Uruguay Presidencia | agesic

Report under Article 74 of Law No. 20.212

Recommendations for regulating Artificial Intelligence (AI) to promote ethical development, protect human rights, and foster technological innovation

Authors: Legal Secretariat and Information Society Divisions

Version 1 Year: 2024

Contents

Foreword 7

Background 9

- Objectives 9
- Structure of the report 10
- Guidelines for preparing this report 11
- The ethical development of AI, the protection of human rights, and the democratic system 11
  - The ethical development of AI 11
  - Protecting human rights and democracy in the context of AI development 15
  - Fostering technological innovation and pursuing AI sovereignty 18
- Underlying premises of this report 22
- International AI instruments and lessons learned 23
- Basic definitions for the report 27
- Entities that contributed to the preparation of the report 34

Thematic areas considered 35

- General aspects 35
- Institutional framework and governance area 35
  - Preliminary considerations 35
  - Selected international precedents 37
  - Assessment of the institutional framework and governance of AI 40
- Human rights area 43
  - Preliminary considerations 43
  - Selected international precedents 44
  - Assessment of AI and human rights 50
- Intellectual property area 56
  - Preliminary considerations 56
  - Selected international precedents 58
  - Assessment of AI and intellectual property 59
- Infrastructure and cybersecurity area 63
  - Preliminary considerations 63
  - Selected international precedents 64
  - Assessment of infrastructure and cybersecurity for AI 65
- Work and AI training area 68
  - Preliminary considerations 68

Selected international precedents 69
Assessment of work and training for AI 69
Civil liability and consumer rights area 71
Preliminary considerations 71
Selected international precedents 73
Assessment of civil liability and consumer rights 74
AI support measures area 76
Preliminary considerations 76
Selected international precedents 77
Preliminary assessment of AI support measures 78
Other thematic areas identified from the contributions received 79
The use of AI systems for surveillance 79
International engagement and cooperation 80
Institutional framework and governance area 82
Human rights area 82
Work and training for AI area 83
Intellectual property area 83
Civil liability and consumer rights area 84
Infrastructure and cybersecurity area 84
Support measures area 85
Recommendations 87
Preliminary concepts 87
General recommendations 88
Specific recommendations 93
AI institutional framework and governance 93
The role of Agesic in the AI institutional framework 93
The institutional framework for AI within organizations 95
A multisectoral and multidisciplinary perspective 96
Data governance 97
Ethics, human rights, and democracy 100
The starting point for protecting human rights 100
Special measures aimed at protecting human rights 101
Implementing rights 104
Equality and nondiscrimination 104
Addressing the challenges facing democracies 105

Accessible, appropriate, and effective mechanisms and remedies 106
Regulating the development, use, and procurement of AI in the public sector 107
Training and education for AI 108
Responsible innovation 111
Legal certainty in matters of civil liability and intellectual property 111
Infrastructure and cybersecurity 113
A comprehensive perspective on infrastructure and processes for digital transformation 115
Environmental impacts of infrastructure 116
Support measures 117
Annex 1: National background 121
Mapping national legislation 121
AI institutional framework 121
Data governance 122
Applying AI principles 124
Intellectual property 124
Infrastructure and cybersecurity 127
Work and training for AI 130
Civil liability and consumer rights 131
Support measures 132
Annex 2: International background 135
International principles and recommendations 135
United Nations 136
UNESCO Recommendation on the Ethics of AI (2021) 136
Preliminary principles and recommendations of the High-level Advisory Body on Artificial Intelligence (2023). 142
UN General Assembly Resolution A/RES/78/265 (2024) 145
Other intergovernmental processes 148
OECD Recommendation on Artificial Intelligence (2019) 148
G20 AI Principles (2019) 151
International Guiding Principles for Organizations Developing Advanced AI Systems, Hiroshima Principles (2023) 151
Council of Europe Framework Convention (2024) 154
Processes in Latin America and the Caribbean 159
Digital Agenda for Latin America and the Caribbean, e-LAC (2022) 159

Santiago Declaration (2023) 160
Recent regulations in the United States and the European Union 161
2023 United States Executive Order 161
European Union Artificial Intelligence Act 165
Annex 3: Contributions received during the consultation process 169

Foreword

The rapid expansion of Artificial Intelligence (AI), and its potential uses and impacts, has generated extensive debate about its ethical, social, economic, and political implications, among others. The issue has featured in discussions on the agendas of international and regional organizations and national governments.

In our country, in 2023 Parliament established the first guidelines for an AI policy based on international standards and aimed at ethical development, the protection of human rights, and the promotion of innovation.

Article 74 of Law No. 20.212 of November 6, 2023, also sets a deadline for this Agency to submit recommendations based on those guidelines. This led to a drafting process that sought to take into account different perspectives and opinions from various sectors of society.

This report and its associated recommendations are the result of that process. At this Agency, we hope they will enable a public debate and a collective effort on an issue that undoubtedly has, and will continue to have, significant and lasting impacts on our society.

Hebert Paguas

Executive Director

Background

Objectives

Article 74 of Law No. 20.212 of November 6, 2023, introduced two major innovations concerning the regulation of Artificial Intelligence (AI) in our country:

Regarding the National AI Strategy, it emphasized the leadership of the Agency for the Development of Electronic Government Management and the Information and Knowledge Society (Agesic) in its development and implementation; required the involvement of the Personal Data Regulatory and Control Unit (Urcdp) whenever personal data were involved; linked that strategy to the National Data Strategy; defined its guiding principles; assigned a fundamental role to multistakeholder participation through the possible creation of committees or groups; and established a 180-day deadline for preparing this report.

Regarding the development and implementation of AI systems, it defined the role of Agesic in preparing specific recommendations for public- and private-sector entities, including recommendations for overseeing compliance, all without prejudice to the powers of the Urcdp and other public entities within their respective spheres of action.

This report was prepared using a predefined methodology and through a process involving officials and consultants from various public bodies. Following a number of meetings with them, a consultation document was drawn up and made available to other previously identified stakeholders (private organizations and entities, academia, and civil society), using the citizen participation platform managed by Agesic.

Structure of the report

The report is structured into three chapters and three annexes. The first chapter describes the background to the report, its objectives, underlying premises, the international precedents considered, basic definitions, and the entities that contributed during the first phase of the process.

The second chapter develops the thematic areas considered by this Agency, providing preliminary considerations, selected specific international precedents, and a preliminary assessment for each. That assessment includes opinions not only from the Agency but also from the contributions of other entities. This chapter also includes other thematic areas that emerged during the drafting process.

Finally, the third chapter presents the recommendations prepared by this Agency, divided into general and specific recommendations concerning three central aspects: the AI institutional framework and governance; ethics, human rights, and democracy; and responsible innovation.

Three annexes were also added to the report: the first briefly maps the most relevant legislation applicable to the thematic areas considered; the second details international legislation in various fields; and the third contains the contributions received from the institutions that collaborated in the consultation process conducted through the citizen participation platform.

Guidelines for preparing this report

The aforementioned Article 74 establishes that the recommendations produced must be aimed at:

- The ethical development of AI.
- The protection of human rights.
- The promotion of technological innovation.

The following chapters will specify how efforts have been made to reflect these guidelines in the analyses and recommendations formulated.

The ethical development of AI, the protection of human rights, and the democratic system

The ethical development of AI

In the document currently under review, “AI Strategy for Digital Government,”[1] Agesic defines AI as “a term used to describe a field of study and a set of technologies that study and develop systems capable of performing tasks normally attributed to human intelligence.”

Other definitions exist today that incorporate aspects not considered when that Strategy was designed. In fact, the report highlights the importance of considering definitions recognized and updated by the Organization for Economic Co-operation and Development (OECD). Thus, it can be stated at this point that this Agency understands an AI system to be a “machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions,

[1] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial-para-gobierno-digital/estrategia-2 . Last accessed on 09/02/2024.

content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment." This definition will be considered again later.

In analyzing the links between privacy and AI, SOLOVE[2] argues that the latter is an "old" technology, no different from those that began to generate privacy concerns in the second half of the twentieth century. The difference, however, is that today more data are processed, computing power is greater, and analytical mechanisms are better.

The document "The governance of artificial intelligence: interim report"[3] by the Science, Innovation and Technology Committee of the House of Commons of the British Parliament clearly states that AI has been a field of interest since the 1950s. However, it was only with the expansion of Large Language Models (LLMs)[4] that AI became a general-purpose technology accessible to everyone.

The Committee identifies 12 challenges for those developing AI frameworks and policies: bias, privacy, misrepresentation, access to data, access to computing power, "black boxes," open source, intellectual property and copyright, liability, employment, international coordination, and finally the existential challenge—the latter associated with the belief held by some people that AI threatens life worldwide.

[2] SOLOVE, Daniel. "Artificial Intelligence and Privacy". 77 Florida Law Review, GWU Legal Studies Research Paper. Available on SSRN: https://ssrn.com/abstract=4713111 or http://dx.doi.org/10.2139/ssrn.4713111 . Last accessed: 20/06/2024.

[3] https://committees.parliament.uk/work/6986/governance-of-artificial-intelligence-ai/news/197236/ai-offers-significant-opportunities-but-twelve-governance-challenges-must-be-addressed-says-science-innovation-and-technology-committee/ . Last accessed: 20/05/2024.

[4] This year's report by the Communications and Digital Committee of the House of Lords, also part of the British Parliament, entitled "Large language models and generative AI," defined large language models as a subset of foundation models—those that use deep learning techniques and are trained on large datasets—focused on written text. The report is available at: https://publications.parliament.uk/pa/ld5804/ldselect/ldcomm/54/54.pdf . Last accessed 20/05/2024.

The aforementioned report begins with an AI-generated summary. Inspired by this, after all the thematic areas had been considered and the drafting process for this report had been completed, ChatGPT—one of the best-known LLMs—was asked to suggest, in fewer than 150 words, what should be recommended for AI regulation aimed at ethical development, the protection of human rights, and the promotion of innovation.

Its response was: “For AI regulation that promotes ethical development and the protection of human rights, it is essential to establish clear and robust regulatory frameworks. These must include principles of transparency, responsibility, and accountability, ensuring that automated decisions are understandable and justifiable. It is fundamental for AI systems to respect data privacy and security, implementing mechanisms to prevent bias and discrimination. There must also be ongoing oversight and audit mechanisms to ensure compliance with these regulations, along with appropriate penalties for violations.

Regarding the promotion of innovation, regulations must be flexible and adaptable, allowing experimentation and technological development without imposing excessive burdens. It is crucial to encourage collaboration between the public and private sectors, as well as investment in research and development. Policies must foster an inclusive ecosystem in which startups and small businesses have access to resources and opportunities to innovate. In addition, education and training in AI must be priorities to prepare the workforce of the future and ensure that technological progress benefits society as a whole.”

Clearly, one can agree with these statements, but reality reveals further complexities, especially in the Latin American context.

