial backgrounds depends on the algorithm at the core of the system, the application in which it is used, and the data it processes.[76] The report highlights that, although facial recognition algorithms are becoming increasingly accurate and generalizations are not possible, some algorithms exhibited demographic differentials.[77] Examples include higher rates of false positives among Asians, African Americans, Native Americans, and women.[78]

Inter-American standards already suggest that the analysis must be holistic and that the rights to equality and non-discrimination must be assessed in relation to other rights, such as the right of access to justice (Article 25 ACHR), the right to due process (Article 8 ACHR), and the rights to personal integrity and liberty (Articles 5 and 9 ACHR), among others. States must take all appropriate measures to ensure

[72] United Nations Committee on the Elimination of Racial Discrimination (CERD) (2020) Recomendación General No. 36 [eneral Recommendation No. 36] (2020), para. 12.

[73] United Nations, A/HRC/41/35, para. 12.

[74] United Nations High-level Advisory Body on Artificial Intelligence (2024). Gobernanza de la IA en beneficio de la humanidad [Governing AI for Humanity], p. 9 https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.

[75] United Nations, Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, Formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, [Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance] A/HRC/56/68, para. 17

[76] National Institute of Standards and Technology, U.S. Department of Commerce, 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[77] "Demographic differential" refers to the fact that an algorithm's ability to match two images of the same person varies across different demographic groups.

[78] CERD/C/MUS/CO/20-23 and Corr.1, para. 20; and CERD/C/RUS/CO/23-24, paras. 15 b) and 16 c);

transparency regarding the use of algorithmic profiling systems or even neurotechnologies. This includes public disclosure of the use of such systems and meaningful explanations of how they operate, the datasets used, and the measures implemented to address the risks that the implementation of these technologies poses to the exercise of human rights without discrimination.[79]

These standards also require States to adapt their legislation and to ensure its effective implementation to prevent not only discriminatory laws but also the discriminatory impacts of State practices, policies, or regulations. The obligation to ensure human rights enables States to enforce some obligations on the private sector and even to limit the deployment of certain technologies in spaces or for uses that are particularly sensitive to human rights abuses. It also entails ensuring access to justice when any of these rights are violated.

iv. Due Process and Access to Justice

Articles 8 and 25[80] of the American Convention on Human Rights enshrine the right of every person to due process and access to justice. Article 8 establishes a set of guarantees applicable both to judicial proceedings in general and to criminal proceedings in particular, in light of the vulnerability of the accused to the punitive power of the State.[81] This provision affects not only strictly judicial proceedings but also all organs of the State that "exercise functions of a materially jurisdictional nature [...] although Article 8.1 of the Convention refers to the right of every person to be heard by a 'competent judge or tribunal' for the 'determination of his rights', this article is equally applicable to situations in which a public authority, not necessarily judicial, issues decisions that affect the determination of such rights."[82]

State measures restricting rights must be subject to prior judicial authorization in accordance with due process guarantees, and, where this is not possible in exceptional circumstances, to subsequent review by a competent judicial authority.

Due process includes fundamental guarantees such as the right to be heard within a reasonable time by a competent, independent, and impartial judge previously established by law;[83] the right to a defense; the presumption of innocence; the right to be informed and to participate actively in the proceedings; the right to legal counsel or to self-representation; the right to an interpreter; and the right to appeal the judicial decision. Furthermore, it requires that decisions be reasoned, which contributes both to the legitimacy and transparency of State action and to protection against arbitrariness and unlawfulness.[84]

---

[79] United Nations Committee on the Elimination of Racial Discrimination (CERD) (2020). *Recomendación General No. 36*, [General Recommendation No. 36] para. 61.

[80] Organization of the American States (OAS) (1969) *Convención Americana sobre Derechos Humanos* [American Convention on Human Rights]. Articles 8 and 25. Retrieved from: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf.