One of the most important challenges, given AI’s potential to affect how people live and function in society, is to develop an approach that incorporates certain indispensable principles, which are now reflected in instruments issued by various national, regional, and international entities.

In particular, various international instruments advocate the ethical development of AI, understood as compliance with certain ethical principles and values associated, among other things, with respect for the human person, risk prevention, and the protection of vulnerable groups.

From a critical perspective, CRAWFORD[5] observes that "(…) when the rapid expansion of AI is seen as unstoppable, it is only possible to improvise legal and technical restrictions on systems after the fact: clean up datasets, strengthen privacy laws, or create ethics committees. But these will always be partial and incomplete responses that take the technology for granted and require everything else to adapt to it. But what happens if we reverse that polarity and begin with a commitment to a more just and sustainable world? How can we intervene to address the interdependent problems of social, economic, and climate injustices? Where does technology serve that vision? Are there places where AI should not be used, where it undermines that justice?"

The author's questions prompt reflection on the underlying motivation for using AI and on collective policies aimed at preserving common goods, developed through discussion with multiple stakeholders.

Regarding the ethical development of AI as a guiding principle for the report, this Agency has given particular consideration to the Recommendation on the Ethics of Artificial Intelligence of the United Nations Educational, Scientific and Cultural Organization (UNESCO), adopted on November 23, 2021, and endorsed by our country on June 8, 2023, [6] which contains principles as well as highly relevant practical tools.

Within its scope of application, the Recommendation specifies that the ethics of AI is approached "as a systematic normative reflection, based on a holistic, comprehensive, multicultural and evolving framework of interdependent values, principles and actions

[5] CRAWFORD, Kate. "Atlas de Inteligencia Artificial. Poder, política y costos planetarios". Fondo de Cultura Económica. First Edition. 2022. P. 342 et seq.

[6] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-recomendacion-etica-inteligencia-artificial-unesco . Last accessed: 25/06/2024.

that can guide societies in dealing responsibly with the known and unknown impacts of AI technologies on human beings, societies and the environment and ecosystems, and offers them a basis to accept or reject AI technologies."

Article 74 of Law No. 20.212 enshrines a set of principles aligned with those arising from the aforementioned Recommendation and other international instruments to be discussed: equity, nondiscrimination, responsibility, accountability, transparency, auditing and safe innovation, respect for human dignity, the democratic system and the republican form of government, and the data protection principles enshrined in Law No. 18.331 of August 11, 2008 (legality, accuracy, purpose, prior informed consent, data security, confidentiality, and responsibility).

On the understanding that AI ethics relates to compliance with these principles, which enable the safe and responsible development of systems based on this technology, this Agency believes that we must focus on their effective application and provide concrete examples.

Protecting human rights and democracy in the context of AI development

The second guideline established by Article 74 is the protection of human rights. This technology, or any other technology past or future, should not undermine a legal system built through the recognition of rights inherent to the human person and the republican form of government, enshrined in national and international instruments currently in force.

From this perspective, and as will be discussed later, this Agency considers it necessary to begin by considering the obligations arising for states under international human rights law: the duty to respect, the duty to protect, and the duty to fulfill, taking all measures within their reach to ensure the realization of rights. In keeping with this approach, it is appropriate to highlight the need not only to safeguard people against possible harmful effects of AI, but also to harness its

potential to promote beneficial effects on their lives and on the development of our societies.

Regional and international instruments reflect a consensus on placing the human person and the defense of their rights at the center of any regulatory development. PEREZ COMENALE[7] notes an emphasis on protecting fundamental rights, with the human being at the center of regulation, and highlights the need to preserve principles concerning personal data protection, the protection of vulnerable sectors, digital inclusion, connectivity, and digital education, all in a manner consistent with international guidelines and recommendations.

In particular, this Agency wishes to emphasize the impacts of AI on the democratic system, following the views of INNERARITY,[8] who seeks to give concrete form to UNESCO's ethics recommendations with this focus. From this perspective, he considers how automatic decision-making systems affect the normative principles of democratic self-government, explicitly stating: "The issue is to what extent and in what way algorithmic institutionalism, characterized by the use of automated decision systems (ADS), is compatible with what we consider to be a political decision-making system."

The author offers various recommendations, including education and awareness; regulation and legislation—in which he assigns a leading role to parliamentary futures committees in carrying out foresight work; public participation and the protection of democracy through instruments that improve the quality of democratic conversation; regulation and legislation on data; transparency, explainability, and contestability; inclusiveness; comprehensive national strategies; a multistakeholder approach; and the development of global frameworks.

7 PEREZ COMENALE, Agustina. "ChatGPT. Retos y oportunidades de la Inteligencia Artificial Generativa. Desafíos de su regulación". Digital book, EPUB. Granero H., et al. 2023. P. 105.

8 INNERARITY, Daniel. "Inteligencia artificial y democracia". Year 2024. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000389736_spa

People's ability to participate freely in democratic life has also been considered when analyzing the impact of AI in other fields, such as neurotechnology. It is true that the synergy between AI and neuroscience has enabled substantial advances that should be promoted responsibly, but it has also increased the risks of manipulating people and their individual autonomy. These reflections form part of the Working Document "Towards a draft text of a recommendation on the ethics of neurotechnology," prepared by the Ad Hoc Expert Group established within UNESCO.[9][10]

Focusing on neurotechnology, AI, and the impact on how people analyze situations and make decisions allows us to see that potential uses will outpace any regulatory effort that is not based on flexible and adaptable instruments.

The European Parliament,[11] for its part, highlights the importance of applying AI tools to improve political engagement and empower people, giving political actors the opportunity to better understand people's demands through various systems and provide personalized responses to them. It also identifies risks, such as disinformation, deepfakes, and other mechanisms that may affect political campaigns and influence public opinion.

The European Parliament therefore proposes a set of tools to counter the negative impacts of AI, including tools for automatically detecting AI-generated content, watermarks,

[9] Document in English available at: https://unesdoc.unesco.org/ark:/48223/pf0000389438 . Last accessed: 18/06/2024.

[10] It should also be noted that UNESCO has made available a first version of the recommendation on the ethics of neurotechnology, which is open for public consultation and is available at: https://unesdoc.unesco.org/ark:/48223/pf0000389768 . Last accessed: 19/06/2024.

[11] European Parliament. "Artificial intelligence, democracy and elections". Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf . Last accessed: 15/6/2024.

tools for checking information on social media, and in particular, legislation aimed at mitigating AI risks.

The Council of Europe (CoE) Framework Convention on Artificial Intelligence[12] states that measures must be adopted to protect people in democratic processes and their access to public debate, and to safeguard them against harmful or malicious external influences (Article 5). Paragraph 43 of the Convention's explanatory report clarifies that AI has the potential to generate new forms of citizen participation and communication between citizens and their representatives, but also the potential to fragment the public sphere and undermine civic participation and trust in democracy.

We share the view expressed in that explanatory report that the integrity of democracy and its processes rests on people's ability to form an opinion and act on it, as well as to influence the decisions made by their representatives. Some recommendations set out in the report are therefore worthy of consideration, such as adopting cybersecurity measures against malicious foreign interference in electoral processes or against the spread of disinformation, while taking care not to affect preexisting fundamental rights such as freedom of expression, association, and assembly.

It is therefore a matter of being able to recognize and assess the impacts of AI on people, their rights, and our system in general, promoting the development and application of tools that facilitate democratic discussion without undue influence on people's behavior, and others that help political actors understand the needs of people and society, and make informed and fair decisions accordingly.

Fostering technological innovation and pursuing AI sovereignty

Finally, the promotion of technological innovation relates precisely to the benefits this technology may have for the economic, but

[12] https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence . Last accessed: 18/06/2024.

also social, development of our populations, particularly at the national and Latin American regional levels.

Technological innovation serves in our country as a basis for adopting various strategies and promoting different incentives included in legal and regulatory provisions currently in force.

Decree No. 216/023 of July 17, 2023, which creates the Uruguay Innovation Hub (UIH) program, refers to innovation as the "(…) activity that, supported by novel knowledge, is capable of incorporating significant changes into products or processes that result in greater economic value."

At this point, the Agency wishes to focus on certain aspects it considers central to this guideline: institutional framework, strategic objectives, instruments or tools, financial support, and infrastructure.

Regarding the institutional framework, the National Research and Innovation Agency should be mentioned first. It was created by Article 256 of Law No. 17.930 of December 19, 2005, and various aspects of its organizational structure were amended by Law No. 18.084 of December 28, 2006, which also created the National Council for Innovation, Science and Technology (CONICyT), comprising various entities linked to science, technology, and innovation.

More recently, the aforementioned Decree No. 216/023 created the Uruguay Innovation Hub (UIH) program, whose many objectives include strengthening the innovation ecosystem.

This institutional framework is complemented by many other public entities focused on developing innovation, such as the Universidad de la República, Universidad Tecnológica del Uruguay, Centro Ceibal, Laboratorio Tecnológico del Uruguay, the National Directorate for Innovation, Science and Technology of the Ministry of Education and Culture, the National Development Agency, the Public Policy Monitoring and Evaluation Agency, and Agesic itself, among others, whose responsibilities in one way or another include promoting innovation within and outside the public sector.

When we speak of strategic objectives, we refer to the intention, preferably expressed through legal rules, to promote certain areas of activity.

For example, Decree No. 216/023, which creates the UIH program, establishes advanced digital technologies (Deep Tech), biotechnology (Bio Tech), and green technologies (Green Tech) as priorities.

This program also serves to channel the funds provided for in Article 461 of Law No. 20.075 of October 20, 2022, with the aim of promoting projects in science, technology, and innovation. Funding for these types of projects is essential and must be part of any discussion of promoting innovation in AI.

Provisions enacted after Law No. 16.906 of January 7, 1998, also incorporated technological innovation aspects into the criteria for granting the benefits that this law provides in the field of investment promotion.

Regarding innovation tools, the controlled testing environments—regulatory sandboxes—introduced through Article 75 of Law No. 20.212, for which implementing regulations are being developed, deserve particular mention. These will constitute a fundamental instrument for the controlled testing and development of products and services before they are put into production.

However, promoting innovation also goes hand in hand with adequate infrastructure, which should aim to ensure that the country has the capacity not only to produce technologies, but also to maintain and develop them further, building the necessary technical and educational capabilities internally.

Related to this, although broader in scope, the concept of AI sovereignty has been developed. BELLI[13] has described it as “(…) the capacity of a given country to understand, develop, and regulate AI systems (…) should be

[13] BELLI, Luca. “Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to build an AI Sovereignty Stack” in “THE QUEST FOR AI SOVEREIGNTY, TRANSPARENCY AND ACCOUNTABILITY. Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition” available at https://www.intgovforum.org/en/filedepot_download/288/26421 . Last accessed on 30/04/2024.

seen as essential for retaining control, use, and self-determination over AI systems."[14]

The author proposes a framework of interconnected elements (called KASE, for "Key AI Sovereignty Enablers") that will enable a country to determine its sovereignty in this field. These concern appropriate personal data and algorithm governance, strong computing capacity, meaningful connectivity, reliable electric power, a digitally educated population, robust cybersecurity, and an appropriate regulatory framework.