[81] Medina Quiroga, C. (2005*), La Convención Americana, teoría y jurisprudencia. Vida, integridad personal, libertad personal, debido proceso y recurso judicial*. Retrieved from: https://www.corteidh.or.cr/tablas/23072.pdf

[82] Inter-American Court of Human Rights (2001), *Case Ivcher Bronstein Vs. Perú. judgment of Reparations and Costs*. Series C N. 74 paras. 105 and 106 [Original in Spanish]. Retrieved from: https://www.corteidh.or.cr/docs/casos/articulos/Seriec_74_esp.pdf

[83] Organization of the American States (OAS) (1969) *Convención Americana sobre Derechos Humanos* [American Convention on Human Rights]. Article 8.1. Retrieved from: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

[84] Ibañez Rivas, J.M. (2014), *Artículo 8, Garantías Judiciales, en Convención Americana sobre Derechos Humanos, Comentario*, Ed.Eudeba.

This right intersects with other fundamental rights, such as the right to equality and non-discrimination and the right to privacy. Violations of the latter may directly impact due process guarantees, particularly as proceedings increasingly incorporate emerging technologies, such as biometrics, AI, and neuroscience, from the prevention and investigation stages onward. The concern, however, is not new. In 2016, the Electronic Frontier Foundation (EFF) conducted a study in six Latin American countries analyzing and evaluating State surveillance regimes and related technologies, and their impact on fundamental rights. At that time, particular attention was paid to State access to subscriber data, connection data, metadata, and electronic records, as well as to the requirements that the State must meet in order to obtain such access.[85] In Latin America, most of the jurisdictions studied require prior judicial authorization for the adoption of State surveillance measures, as well as judicial oversight regarding their duration and admissibility. However, a recurring and widespread problem across the region concerned the opacity of State surveillance mechanisms, the lack of adequate safeguards to ensure effective judicial oversight, and the lack of transparency surrounding these measures, particularly in the field of intelligence, but also in criminal investigations.[86]

The proliferation of emerging technologies in judicial and administrative proceedings poses significant challenges for the guarantee of due process, both in investigations and evidence gathering. For example, the use of artificial intelligence in biometrics or in mass surveillance is inherently problematic; similarly, the use of biometrics in public spaces presents significant challenges for the presumption of innocence that must govern State action. Both Aguerre and De Brigard and Botero highlight some of the problems that these uses can generate.

The use of biometrics in public spaces has been the subject of litigation in several cities. This is the case of Buenos Aires, where the Observatorio de Derecho Informático (ODIA) and subsequently the Centro de Estudios Legales y Sociales (CELS) argued that the use of biometric systems in the city infringed the rights to privacy, equality and non-discrimination, and the presumption of innocence. In addition, the system lacked sufficient safeguards to regulate its use in accordance with the law. The City Court of Appeals confirmed in April 2023 the suspension of the use of this system until adequate oversight mechanisms were established and sufficient public disclosure was provided regarding the functioning of the system.[87] Similarly, the use of neurotechnologies in criminal proceedings may undermine the right against self-incrimination.

The use of AI in public administration, especially in allocating social benefits, subsidies, and educational resources, may lead to arbitrary exclusions or systemic errors that undermine the rights to social security and education and hinder efforts to combat poverty. To address this, States must ensure effective mechanisms of transparency, review, and oversight in automated processes that impact economic, social, cultural, and environmental rights (ESCER), guaranteeing access to justice and remedies for potential rights violations.

The adoption of emerging technologies, such as artificial intelligence in various aspects of legal proceedings, may, of course, improve access to justice and help ensure the right to be heard within a reasonable time. This argument, which has been invoked in countries that have adopted or promoted the use of artificial intelligence at different stages of judicial activity, is undoubtedly important. After all, justice delayed is justice denied. However, the use of these technologies must be instrumental and not determinative of outcomes. In the development of public policies and regulatory frameworks for the adoption of emerging

---

[85] Electronic Frontier Foundation (EFF) (2016). *Unlinking Eyes, the state of government surveillance in Latin America*. Retrieved from: https://www.eff.org/deeplinks/2016/10/unblinking-eyes-latinamerica-surveillance.

[86] Ibid.

[87] Centro de Estudios Legales y Sociales (CELS) (2023). *Confirman la inconstitucionalidad del uso del sistema de reconocimiento facial.* Retrieved from: https://www.cels.org.ar/web/2023/04/confirman-la-inconstitucionalidad-del-uso-del-sistema-de-reconocimiento-facial/.

technologies, these fundamental considerations require extensive public debate and transparency to avoid a zero-sum logic in which efficiency and timeliness are opposed to the protection of fundamental rights, or where the logic implies sacrificing one for the others. In all cases, however, in accordance with Inter-American standards on due process and access to justice, the use of technological tools in judicial proceedings must be transparent, subject to adequate oversight, and respectful of the rights of the parties involved. Moreover, in all cases, decisions issued by courts and other bodies responsible for determining rights must be sufficiently reasoned and subject to appeal.

Conclusion

The development of emerging technologies offers significant opportunities for progress in areas such as science, knowledge, culture, work, and other fundamental aspects of everyday life. Access to these technologies is essential for achieving the United Nations Sustainable Development Goals (SDGs). Given their transformative potential, these technologies require attention from all sectors. In this context, a wide range of documents, guidelines, declarations, and principles have proliferated, seeking to regulate their development at the local, comparative, and international levels. Nevertheless, they also bring challenges. In some cases, they amplify or perpetuate preexisting problems; in others, they generate new challenges stemming from the very expansion of technological frontiers.

Scientific and technological progress is necessarily accompanied by ethical, political, social, and economic considerations, as well as by legal regulation. One common feature of many of the documents currently circulating on technological development is the convergence of considerations of different natures. While all of them are necessary, they often belong to different spheres of society, and it is for different institutions—public, private, and mixed—to establish clear rules for their development, deployment, and oversight. Dialogue among these actors is essential to ensure a coherent regulatory framework. Universal and regional human rights systems emphasize that any limitation on these rights must comply with the principles of legality, necessity, and proportionality. These same principles require States to establish clear rules regarding measures that have an impact on human rights, whether in terms of access to technologies or the development and exercise of human rights through specific technologies.

The proliferation of regulatory instruments at the global level brings with it some degree of certainty, but also significant interpretive challenges. For example, the United Nations Advisory Body on Artificial Intelligence concluded in its final report that:

"There is, today, a global governance deficit with respect to AI. Despite much discussion of ethics and principles, the patchwork of norms and institutions is still nascent and full of gaps. Accountability is often notable for its absence, including for deploying non-explainable AI systems that impact others. Compliance often rests on voluntarism; practice belies rhetoric."

The final report of this group of experts was not without criticism, including concerns about the vagueness of some of its recommendations, the ambitious scope of its proposals, and its holistic approach to a specific type of technology, namely, artificial intelligence. As in many other areas, the report makes certain references to the exceptional nature of the risks generated by these technologies, as well as a certain lack of granularity regarding the specific governance needs of these technologies depending on their uses, actors, and beneficiaries. However, in line with many other reports, it does emphasize the need to develop governance standards grounded in the existing human rights framework.

This article focuses on the potential of the Inter-American legal framework to address the most significant challenges that emerging technologies pose to recognized human rights. A primary conclusion of the analysis is that the tools proposed by the Inter-American Human Rights System (IAHRS) are legal in nature, at least for all States that recognize international human rights law as an integral part of their domestic legal systems. This is the case for most Latin American countries, which have incorporated the provisions of the main international human rights treaties into their statutory and/or constitutional frameworks. A second, perhaps obvious, conclusion is that the obligations generated within human rights frameworks impact the State first and foremost, and the private sector indirectly or secondarily. It is States that are called upon to act as guarantors of human rights in accordance with Articles 1 and 2 of the American Convention on Human Rights. This is without prejudice to the recognition by some States of the transversal and horizontal nature of international human rights law, making it enforceable even in the private sphere. Ultimately, this depends on each jurisdiction and on the existence of legal systems and institutions that recognize and enforce such obligations.

The binding nature of international human rights law with respect to businesses remains a matter of scholarly debate. The United Nations Guiding Principles on Business and Human Rights, adopted in 2011, are a key example in this regard. Likewise, recent regulatory developments, such as the European Digital Services Act (DSA), have sought to incorporate certain corporate obligations related to human rights into their legal frameworks.