For its part, the World Economic Forum[15] considered the application of 6 pillars to achieve this sovereignty: digital infrastructure; workforce development; research, development, and innovation (R&D&I); regulatory and ethical framework; support for the AI industry; and international cooperation.

The AI sovereignty argument must be given particular consideration when promoting regulatory initiatives. In this regard, the Montevideo Declaration on Artificial Intelligence and its Impact in Latin America,[16] signed on March 10, 2023, during the Khipu event, maintains that it is essential to strengthen Latin American countries' sovereignty over strategic and regulatory AI issues, considering advanced training and the development of critical thinking to be crucial.

[14] In the aforementioned original, BELLI states that he defines "AI Sovereignty as the capacity of a given country to understand, develop and regulate AI systems. I argue that AI Sovereignty should be seen as essential to retain control, agency, and self- determination over AI systems".

[15] https://www.weforum.org/agenda/2024/04/sovereign-ai-what-is-ways-states-building/ . Last accessed: 30/04/2024.

[16] https://khipu.ai/ . Last accessed: 20/06/2024.

Underlying premises of this report

The inevitable question, which this Agency does not intend to evade, is: does our country need an Artificial Intelligence law?

This Agency believes that legislation is not the only applicable regulatory instrument and that any potential statutory regulation should focus not on regulating a technology in itself, but on its potential and actual positive and negative impacts on people and society, without limiting innovation and technological development.

It must be recognized that Uruguay has a regulatory foundation covering many aspects of the ethical development of technology, human rights, and the promotion of innovation. We must continue the discussion and build on international provisions and commitments assumed by our country that provide a framework for protection and for promoting innovation and the development of responsible AI. We must consider complementary regulation in areas that significantly affect people's lives and the development of our societies. We will therefore seek to offer proposed guidelines on how to conduct this discussion.

DANESI[17] states that "we need legislation on artificial intelligence, but not just any legislation, because otherwise we risk curbing innovation and leaving our countries outside the path of progress," proposing a series of dialogue, analysis, and assessment processes involving multiple stakeholders and focusing on high-risk AI systems.

Ultimately, in the Agency's view, this is not a dichotomy between regulating and not regulating, but rather a matter of answering the question: what should be regulated? On this basis, the recommendations presented in this report rest on three underlying premises:

1. What we understand as "technological regulation" must not be associated with regulating a technology in itself but with mitigating negative impacts

[17] DANESI, Cecilia. "El Imperio de los Algoritmos". Kindle edition. Pp. 215-216.

or promoting positive impacts on people and/or society. As a corollary of this understanding, it should be affirmed that, in terms of the scope of the concept of “regulation,” it encompasses a range of normative instruments in a broad sense, not limited to laws or regulations, but extending to other “soft” instruments, such as protocols, guidelines, recommendations, codes, etc.

2. Any regulation of the negative impacts of technology in general, and AI in particular, must be human-centered and based on the defense of our society and our democratic system. Limitations should be expressly established by law and be strictly necessary and proportionate to ensure legitimate objectives in a democratic society.

3. Any regulation of positive impacts, in turn, must focus on achieving the objectives we define as strategic at the national level, so that the limited resources available are allocated more efficiently, and on creating and promoting the structural conditions needed to achieve them. The measures adopted may vary in scope, from general to sector-specific, and our level of success will depend on how appropriately they are determined.

International AI instruments and lessons learned

The importance of AI in our society has been recognized in various international instruments, which have also developed concepts that serve the objectives of this report.

In particular, the OECD Council Recommendation on Artificial Intelligence[18] establishes a set of definitions of what should be understood by AI System, AI Lifecycle, AI Knowledge, and AI Actors—to be

[18] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 . Last accessed on 09/02/2024.

discussed in the following chapters—as well as a set of principles applicable to AI.[19]

The organization also made recommendations for the development of national policies and international cooperation, particularly geared toward small and medium-sized enterprises (SMEs), namely:

1. invest in AI research and development (including long-term public investment and the promotion of private investment in research and development focused on responsible AI innovation and on the use of open data that respects data protection, is unbiased, and improves interoperability and the use of standards);

2. foster a digital ecosystem for AI (particularly promoting mechanisms such as data trusts for sharing information legally, ethically, and securely);

3. define and enable a policy framework for the use of AI (thereby enabling the transition from research and development to deployment and operation through mechanisms such as controlled environments, and reviewing and adapting regulatory and policy frameworks and the analytical mechanisms to be applied to promote innovation and competition in trustworthy AI);

4. build capacity and prepare for the transformation of the labor market (working with various stakeholders to prepare society and the world of work by empowering people, developing training programs, improving worker security, and promoting entrepreneurship, among other measures);

5. cooperate internationally for trustworthy AI (cooperation with other countries and stakeholders, work on joint initiatives, use of internationally comparable metrics, and collection of evidence, among other measures).

[19] At the time this report was prepared, Uruguay was in the process of adhering to these principles.

The OECD principles have served as a basis for subsequent developments, such as the eleven guiding principles for advanced AI endorsed by the G7 and known as the Hiroshima Principles,[20] which in turn gave rise to a code of conduct for developers.

For reference only,[21] the Hiroshima AI Process Comprehensive Policy Framework consists of four pillars: 1. analysis of the priority risks, challenges, and opportunities of generative AI; 2. the Hiroshima Process International Guiding Principles for all AI actors in the AI ecosystem; 3. the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems; and 4. project-based cooperation to support the development of responsible AI tools and best practices.

As mentioned, Uruguay recently endorsed[22] UNESCO's Recommendation on the Ethics of AI,[23] a framework adopted by its 193 members and based on 4 fundamental values: 1. human rights and human dignity; 2. living in peaceful, just, and interconnected societies; 3. ensuring diversity and inclusiveness; 4. the flourishing of the environment and ecosystems. This Recommendation promotes a dynamic understanding of AI, defining it as "systems which have the capacity to process data in a way which resembles intelligent behavior."

For the purposes of the commissioned report, two aspects of the Recommendation should be highlighted. First, the identification of 11 significant areas for governments to take relevant action, to move from high-level principles to practical strategies. These areas of action and the strategies proposed by UNESCO help determine the steps to

[20] https://www.mofa.go.jp/files/100573466.pdf . Last accessed on 12/02/2024.

[21] https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process . Last accessed on 11/02/2024.

[22] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-recomendacion-etica-inteligencia-artificial-unesco . Last accessed on 09/02/2024.

[23] https://www.unesco.org/es/artificial-intelligence/recommendation-ethics . Last accessed on 09/02/2024.

follow in structuring a regulatory framework that addresses aspects beyond the institutional dimension that are affected by AI in our societies.

Second, the Recommendation proposes two practical methodologies that support its implementation: the Readiness Assessment Methodology (RAM) and the Ethical Impact Assessment (EIA). RAM, in particular, raises questions about issues such as AI legislation and country-level infrastructure to enable access to AI technologies, and aims to help determine the regulatory and institutional changes needed both to take advantage of these technologies and to provide safeguards when using them.[24]

At the time this report was prepared, Uruguay was being assessed under this methodology, with the support of the Development Bank of Latin America (CAF).[25]

More recently, the adoption of Resolution A/RES/78/265 by the UN General Assembly[26] should be mentioned for its relevance. It urges all States parties and other organizations in the private sector, civil society, among others, to develop and support regulatory and governance approaches and frameworks for the safe and trustworthy use of AI.

There are other initiatives that affect how AI systems will be addressed internationally, which will be discussed in greater detail throughout this report.

[24] https://www.unesco.org/es/articles/la-unesco-ayudara-mas-de-50-paises-elaborar-una-politica-etica-en-materia-de-ia-este-ano . Last accessed on 09/02/2024.

[25] https://www.unesco.org/es/articles/unesco-apoya-proceso-de-revision-de-la-estrategia-de-etica-de-la-inteligencia-artificial-en-uruguay . Last accessed on 09/02/2024.

[26] UN – General Assembly. Resolution adopted by the General Assembly on March 21, 2024. 78/265. “Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development”. A/RES/78/265. Available at: https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=hxXvAKO8RS5xFkIlcb&fe=true . Last accessed:29/4/2024.

Basic definitions for the report

The objective here is to define what is considered an artificial intelligence system for the purposes of the analysis and recommendations set out in this document, as well as to introduce fundamental concepts that help explain the characteristics and operation of these systems.

The beginnings of artificial intelligence development date back to the middle of the last century, but the dizzying pace of technological advances in how these systems are built and function makes answering the question of what artificial intelligence is an ongoing challenge.

In response to the need for a technical definition that reflects what AI systems are today, while ensuring flexibility in the face of constant technological advances, on November 8, 2023, the Organization for Economic Co-operation and Development (OECD) updated the definition of artificial intelligence systems included in the OECD Recommendation on AI adopted in 2019. The revised definition agreed upon in this forum has constituted the technical basis for various international and regional processes.

As indicated, for the purposes of this document, the revised OECD definition will be adopted, as follows: “a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment[27]” (Unofficial translation[28]).

[27] OECD, OECD Recommendation on AI, OECD/LEGAL/0449, 2019, amended in 2023. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 . Last accessed: 16/4/2024.

[28] Original text in English: “An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment”.

As recently analyzed by the Council of Europe's Committee on Artificial Intelligence (CAI), this updated definition seeks to identify the main characteristics that distinguish artificial intelligence systems from simpler software systems that allow operations to be performed automatically based on rules set by natural persons.[29] It has served as the basis for the definitions of AI systems established by the European Union Artificial Intelligence Act[30] and the draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law[31] adopted within the CAI, in which Uruguay participates as an observer.

Evolution of the definition

The OECD Recommendation on AI adopted in 2019 [32] defined artificial intelligence systems "as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI

[29] COE (2024). Draft Explanatory Report, Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law. CM(2024)52-addprov), Para. 24. Available for download at: https://www.coe.int/en/web/artificial-intelligence/cai. Last accessed: 16/4/2024.

[30] Article 3 of the European Union Artificial Intelligence Act establishes the following definition: "'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf . Last accessed: 16/4/2024.

[31] Article 2 of the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law provides the following definition: "For the purposes of this Convention, "artificial intelligence system" is a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment". Available at: https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411 . Last accessed: 16/4/2024.

[32] OECD, C/MIN(2019)3/FINAL available at https://one.oecd.org/document/C/MIN(2019)3/FINAL/en/pdf . Last accessed: 26/4/2024.

systems are designed to operate with varying levels of autonomy" (unofficial translation[33]).

According to the organization, the amendments introduced in 2023 to reflect the current characteristics and operation of artificial intelligence systems aim to:[34]

- Clarify the objectives of an AI system, which may be explicit or implicit.

- Reflect that the input the system receives may be provided by humans or machines.

- Specify that the Recommendation applies to generative AI systems.