A second conclusion that this essay allows is that regulatory regimes differ depending on who develops, deploys, and uses the technology. They may also vary according to the purposes for which the technology is used. Thus, neurotechnologies aimed at developing communication tools for persons with neurological impairments are subject to different legal rules than the deployment of neurotechnologies for prison rehabilitation or public education. The applicable obligations differ, the actors involved are different, the relationships created are distinct, and they are governed by different branches of law, involving different impacts on human rights as well. Similarly, the use of biometrics to control or monitor public demonstrations is not equivalent to biometrics implemented by a local sports club to verify membership.

The Inter-American Human Rights System establishes clear limits regarding the uses and processes through which States may employ emerging technologies in the exercise of their public functions. Guarantees such as due process, impartial judges, and reasoned decisions, stemming from the right of access to justice enshrined in Article 25, undoubtedly impose limits and provide guidance for States that, for example, seek to adopt artificial intelligence technologies in the exercise of judicial functions. Moreover, the IAHRS requires States to ensure access to information, for instance, regarding the acquisition, development, deployment, and use of emerging technologies. This is particularly relevant when such technologies are in an experimental stage and are applied to public uses that impact the exercise of human rights, thereby imposing specific obligations related to necessary judicial oversight for their deployment, notification requirements, and related safeguards.

Finally, without taking a position on the appropriateness or desirability of a risk-based approach to these technologies, such approaches—so common in the ICT sector—must be strictly anchored in a human rights framework that allows the analysis of those risks to be informed by the substantive norms and standards developed in this field to date.[88] The asymmetry in available information, particularly regarding the impacts of technology on society, has been a catalyst for approaches that are more risk-driven than rights-based. Many of the documents and principles that aim to regulate technological development do so from the perspective of each new technology and from a risk perspective. This includes technical risks,

[88] Del Campo,A., Zara N., and Alvarez Ugarte R., *Are Risks the New Rights: the perils of the risks approach in tech regulation, (forthcoming)* Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5161173.

which in some cases may affect the ethics or legality of certain practices, but are ultimately governed by different protocols and principles. In developing these types of approaches, the standards of legality, proportionality, and necessity constitute clear and necessary limits on legislative, regulatory, and judicial discretion, especially with regard to guiding the practices and conduct of the private sector in relation to user rights.

General approaches grounded in ethical or moral perspectives may foster a sense of legal dilution and the perception of an absence of rights where, in fact, there are clear minimum standards and safeguards, particularly for the State. Even in documents that explicitly refer to human rights as a framework—which is not always the case—vagueness and a lack of granularity regarding existing concrete and specific obligations undermine the effectiveness of the regime as a guiding framework for both State and private conduct in this process of technological change and development.

Strengthening the Inter-American legal framework in the field of emerging technologies requires a comprehensive approach that incorporates economic, social, cultural, and environmental rights (ESCER) as a cross-cutting element of technological governance. The protection and promotion of these rights must be a priority in the regulation and oversight of artificial intelligence, ensuring that technological innovation does not result in new forms of exclusion or violations of fundamental rights. It is recommended that States conduct human rights impact assessments, with particular emphasis on ESCER, prior to implementing AI systems in public services and social policies.

The Inter-American Human Rights System (IAHRS) has been a fundamental framework at the regional level. States in the region are receptive to international human rights law, and particularly to the Inter-American system. Unlike Europe, where a regional political and economic body exists, Latin America lacks a comparable institutional structure. As a result, its common legal framework is largely confined to the Inter-American human rights system, which allows for a degree of harmonization of principles and standards and has proven effective in addressing some of the challenges posed by technological development. One of the greatest challenges to maintaining the continued relevance of this framework lies in the reaffirmation and development of clear standards as these challenges evolve, supported by updated and detailed jurisprudence. Ultimately, the law is shaped by the interpretation given to it by the various actors within a political system, but above all by its courts. The role of the Inter-American Commission in the development and systematization of standards has been fundamental, and it should be further promoted so that these standards are incorporated as binding legal standards both in the jurisprudence of the Inter-American Court and in that of domestic courts, which together form part of the IAHRS and contribute to its interpretation.