- Replace the term "real" with "physical" to refer to environments.

- Reflect the fact that some AI systems may continue to evolve after their design and implementation.

In this regard, the explanatory memorandum indicates that:[35]

- Although the setting and development of an AI system's objectives can always be traced back to a human who initiates the AI system development process, some types of systems may develop implicit sub-objectives and, at times, set objectives for other systems.

- Although human oversight may occur at any stage in the AI system lifecycle, some AI systems may generate outputs

[33] Original text in English: "AI system: An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy"

[34] See Background information at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#backgroundInformation . Last accessed:16/4/2024.

[35] OECD (2024), "Explanatory memorandum on the updated OECD definition of an AI system", OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris. Available at: https://doi.org/10.1787/623da898-en . Last accessed:16/4/2024.

without these being explicitly described in the AI system's objective and without specific instructions from humans.

• Some systems may develop the ability to perform new forms of inference not initially anticipated when they were programmed, that is, to modify their behavior through direct interaction with inputs and data, before or after deployment.

• The reference to "inferring" must be understood as "generating outputs" from inputs. The concept of output(s), in turn, refers to the results generated by an AI system, which vary according to the different capabilities and functions they perform.

In conclusion, the definitions taken from the OECD that will be considered are:

AI system: an AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

AI system lifecycle: the phases of the AI system lifecycle involve: i) "design, data and models," a context-dependent sequence encompassing planning and design, data collection and processing, and model building; ii) "verification and validation"; iii) "deployment"; and iv) "operation and monitoring." These phases often take place iteratively and are not necessarily sequential. The decision to withdraw an AI system from operation may occur at any point during the operation and monitoring phase.

AI knowledge: AI knowledge refers to the skills and resources, such as data, code, algorithms, models, research, know-how, training programs, governance, processes, and best practices, needed to understand and participate in the AI system lifecycle.

AI actors: AI actors are those who play an active role in the AI system lifecycle, including organizations and individuals that deploy or operate AI.

Other fundamental concepts that help explain the characteristics and operation of AI systems are addressed below.

Machine learning

Machine learning (ML) is a field of Artificial Intelligence.

In the words of the United Nations Educational, Scientific and Cultural Organization (UNESCO), it "is a set of techniques that enables machines to learn automatically using patterns and inferences rather than direct instructions from a person. ML techniques often teach machines to achieve an outcome by providing numerous instances of correct outcomes. However, they can also specify a set of patterns and let the machine discover them in the data on its own."[36]

The model is trained on input data that may be labeled (supervised machine learning) or unlabeled (unsupervised machine learning). A third type is known as reinforcement learning, which involves continuous improvement of the model based on feedback.[37]

The effectiveness of machine learning models depends, among other factors, on the volume and quality of the training data.

[36] UNESCO (2023). Global Toolkit on AI and the Rule of Law for the Judiciary. CI/DIT/2023/AIRoL/01. Glossary. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa . Last accessed:16/4/2024.

[37] UNESCO (2021). AI and education: guidance for policy-makers, P.9. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000379376 . Last accessed:16/4/2024.

Artificial neural networks

An artificial neural network (ANN) is inspired by the structure of neural networks in the human brain.

Following UNESCO's description, artificial neural networks "are a type of machine learning technique that allows computers to learn to perform tasks by analyzing training examples."38 An ANN is designed with interconnected processing nodes, usually organized into layers. Each node receives data from nodes in the layer below and sends data to nodes in the layer above.[39]

Deep Learning

UNESCO has defined Deep Learning as an advanced machine learning technique that "allows the machine to recognize complex concepts on its own, such as faces, human bodies, or images of cats, by sifting through millions of images taken from the Internet, without those images having been labeled beforehand by humans. Born from the combination of machine learning algorithms with formal neural networks and the use of big data, Deep Learning revolutionized artificial intelligence."[40]

Generative AI

Generative artificial intelligence is a subset of Deep Learning. Generative AI learns patterns in content so that it can generate new content. The AI output will be based on the massive amounts of data on which the model was

[38] UNESCO (2023). Global Toolkit on AI and the Rule of Law for the Judiciary. CI/DIT/2023/AIRoL/01. Glossary. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa . Last accessed:16/4/2024.
[39] UNESCO (2023). Global Toolkit on AI and the Rule of Law for the Judiciary. CI/DIT/2023/AIRoL/01. Glossary. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa . Last accessed:16/4/2024.
[40] UNESCO. Artificial Intelligence Glossary. Available at: https://www.unesco.org/es/articles/lexico-de-la-inteligencia-artificial-0 . Last accessed:16/4/2024.

trained. The new content can take different forms: text written in natural language, images, audio, and software code.

In UNESCO's words, "Generative AI is an artificial intelligence technology that automatically generates content in response to instructions written in natural-language conversational interfaces (prompts)."[41]

The techniques used in generative AI vary.

For example, UNESCO explains that text-generating AI "uses a type of artificial neural network known as a general-purpose transformer, and a type of general-purpose transformer called a large language model. For this reason, text-generating artificial intelligence systems are often referred to as large language models (or LLMs). The type of large language model used by generative artificial intelligence is known as a generative pretrained transformer, or GPT" (UNESCO, 2023).

Similarly, the October 2023 United States Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence defines generative AI as "the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content" (unofficial translation).[42]

Foundation or general-purpose models

These are models with broad capabilities that can be adapted to different scenarios.

The European Union AI Act defines them as an AI model trained with a large amount of data using self-supervision at

[41] UNESCO (2023). Global Toolkit on AI and the Rule of Law for the Judiciary. CI/DIT/2023/AIRoL/01. Glossary. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa . Last accessed:16/4/2024.

[42] See Article 3, subsection p. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ Last accessed: 22/06/2024.

scale, displaying significant generality and capable of competently performing a wide range of distinct tasks; it can be integrated into various downstream systems or applications.[43]

Entities that contributed to the preparation of the report

In preparing this report, Agesic received contributions from representatives of various implementing units and entities that participated in the working groups associated with the thematic areas discussed below, including: the Office of the President of the Republic (Deputy Secretariat of the Presidency and Secretariat for Human Rights), Ministry of Education and Culture (Copyright Council), Ministry of Economy and Finance (Consumer Protection Unit), Ministry of Industry, Energy and Mining (National Telecommunications Directorate and National Industrial Property Directorate), Ministry of Labor and Social Security (General Inspectorate of Labor and Social Security), Communications Services Regulatory Unit, National Research and Innovation Agency, Uruguay Innovation Hub Program, Personal Data Regulatory and Control Unit, and National Human Rights Institution and Ombudsperson's Office.

Contributions were also received during the consultation process from the Asociación de Escribanos del Uruguay (AEU), Laboratorio de Datos y Sociedad (DATYSOC), DATA Uruguay, Cámara Uruguaya de Tecnologías de la Información (CUTI), and National Human Rights Institution and Ombudsperson's Office (INDDHH).

Although not all the recommendations from those who responded to the consultation were incorporated, it was considered necessary to include the submitted documentation to illustrate the different perspectives put forward. It appears in an Annex to this report.

[43] See Article 3. Point 63. Available at: Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf . Last accessed: 22/06/2024.

Thematic areas considered

General aspects

In preparing the report, and considering the progress and input obtained from the processes of reviewing the National Data Strategy and creating the National AI Strategy, respectively, the following thematic areas were defined:

- Institutional framework and governance
- Human rights
- Work and training
- Intellectual property
- Civil liability and consumer relations
- Infrastructure and cybersecurity
- Support measures

The following pages reproduce the scope of these areas.

Institutional framework and governance area

Preliminary considerations

The objective of this area is to determine the fundamental aspects needed to ensure an adequate institutional framework for AI in our country.

The institutional framework for AI and the institutional framework for data, like AI governance and data governance, are inextricably linked because of AI's dependence on data. In this area, Agesic proposes to address the institutional framework from the perspective of the structure needed to develop, monitor, and audit public policy on AI and data; the competencies required within public organizations; and the rules that already govern how data are managed at the national level.

Regarding the institutional framework for AI, it is important to consider international precedents, but through the lens of local characteristics, since structures that may be effectively applied in other countries or regions

may prove inefficient or simply unsuitable for our country, and vice versa.

One example of differing structures related to data management, and also AI, is the way in which personal data protection has been organized through regulation. In our country, Law No. 18.331 of August 11, 2008, creates a deconcentrated body within Agesic, called the Personal Data Regulatory and Control Unit (Urcdp), with the power to determine its own budget and technical autonomy, while remaining within the hierarchical structure of the Office of the President of the Republic.

Other Latin American countries have self-governing entities—for example, the Agency for Access to Public Information of the Argentine Republic, Brazil's National Data Protection Authority, or Mexico's National Institute for Transparency, Access to Information and Personal Data Protection—or entities under ministries—as in Colombia, where the data protection entity is a delegated office within the Superintendence of Industry and Commerce of the Ministry of Commerce, Industry and Tourism. Some of these entities share powers relating to data protection and access to public information; some have sanctioning powers over all categories of data controllers, while others distinguish between public and private controllers.

These differences do not prevent them from carrying out their activities within their respective national jurisdictions, representing their countries in this field, making recommendations, and imposing the appropriate penalties for violations of the law.

The purpose of this discussion is to clarify that Uruguay's institutional framework for AI must indeed consider the international and national precedents associated with the issue, but, as we reiterate, these must be analyzed in light of local characteristics.

Alongside the institutional framework for AI, it is essential to consider data governance, since it is one of the essential elements for developing AI systems. Data governance includes different types

of data—personal and nonpersonal—their management, the entities that generate and manage those data, reuse, interoperability, and ultimately the standards to be met by both the public and private sectors when using data that feed into or are generated by AI systems.

Selected international precedents

The current text of the Council of Europe (CoE) AI Convention[44] establishes in Article 1 that parties must adopt and maintain legislative, administrative, or other appropriate measures to give effect to the Convention's provisions. These measures must be graduated and differentiated according to the severity and likelihood of adverse impacts on human rights, democracy, and the rule of law. The Convention provides, with certain nuances, for the applicability of its provisions to the public and private spheres.

Regarding innovation, the Convention provides for the possibility of establishing controlled environments for developing and testing artificial intelligence systems under the supervision of competent authorities. It should be recalled that Article 75 of Law No. 20.212 provided for the possibility of creating controlled testing environments or regulatory sandboxes, for which implementing regulations are currently being developed by Agesic with the support of other entities.

Transparency is a central principle within the Convention; ensuring that people actually know they are interacting with an AI system, and providing oversight mechanisms, are integral parts of that transparency.

Regarding the European AI Act,[45] Title VI addresses AI governance, creating in its chapters the European Artificial Intelligence Board (an EU body composed of national supervisory authorities), with powers to assist national authorities, coordinate guidance and analysis, and contribute to effective cooperation.

[44] https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence . Last accessed: 13/06/2024.
[45] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206 . Last accessed: 19/03/2024.

Chapter 2 of Title VI of the Act addresses National Competent Authorities, whose purpose is to ensure its application and enforcement and which must preserve the objectivity and impartiality of their activities and functions. They must have adequate financial and human resources, with in-depth knowledge of AI technologies, data, data computing, risks to fundamental rights, health and safety, and knowledge of applicable legal rules and requirements.

The European AI Regulation, or EU AI Act, is part of a set of data governance regulations that seek—within the European Data Strategy[46]—to create a single market in which data flow freely between different sectors of society. This ecosystem comprises the Digital Services Act, Digital Governance Act, Digital Markets Act, Data Act, e-Privacy Regulation, and GDPR (European General Data Protection Regulation).

In the United States, there is the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[47] It emphasizes 8 principles that Federal Government entities must comply with to achieve the desired objectives and establishes a set of AI-related actions to be taken by different federal government agencies within their respective areas of competence. It does not provide for a single exclusive central authority with AI powers, but rather distributes AI-related issues among the institutions that legally have the relevant competence.

The influence of the People's Republic of China in this field cannot be overlooked. In addition to preexisting cybersecurity and personal data protection rules, it has promoted measures to regulate AI in general and generative AI in particular. These provide for specific measures on transparency in the use of AI systems, safeguards for certain uses, government

46 More information on this strategy is available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en . Last accessed: 21/06/2024.

47 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ . Last accessed 19/3/2024.

approval for listed uses, prevention of discrimination, the exercise of rights by users, and responsibilities enforceable through fines.[48]

The United Kingdom, for its part, published a document setting out a pro-innovation approach to AI regulation,[49] following a public consultation held over a 1-year period. In addition, the United Kingdom created an Office for Artificial Intelligence as part of the Department for Science, Innovation and Technology, and a Responsible Technology Adoption Unit. The latter, in particular, aims to promote responsible innovation in the public and private sectors by developing tools to build trust within organizations in AI and data management systems. Previously, until June 2023, it had an AI Council composed of experts from multiple sectors, whose objective was to contribute to the development of the AI strategy.

The UK government also currently has a Central Digital and Data Office that leads digital, data, and technology functions for government and works particularly on developing AI policy and strategy, including standards for government use.

All these provisions place particular emphasis on how data are used and on the principles that should guide regulation. There is also a tendency to create governance arrangements involving multiple stakeholders, without prejudice to the leadership of a body within the state structure.

[48] A summary of what to expect from Chinese legislation can be found in the Parliamentary Observatory, Asia-Pacific Program of the National Library of Chile, available at https://www.bcn.cl/observatorio/asiapacifico/noticias/andamiaje-institucional-inteligencia-artificial-china . Last accessed: 21/06/2024. An English translation of the legislative proposal can also be found on the website of the “Center for Security and Emerging Technology - Georgetown University’s Walsh School of Foreign Service” https://cset.georgetown.edu/publication/china-ai-law-draft/ . Last accessed: 21/06/202.

[49] https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response . Last accessed 19/3/2024.

There is also a need to place strong emphasis on the responsible innovation component and to ensure the protection of human rights, with the training of the technical staff associated with this regulatory entity being a central element.

Assessment of the institutional framework and governance of AI

Under the rules surveyed, from an institutional standpoint there are two entities tasked with establishing general criteria in this field: Agesic and the Urcdp.

Article 74 of Law No. 20.212 provides for the design and implementation of the Data and Artificial Intelligence Strategy, placing Agesic in charge of its leadership. Within these powers, the Agency is authorized to create working groups and other forums involving different stakeholders who contribute to implementing the strategies.

Under this Article, Agesic recently created the Public Sector Strategic Committee for Artificial Intelligence and Data, composed of representatives of that Agency, the Ministry of Industry, Energy and Mining, the Ministry of Education and Culture, the Ministry of Labor and Social Security, the Ministry of Economy and Finance, the National Statistics Institute, the National Human Rights Institution and Ombudsperson's Office, the National Research and Innovation Agency, and the Personal Data Regulatory and Control Unit.

In addition, the final paragraph of Article 74 establishes a task that goes beyond the strategy and concerns the development of artificial intelligence systems, for which Agesic may establish criteria and define mechanisms to oversee compliance. Specifically, that paragraph states: "AGESIC will make specific recommendations to public- and private-sector entities for the development and implementation of the aforementioned artificial intelligence systems, and for overseeing compliance, without prejudice to the powers of the URCDP and other public entities within their respective spheres of action."

Consistent with this provision, that competence is established without prejudice, first, to the powers of the Urcdp, which may determine criteria for the use of personal data in any processing operation, particularly those established in Article 16 of Law No. 18.331—automated processing that generates, among other things, profiles of individuals—in accordance with Article 34 of that law.

Regarding the institutional framework, this assessment should mention the reflections emerging from the consultation process. The INDDHH, for its part, proposes that, given the powers assigned to Agesic and the Urcdp to establish general criteria and exercise oversight, their sphere of action should be situated outside the Executive Branch, specifically suggesting the legal form of a decentralized service.

In this regard, this Agency believes that, although the proposal is understandable and worthy of consideration, the existing institutional framework would enable adequate AI governance, at least at present. Nevertheless, the full INDDHH proposal is attached as an annex for consideration by the Legislative Branch.

In its contributions, CUTI states that Uruguay's existing institutional framework would be appropriate for addressing the challenges raised, without prejudice to the need for advisory groups with multistakeholder participation and a significant role in defining policies.

For AI governance and the adoption of this technology to be trustworthy and responsible, measures for adequate data governance and management must also be considered. Data are one of the technology's main inputs and its principal output. In turn, for data to be trustworthy and usable, it is important to ensure that they are properly managed by defining and adopting rules, policies, and guidelines. In doing so, national, regional, and international standards in this field should be considered.

Although our country does not have a fully established data governance framework in the public sector, certain advances are contributing to its construction.

Agesic has certain powers in this field, such as rules on information exchange and interoperability, open government, and open data, compiled in Decree No. 184/015 of July 14, 2015. In addition, the Agency's deconcentrated units, the Urcdp and the Access to Public Information Unit (Uaip), have national competence regarding the management of personal information and public information, respectively.

The contributions to the consultation suggested specific mechanisms for data protection (such as analyzing the data trusts proposed by the INDDHH), adopting mechanisms to resolve conflicts between promoting innovation in public service development and the impact of a possible failure in that field (CUTI), and generating standards that allow Uruguayan solutions to be assessed and "exported" (CUTI).

Concerning how AI systems are used, the AEU mentions the importance of considering specific sectors or uses, particularly in the judicial sphere (proposing "white box" systems based on techniques for making predictions, classifications, and intelligent detections), scoring (emphasizing the impermissibility of using data other than those employed for the specified purpose and the need for explainability), and the contractual and notarial fields (where it advises against using synthetic data).

Human rights area

Preliminary considerations

The objective of this area is to identify risks that cannot be overlooked when developing public policy on AI and that may require—if considered necessary —special measures because of their impact on people's rights.

An additional objective is to identify measures to harness AI systems for the benefit of people and their rights, particularly regulatory measures.

To this end, consideration will be given to the norms and associated international obligations of international human rights law ratified by the country, the specific AI recommendations made by international organizations, and regulations in force or under development at the regional and international levels.

The impacts of AI on human rights have been analyzed in various forums. At the High-level Side Event of the 53rd Session of the Human Rights Council,[50] UN High Commissioner for Human Rights Volker Turk noted that human rights are being tested in our world today, and that the question of where AI's limits lie is one of "(…) the most pressing issues for our society, for governments and for the private sector." The High Commissioner identifies two schools of thought on AI regulation: a) one focuses on risks, self-regulation, and self-assessment by developers, placing very substantial responsibility on the private sector; b) the second takes an approach that integrates human rights throughout the AI lifecycle, incorporating human rights principles from "(…) data collection and selection; as well as into the design,

[50] The High Commissioner's speech can be found at: https://www.ohchr.org/es/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner . Last accessed: 20/03/2024.

development, deployment and use of the resulting models, tools and services.”

At this point, the High Commissioner makes several proposals: 1) listen to groups most vulnerable to the use of this technology; 2) pay attention to AI use in public and private services where there is a greater risk of abuse of power or intrusion into privacy; 3) require human rights risk and impact assessments before, during, and after the use of AI systems (transparency, independent oversight, and access to effective remedies); 4) ban or suspend AI technologies that do not comply with international human rights law; 5) apply existing data protection regulation and other sector-specific protective legislation; 6) do not allow an approach based solely on self-regulation; 7) create an international advisory body.

In our country, regarding human rights policy, particular mention should be made of the National Human Rights Plan 2023-2027, which includes the impact of artificial intelligence, among other issues, and the need to advance toward the ideals of the Universal Declaration of Human Rights. This Plan complements the objectives mentioned above by establishing coordination mechanisms, regulatory frameworks, and action protocols that allow a human rights approach to be incorporated into public policies such as the one intended to be institutionalized in the field of AI. It therefore seems relevant to accompany the development of these guidelines so that AI is included in the defined objectives.

Selected international precedents

The aforementioned “Recommendation on the Ethics of Artificial Intelligence” highlights the role of human rights protection in the ethical development of AI systems, based on principles of transparency and equity.

The Recommendation also considers the following instruments: the Universal Declaration of Human Rights (1948), the instruments of the international human rights framework, including the Convention relating to the

Status of Refugees (1951), the Discrimination (Employment and Occupation) Convention (1958), the International Convention on the Elimination of All Forms of Racial Discrimination (1965), the International Covenant on Civil and Political Rights (1966), the International Covenant on Economic, Social and Cultural Rights (1966), the Convention on the Elimination of All Forms of Discrimination against Women (1979), the Convention on the Rights of the Child (1989), the Convention on the Rights of Persons with Disabilities (2006), the Convention against Discrimination in Education (1960), and the Convention on the Protection and Promotion of the Diversity of Cultural Expressions (2005), as well as any other relevant international instruments, recommendations, and declarations. It also notes the Declaration on the Right to Development (1986); the Declaration on the Responsibilities of the Present Generations Towards Future Generations (1997); the Universal Declaration on Bioethics and Human Rights (2005); the United Nations Declaration on the Rights of Indigenous Peoples (2007); the United Nations General Assembly resolution on the review of the World Summit on the Information Society (A/RES/70/125) (2015); the United Nations General Assembly resolution entitled “Transforming our world: the 2030 Agenda for Sustainable Development” (A/RES/70/1) (2015); the Recommendation concerning the Preservation of, and Access to, Documentary Heritage Including in Digital Form (2015); the Declaration of Ethical Principles in relation to Climate Change (2017); the Recommendation on Science and Scientific Researchers (2017); the Internet Universality Indicators (endorsed in 2018 by UNESCO’s International Programme for the Development of Communication), including the ROAM principles (endorsed by UNESCO’s General Conference in 2015); the Human Rights Council resolution on “The right to privacy in the digital age” (A/HRC/RES/42/15) (2019); and the Human Rights Council resolution entitled “New and emerging digital technologies and human rights” (A/HRC/RES/41/11) (2019).

On the basis of this background, UNESCO recommends that member states apply appropriate measures—legislative and otherwise—to give effect to the

principles and norms developed, in accordance with international law and particularly international human rights law.

The Recommendation explicitly states that AI systems should improve human beings' quality of life and that they should not suffer any form of harm at any stage of the systems' lifecycle. It also emphasizes the need for means to promote, defend, and exercise human rights. To this end, it proposes a set of principles: proportionality and do no harm; safety and security; fairness and nondiscrimination; sustainability; right to privacy and data protection; human oversight and determination; transparency and explainability; responsibility and accountability; awareness and literacy; and adaptive multistakeholder governance and collaboration. These principles are associated with concrete measures to be analyzed later, particularly the so-called Ethical Impact Assessment.

The Ethical Impact Assessment proposes that Member States establish "(…) impact assessment frameworks, such as ethical impact assessments, to identify and assess the benefits, concerns and risks of AI systems, as well as appropriate risk prevention, mitigation and monitoring measures, among other assurance mechanisms. Such impact assessments should identify impacts on human rights and fundamental freedoms, particularly, but not exclusively, the rights of marginalized and vulnerable people or people in vulnerable situations, labor rights, the environment and ecosystems, as well as ethical and social implications, and facilitate citizen participation, in accordance with the values and principles set out in this Recommendation."

As mentioned earlier, the recent UN General Assembly resolution[51] promoting safe and trustworthy AI systems that

[51] More information is available at: https://news.un.org/es/story/2024/03/1528511#:~:text=La%20Asamblea%20General%20de%20la%20ONU%20adopt%C3%B

enable achievement of the Sustainable Development Goals (SDGs) contains specific recommendations for measures to be adopted by Member States.

Also within the UN framework, the December 2023 document “Interim Report: Governing AI for Humanity”[52] deserves particular mention. Among other things, it categorizes risks in terms of existing or potential vulnerability for individuals, groups, the economy, (eco)systems, values and norms, and society. This is in addition to considering international human rights norms and commitments under the SDGs as a guiding principle for AI governance.

Continuing with international precedents, European Union legislation approved by member countries on March 13, 2024, establishes several relevant aspects highlighted by the organization itself:[53]

1) Rules for different types of Risks:

    a. Unacceptable risks, prohibited because they pose a threat to people: cognitive behavioral manipulation of vulnerable groups, social “scoring,” biometric identification and categorization of people, and remote and real-time biometric identification systems—in this last case there are exceptions based on law enforcement purposes.

    b. High risks, divided into two categories and requiring an assessment before being put into production: i. systems used in products covered by EU product safety legislation (toys, aviation, cars, medical devices, and elevators); ii. systems in specific

3%20por,que%20beneficien%20tambi%C3%A9n%20al%20desarrollo%20sostenible%20para%20todos . Last accessed: 25/03/2024.

[52] Available at https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf . Last accessed: 02/04/2024.

[53] See: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence . Last accessed: 24/03/2024.

areas that must be registered in an EU database (management and operation of critical infrastructure; vocational training and education; work, worker management, and access to employment; access to and enjoyment of essential private services and public services and benefits; law enforcement; migration, asylum, and border control management; assistance in the legal interpretation and application of the law)

2) Transparency requirements. Some AI systems, such as generative AI, even when not considered high-risk, must comply with transparency requirements and intellectual property rules, namely:

a. Disclose that the content was generated by AI

b. Design the model to prevent it from generating unlawful content

c. Publish summaries of intellectual-property-protected data used for training

High-impact general-purpose AI models that may generate systemic risk must be assessed, and any serious incidents they experience must be reported to the European Commission.

Likewise, content generated and modified with the help of AI must be labeled so that users are aware of that fact.

3) Support for innovation. This involves creating conditions that encourage testing AI models before they are put into production.

In the United Kingdom, the regulatory proposal presented and submitted for public consultation during the past year aimed to achieve a pro-innovation and pro-safety approach.

That proposal distinguishes 3 risk categories: 1) societal risks; 2) misuse risks; 3) autonomy risks. The first category addresses the world of work, innovation and intellectual property, protecting people from bias and discrimination, personal data protection, trust and safety in online content, ensuring competition in digital

markets, and best practices in the public sector. The second risk category mentions safeguarding democracy against interference in electoral processes and preventing misuse of technology. Finally, the last risk category concerns the extent of human control over AI systems.

The distinction between risks is also present in proposals under discussion in South America, such as Bill No. 2338 [54] of the Federative Republic of Brazil, which distinguishes between high-risk and excessive-risk systems, with the possibility of imposing strict measures for their development and implementation. The Chilean government, for its part, submitted a bill[55] to Parliament on May 7, 2024, that also distinguishes unacceptable-risk and high-risk AI systems and adds limited-risk systems.

In October 2023, the United States government issued an Executive Order on the Safe and Trustworthy Development of Artificial Intelligence to be applied by government agencies.[56] Measures provided for in the Executive Order include developing safety standards, protecting Americans' privacy, advancing civil rights and equity, protecting consumers, patients, and students, supporting workers, promoting innovation and competition, advancing United States leadership abroad, and ensuring responsible and effective government use of AI (the annex on international legislation presents the measures in greater detail).

[54] https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1718367327465&disposition=inline . Last accessed: 13/06/2024.

[55] https://www.camara.cl/verDoc.aspx?prmID=17048&prmTIPO=INICIATIVA . Last accessed: 14/06/2024.

[56] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ Last accessed: 24/03/2024.

Assessment of AI and human rights

The assessment in this area focuses on 5 central aspects linked to the points mentioned by the UN High Commissioner for Human Rights and detailed above.

1. Is it necessary to strengthen the application of preexisting human rights norms and principles through regulatory instruments that explicitly state and specify their application across the field of AI and/or as pillars of national policy, beyond the provision established in Art. 74 for the National AI Strategy?

2. Can self-regulation constitute an effective remedy for guiding the actions of public and private entities in AI development?

3. Is a risk-based approach sufficient? And, as a corollary, are there AI systems that, because of their impact on people's rights, should be prohibited or restricted, or require the imposition of special measures?

4. What transparency and explainability safeguards should be established in the development of human-centered AI systems?

5. What guiding criteria should be used to define a public policy associated with AI development in our country that also enhances the positive impact on human rights?

Regarding the scope of application of the principles, under Article 74 of Law No. 20.212 they currently apply to the design and development of the National Artificial Intelligence and Data Strategy. However, without prejudice to the fact that the norms of international human rights law ratified by the country and the resulting international obligations are fully applicable, since these principles were established in relation to the development of those Strategies, consideration should be given to whether it is appropriate to expressly establish them in law with a broader

scope. That is, to specify their normative content expressly in relation to AI policy.

As mentioned, the principles included in Article 74 are aligned with those enshrined in the first International Convention on this subject developed by the CoE. This Convention highlights the principles of human dignity and individual autonomy, transparency and oversight, responsibility and accountability, equality and nondiscrimination, privacy and personal data protection, reliability and security, and safe innovation. Under the Convention's own definition, these principles apply to all AI systems throughout their lifecycle.

Regarding the risk-based approach, this perspective is already present in personal data protection regulation, which may also apply to AI systems when they use or generate this type of data.

Thus, Article 12 of Law No. 18.331, as amended by Article 39 of Law No. 19.670 of October 15, 2018, provides for personal data protection impact assessments. Article 6 of Decree No. 64/020 of February 17, 2020, provides for these assessments for personal data processing that generates greater risks for individuals, and Article 7 specifies the instrument's minimum content, emphasizing risk assessment and the security measures to be adopted.

For example, Article 6, subsection c, of that decree makes impact assessments mandatory for processing involving "(…) an evaluation of personal aspects of data subjects in order to create or use personal profiles, particularly by analyzing or predicting aspects relating to their performance at work, economic situation, health, personal preferences or interests, behavioral reliability and financial solvency, and location." Subsection d adds that these assessments are mandatory for "(…) processing large volumes of personal data."

The link with AI is undeniable, and the application of these provisions to AI systems that profile individuals or use large volumes of

data for training is indisputable in both the public and private spheres. It is true that there are certain circumstances in which the scope of this law may not cover some situations, as civil society notes in its response to the consultation and as will be discussed later.

There are many examples of self-regulation. In the field of data in particular, personal data protection rules can serve to illustrate how these mechanisms work (see, for example, the codes of conduct provided for in Article 36 of Law No. 18.331).

Adopting co-regulatory arrangements that establish certain red lines and oversight mechanisms through regulation appears to be a more suitable path. These definitions can be seen in the work of MANTELERO,[57] who proposes considering governments' different spheres of action and the scope of regulation, comparing the Council of Europe and European Commission proposals, and noting that, in addition to the co-regulatory approach, the proposals put forward by these organizations lean toward a risk-based rather than a principles-based approach.

The possible imposition of special measures is also linked to analyzing impacts on people's rights, together with other measures for more effective oversight of system operation. Creating algorithm registers, requiring special prior authorization, or even making testing in controlled environments mandatory may be useful instruments for certain types of systems and particular types of risk.

Regarding the principle of transparency and explainability, the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG), in its "Ethics Guidelines for Trustworthy AI,"[58] states that explainability—a central element of transparency alongside traceability and communication—is the

[57] MANTELERO, Alessandro. "Beyond Data – Human Rights, Ethical and Social Impact Assessment in AI" in "IT&LAW 36". Available at: https://link.springer.com/chapter/10.1007/978-94-6265-531-7_4 . Last accessed: 25/03/2024.

[58] https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai . Last accessed: 14/06/2024.

ability to explain both an AI system's technical processes and the associated human decisions. In our legal system, explainability is expressly enshrined in two provisions of Law No. 18.331: Articles 13 and 16.

Article 13 of that law provides for the Right to Information, and subsection G establishes that the obligation of controllers and processors to provide information to data subjects includes, in the case of "(…) automated data processing regulated by Article 16 of this law, the assessment criteria, the processes applied, and the technological solution or program used."

Article 16, in turn, enshrines the right to challenge personal assessments, stating that: "Individuals have the right not to be subject to a decision with legal effects that significantly affects them and is based on automated data processing intended to evaluate certain aspects of their personality, such as work performance, credit, reliability, and conduct, among others.

The affected person may challenge administrative acts or private decisions involving an assessment of their behavior whose sole basis is personal data processing that offers a definition of their characteristics or personality.

In this case, the affected person will have the right to obtain information from the database controller on both the assessment criteria and the program used in the processing that led to the decision expressed in the act."

Without prejudice to the above, it is necessary to give effective consideration to broader solutions for AI systems that do not process personal data, or for recipients who should be aware of their interaction with those systems even when their own data are not used by them.

Regarding the use of AI systems in the Public Administration, mention should be made of Law No. 18.381 of October 17, 2008, whose purpose is to

promote transparency in the administrative functions of all public bodies, whether state or nonstate, and guarantee individuals' fundamental right of access to public information (Article 1). Its implementing Decree No. 232/010 of August 2, 2010, establishes the principle of maximum disclosure in Article 6, so that obligated entities provide information as broadly as possible. Article 38 includes, among the information that entities subject to the law must disclose on their websites, "any other information that may be useful or relevant to understanding and assessing the functions and public policies for which the obligated entity is responsible."

Thus, the obligation to make transparent, but above all to explain, the decisions adopted by public entities when they use AI systems is grounded not in one but in two foundational laws of the digital environment.

Possible guiding criteria for public policy in this field could be associated with compliance with principles and the provision of practical tools that enable innovative development, verification of compliance with human rights norms, and oversight mechanisms.

In this regard, the law has granted competence to make recommendations on this subject to the National Human Rights Institution and Ombudsperson's Office through Article 4 of Law No. 18.446 of December 24, 2008, and to the Secretariat for Human Rights under Article 67 of Law No. 19.149 of October 24, 2013; and, regarding personal data, to the Personal Data Regulatory and Control Unit under Article 34 of Law No. 18.331 of August 11, 2008.

We can state that most of the concerns received from the entities participating in the consultation focused on this thematic area. For example, CUTI states that, although the current legal and institutional framework would be adequate to manage the potential risks arising from AI use—also taking into account the updates to the personal data protection law—a specific committee or group would be needed to assess the impact on human

rights, along with a cautious approach to risk classification so as not to affect innovation and investment in AI.

The assessment by civil society institutions concerning the adequacy of the rules indicates that the provisions of the personal data protection law are insufficient because, among other things, they are directed exclusively at personal data processing. Provisions should therefore be included that specify the concept of “meaningful human oversight,” enable the exercise of collective rights, require the publication of impact assessments, set requirements for algorithmic explainability, traceability, and auditability, guarantee human and in-person interaction with the public administration, and address the relationships between copyright, trade secrecy, and the auditability of AI systems (DATYSOC proposals).

DATA highlights the importance of the right provided for in Article 16 of the personal data protection law, but clarifies that these standards need to be applied to the public administration through amendments to Law No. 18.381. It also emphasizes discussion of high-risk systems and the establishment of basic safeguards, and the need to support the INDDHH’s work.

The AEU raises, in this area, the question of whether general or sector-specific regulation is necessary and considers a risk-based approach appropriate, also taking into account the assignment and distribution of liability for harm. All this should be human-centered, require companies to state explicitly where and how they use AI, and also consider the duty to prevent discrimination and ensure that discriminatory attitudes are not reflected, and to avoid risks. It also proposes establishing human rights impact assessments for AI developments and strengthening the role of informed consent and the purpose limitation principle provided for in Law No. 18.331.

The responses received from civil society to the consultations indicate the need to focus on analyzing AI use in surveillance by security forces, which will be considered in another chapter.

Intellectual property area

Preliminary considerations

The World Intellectual Property Organization (WIPO)[59] notes that Intellectual Property refers to creations of the mind, from works of art to inventions, computer programs, trademarks, and other commercial signs. It is divided into two categories: industrial property (invention patents, trademarks, industrial designs, and geographical indications) and copyright and related rights (literary, artistic, and scientific works, including performances and broadcasts). Trade secrets will be included as part of the discussion.

The connections between Intellectual Property and innovation are undeniable,[60] as are the impacts of Artificial Intelligence on it.[61] The National Artificial Intelligence Plan of the Argentine Republic,[62] for example, has indicated that intellectual property, along with personal data protection and consumer rights, are regulations in tension for which a regulatory balance should be sought, because of their importance to AI development and application.

In this regard, WIPO[63] recently published a document that seeks to reflect on these aspects and proposes that the starting point should come from:

1) Understanding whether national laws allow an AI system to be named as an inventor or whether human intervention is necessary;

[59] "What is Intellectual Property?" available at: https://www.wipo.int/publications/es/details.jsp?id=4528 . Last accessed: 25/03/2024.

[60] "World Intellectual Property Report 2022: The Direction of Innovation" published by WIPO in 2022 and available at: https://www.wipo.int/edocs/pubdocs/es/wipo-pub-944-2022-es-world-intellectual-property-report-2022-the-direction-of-innovation.pdf . Last accessed: 25/03/2024.

[61] "Getting the Innovation Ecosystem Ready for AI An IP policy toolkit" published by IMPO and available at: https://www.wipo.int/about-ip/es/frontier_technologies/ . Last accessed: 26/03/2024.

[62] https://oecd-opsi.org/wp-content/uploads/2021/02/Argentina-National-AI-Strategy.pdf Last accessed: 26/03/2024.

[63] https://www.wipo.int/edocs/pubdocs/es/wipo-pub-rn2023-11-es-ai-inventions.pdf . Last accessed: 13/06/2024.

2) Analyzing whether the current situation provides incentives, considering the economic and social benefits sought.

It also raises a set of questions concerning how to respond to AI-generated inventions.

On the first point, WIPO proposes looking beyond the question of who should be the inventor and lists alternatives: 1) recognize only inventions made by humans; 2) allow AI to be named as inventor or co-inventor; 3) require a legal entity to be created and designated as inventor or co-inventor when the creation was made by AI; 4) establish a new scheme of Intellectual Property laws for AI-generated creations.

In any event, WIPO proposes working from a multistakeholder perspective that enables different opinions to be considered before amendments to legislation are established.

Regarding AI and intellectual creations, following the same WIPO document, a distinction should be made between AI-assisted, AI-based, and AI-generated creations. At this point, MANTEGNA[64] proposes various alternatives for regulating AI-assisted and AI-generated creations that align with the alternatives proposed by WIPO.

Taking the author's observations into account, the scope of this area concerns authorship under copyright, industrial property, and trade secrets; the relationship of trade secrets to transparency and explainability measures—which form part of the principles considered by the law for AI—; ownership of the databases used to generate creations; and measures to be adopted from a regulatory standpoint during the development and implementation stages of generative AI systems.

[64] MANTEGNA, Micaela. "ARTEficial: Creatividad, Inteligencia Artificial y Derechos de Autor". Ed. CDYT, 2022. Pp. 299 et seq..

In turn, given its impact, it is necessary to assess the issue of intellectual property in developments applied by the State when using AI to provide services and fulfill its responsibilities.

Selected international precedents

A bill to amend intellectual property legislation in France in relation to the impact of AI[65] was recently introduced and is under consideration in its Parliament. In a few articles, the bill proposes several significant provisions:

- Article 1 establishes that the incorporation and subsequent exploitation by an AI system of copyright-protected works is subject to the general provisions on authorization by the authors of the works used;

- Article 2 states that when works are created by AI systems without human intervention, they belong to the authors or right holders of the original works, adding that they may be managed by authors' societies or other collective management organizations;

- Article 3 requires a specific notice on a work created by an AI system stating that the work was generated by this technology, in addition to the names of the authors of the original works;

- Article 4 provides for a specific form of compensation in cases where the origin of the works serving as the basis for the AI system's new creation cannot be determined, for the benefit of collective management organizations, leaving its determination to implementing regulations.

Under United Kingdom legislation, Section 9(3) of the Copyright, Designs and Patents Act 1988 [66] establishes, regarding authorship, that when a literary, dramatic, musical, or artistic work was generated by a

[65] https://www.assemblee-nationale.fr/dyn/16/textes/l16b1630_proposition-loi . Last accessed: 26/03/2024.
[66] https://www.legislation.gov.uk/ukpga/1988/48/contents . Last accessed: 27/03/2024.

computer—defined as a work for which there is no human author—the author shall be taken to be the person by whom the arrangements necessary for its creation were undertaken.

This position is not shared in every jurisdiction. The current difficulty is that many proposals exist on the subject, but it has mainly been addressed through various rulings by administrative and judicial bodies, with different answers depending on the case. The European Union's new AI legislation, for example, does not address this issue—although it does contain some provisions on data mining.

The aforementioned UN General Assembly Resolution A/RES/78/265 [67] focuses on Intellectual Property, stating: "Encouraging, where appropriate and relevant, the implementation of appropriate safeguards to respect intellectual property rights, including copyright-protected content, while promoting innovation."

In light of the above, it seems reasonable in this regard to draw on the opinions of the various international and regional bodies concerning the need to explore alternatives from a multisectoral and pro-innovation perspective.

Assessment of AI and intellectual property

As a first point, it should be mentioned that our country does have rules governing the registration of computer programs, compilations of data, or other materials constituting intellectual creations, and the expression of ideas, information, and algorithms formulated in original ordered sequences for use by an information-processing or automatic-control device. The current rules favor protection through copyright.

Current legislation also allows these rights to be registered by a natural person or a legal entity, including the State. The law also provides for anonymous works and, following the

[67] https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=q7sbXbo0iQB4sT9YhT&fe=true . Last accessed: 14/06/2024.

provisions of the Berne Convention, treats the publisher, or the entrepreneur where applicable, as the copyright holder until the author reveals their identity. Even in that case, however, the issue is not the originality or presumed authorship of the work by a person, but rather the lack of knowledge of the details of that person's identity.

As Alexander CUNTZ et al.[68] point out, this is not only a matter of determining who created the work, but also of how creations generated entirely by AI change the nature of the innovation process and how that change affects the balance of resource and incentive needs in the innovation ecosystem.

Nevertheless, although it may be prudent to ask whether ownership of the rights can be attributed to the AI system—through a form of electronic personality—to a particular natural person or legal entity—developer, user, or others—to a group of people, or whether it should be in the public domain, the conditions do not appear to be in place to provide an answer at this time.

The use of training data in AI models is another issue to clarify, in order to determine whether current legislation—both in relation to the potential use of data protected by intellectual property rights and the use of personal information protected by personal data protection rules—is sufficient to meet the needs of these systems, or whether special exceptions are required—as can be found in the Brazilian AI bill.[69]

It is also important to determine how transparency and explainability requirements operate in relation to intellectual property rights.

[68] CUNTZ, Alexander et al. "Artificial Intelligence and Intellectual Property: An Economic Perspective". Published by WIPO as part of the Economic Research Working Papers. No. 77/2024. Available at: https://www.wipo.int/publications/en/details.jsp?id=4715 . Last accessed: 26/03/2024.

[69] https://www25.senado.leg.br/web/atividade/materias/-/materia/157233 . See Article 42 in particular. Last accessed: 27/03/2024.

Regarding trade secrets, various rules relate to the subject[70]—such as Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

For personal data, Articles 13 and 16 of Law No. 18.331 address the scope of information that companies and organizations must disclose in certain types of automated personal data processing.

Finally, it is appropriate to determine whether the intellectual property rules governing the State's use of applications, indirectly reflected in the provisions on Public Software, should apply to AI systems.

In the discussion about this area's scope, the DNPI raised several points worth mentioning. It noted that the intellectual property system involves an incentive mechanism for capturing value, allowing creators to negotiate and prevent improper exploitation of their creations. It specifically indicates that it is not possible, at this stage, to transfer that rationale to AI creations.

The Directorate also argues that, in our country, which follows the continental European tradition, copyright is viewed as an extension of personality rights, establishing inalienable and nonwaivable moral rights in favor of the author; originality, in turn, is understood as an expression of the author's personality. In the case of patents, inalienable rights concern recognition as the inventor, pursuant to Article 2 of Law No. 17.164 of September 2, 1999.

Thus, under current legislation, for the inventor to be granted exclusive rights over the invention, they must provide a clear, detailed, and

[70] Details of the rules on trade and industrial secrets can be found in the following publication of the Access to Public Information Unit: https://www.gub.uy/unidad-acceso-informacion-publica/politicas-y-gestion/informacion-secreta-definida-ley . Last accessed: 26/03/2024.

complete description of the invention; where algorithms or other AI mechanisms are involved, the issue is whether it is actually possible to provide a complete description of how those algorithms arrive at one result or another, or whether a “black box” effect is generated.

Intellectual Property considerations were also raised in DATYSOC’s responses to the consultation. It mentioned the omission in current legislation regarding the use of works for computational analysis (including the restriction that such uses must not conflict with the normal exploitation of the works or unreasonably harm authors’ interests, for which it also proposes wording), as well as the need to regulate the relationships between copyright, trade secrecy, and system auditability (which, specifically regarding intellectual property, would entail exceptions allowing systems to be accessed, copied, and analyzed for auditing at a Judge’s request or when the law so provides), and to establish prohibitions on competitive uses or uses that unreasonably harm the author or right holder of the works.

DATA aligns with the need to provide greater support for decisions on procuring software or AI-based solutions by the Public Administration, noting the possibility of adapting Law No. 19.179 of December 27, 2014, and its implementing Decree No. 44/015 of January 30, 2015. It also proposes considering a mechanism for Agesic to intervene in determining risk and advising public entities on conducting impact assessments before procuring AI-based solutions in certain sectors.

Infrastructure and cybersecurity area

Preliminary considerations

AI development depends on several factors. One is adequate infrastructure, for which the State plays a central role.

The United Arab Emirates Ministry of Artificial Intelligence published a report[71] in November 2020 on the state of AI hardware infrastructure in that country, noting that the essential elements for supporting innovation in this area come down to three: a) data infrastructure—particularly its availability and the existence of high-performance storage platforms; b) networking—particularly specialized high-performance network systems connecting servers to each other and to storage units; and c) hardware infrastructure—particularly computing platforms and computer chips that accelerate AI application training and development and support large amounts of memory.

In February 2023, the OECD published report No. 350 [72] in its digital economy series, proposing recommendations for building computing capacity for Artificial Intelligence and recognizing this area of action as central to the development and evolution of the technology. The document highlights the need for countries developing AI plans to properly analyze domestic computing capacity to achieve their stated objectives.

Based on the OECD analysis, it is appropriate here to: 1) assess a review of computing capacity specifically for AI among public- and private-sector stakeholders, considering the use of cloud services within the country or abroad; 2) consider the number of existing data centers, define data standards, and analyze processing capacity and hardware needs in the country, among other aspects; 3) determine potential

[71] https://ai.gov.ae/infrastructure_report/ . Last accessed: 28/03/2024.

[72] https://www.oecd-ilibrary.org/science-and-technology/a-blueprint-for-building-national-compute-capacity-for-artificial-intelligence_876367e3-en . Last accessed: 28/03/2024.

demand for AI processing, so as to anticipate needs and plan accordingly; 4) distinguish AI processing needs from other needs; 5) provide skills and training for workers; 6) map and analyze the necessary supply chains in order to develop contingency and resilience plans.

The alternatives considered by the OECD are undoubtedly worthy of attention to ensure the effectiveness of the strategy designed. However, this document's scope concerns possible regulatory recommendations, and in that regard, the existence and adequacy or otherwise of rules relating to the following should be considered:

1) infrastructure for data management and exchange

2) information storage

3) cybersecurity

4) telecommunications networks

Selected international precedents

No legislative precedents expressly addressing this issue at the international level have been identified, beyond isolated references to specific aspects in existing legislation and draft rules; it is not present in the various AI strategies surveyed. This confirms the statement in OECD report No. 350 that many countries have developed national AI strategies without fully analyzing whether they have sufficient AI computing infrastructure and software to achieve their objectives.

The Digital Public Infrastructure initiative promoted by UNDP,[73] mentioned earlier, is linked, according to that entity, to a combination of open standards built for a public-interest purpose, enabling governance, and a community of competitive and innovative market actors to foster innovation, particularly across different public programs.

[73] https://www.undp.org/digital/digital-public-infrastructure , Last accessed: 02/05/2024.

The impacts of this way of considering certain mechanisms applicable to digital transformation solutions have been surveyed in various documents and may help determine the direction of efforts toward AI supported by secure, sovereign, and pro-innovation infrastructure.

Assessment of infrastructure and cybersecurity for AI

Our country has a strong institutional framework for telecommunications policies, cybersecurity, interoperability, and data. The distribution of powers among the different public entities involved appears appropriate, without prejudice to the need for greater coordination among them.

However, no current analyses of physical infrastructure procurement have been found, nor rules specifically governing requirements for the procurement of AI systems by public entities, AI adoption plans from this document's perspective, or objective information on the use of physical infrastructure for these activities by public or private entities.[74]

Planned procurement processes and determining entities' needs are a central issue that must be considered. Two provisions may be significant here: a) Article 74 of Law No. 19.149 of October 24, 2013, which assigns Agesic the task of providing mandatory opinions on IT development and procurement plans of Central Administration departments, and proposing to the Executive Branch general technical requirements for acquiring IT goods and services; and b) Decree No. 431/022 of December 27, 2022, which creates the Governance Committee for Cross-Cutting Processes and Solutions—composed of several public entities, including Agesic—to exercise functional and technological leadership over cross-cutting

[74] Without prejudice to sector-specific information that may help define policies, such as the "Informe de Mercado de Telecomunicaciones de Uruguay" published periodically by URSEC, available at: https://www.gub.uy/unidad-reguladora-servicios-comunicaciones/datos-y-estadisticas/estadisticas/informes-mercado-del-sector-telecomunicaciones . Last accessed: 29/03/2024.

information systems and shared technological platforms related to the internal management of Central Administration budget sections.

Planning procurement associated with the infrastructure needed for AI development would also help comply with other rules, such as Decree No. 339/021 of October 4, 2021 (Annual Procurement Plan).

Regarding information storage, Decree No. 92/014 of April 7, 2014, has been applied by public entities generally—not only those belonging to the Central Administration, whether through express reference to its provisions or through the adoption of similar rules in their respective spheres—as an argument against contracting cloud data processing services. Agesic has sought to clarify the decree's scope,[75] but consideration should be given to updating it in line with the criteria defined by the Agency.[76]

Regarding infrastructure enabling information exchange, Agesic provides the Interoperability Platform, created by Article 17 of Decree No. 178/013 of June 11, 2013, to guarantee secure and reliable electronic information exchanges. Although the platform is geared toward public entities, it could also be used by private entities, in which case the conditions established by Agesic and by entities exposing their services on the platform for information consumption must be met.

Finally, regarding cybersecurity, the National Strategy is under development, so its provisions will need to be followed. It can

[75] "Guía de interpretación del Decreto 92/014 en Ciberseguridad" available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-interpretacion-decreto-92014-ciberseguridad/guia-interpretacion and the document "Uso de la Nube en la Administración Pública" available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/uso-nube-administracion-publica/uso-nube-administracion-publica . Last accessed: 30/03/2024.

[76] "Principios generales de la Nube Pública en el Estado". Available at: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/principios-generales-nube-publica-estado#:~:text=Con%20el%20fin%20de%20guiar%20a%20las%20entidades,este%20documento%20principios%20generales%20a%20tener%20en%20cuenta . Last accessed: 30/03/2024.

be noted that, in addition to extensive preexisting regulation in this field, a recent update was made through Articles 78 et seq. of Law No. 20.212.

During the discussions on preparing the report, DINATEL submitted proposals concerning the scope and assessment in this thematic area.

It proposed considering the state of current legislation on infrastructure for data management and exchange, information storage, cybersecurity obligations, telecommunications networks (robustness and quality of service), identifying critical infrastructure, international data exchange agreements, and legislation relating to civil liability, as well as cloud infrastructure and updating current regulation of data in the cloud.

DINATEL noted that AI development in this area must incorporate infrastructure needs beyond the telecommunications sector, a social impact perspective, and nonrestrictive regulation or promotional laws for establishing and using public and private data centers in the country for public purposes. This was in addition to other contributions attached in the annex to this document.

Work and AI training area

Preliminary considerations

The impacts of AI on the world of work and on workers need to be assessed and addressed from different perspectives to take advantage of opportunities and tackle emerging challenges.

In this particular area, this report sought to identify measures to strengthen people's AI skills, aimed at preventing and mitigating negative impacts on employment and the labor market and enhancing the use of AI for society's benefit.

The OECD report entitled "OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market"[77] indicates that the impact of AI will change skill needs, that a shortage of skills already exists, and that public policies will therefore play an important role in encouraging employer-provided training, as well as training within formal education.

UNESCO shares this view in the Recommendation on the Ethics of Artificial Intelligence, which establishes, within action area No. 10, the need to expand basic and interdisciplinary skills at all educational levels related to the ethical use of AI; support cooperation agreements with educational institutions, industry, civil society, and workers' organizations to reduce gaps; and develop training strategies in medium-sized enterprises, among other measures. It also proposes working with businesses to support fair transitions for employees at risk through upskilling and reskilling programs, among others. Other measures concern research, market competitiveness and consumer protection, the provision of financing when necessary, and so forth.

[77] See in particular Chapter 5 on skills, available at: https://www.oecd-ilibrary.org/sites/638df49a-en/index.html?itemId=/content/component/638df49a-en . Last accessed: 31/03/2024.

Selected international precedents

Through Decree-Law No. 2/2023 of March 8, 2023, the Spanish government established urgent measures to promote AI in the autonomous community of Extremadura.[78] Its first article establishes, as its general primary purpose, increasing technical capacity in AI through public literacy, including training for the working population and public employees. To this end, it proposes promoting the development of entrepreneurial, creative, social, and cultural capabilities; encouraging support measures for businesses that carry out training and skill-building plans in this field; and including this training for unemployed people and public officials.

Within Section 10 (Advancing Federal Government Use of AI), the United States government's Executive Order on the Safe and Trustworthy Development of AI calls for implementing AI training and familiarization programs for employees, managers, and leaders, among others, at the highest level of federal government agencies. These programs must empower employees and others to develop and maintain operational knowledge of emerging AI technologies. It also proposes that agencies provide professional development opportunities, scholarships, and funding for their staff.

Assessment of work and training for AI

Various national provisions promote training among workers. However, the legislation initially analyzed does not show a particular emphasis on AI-related aspects and how to manage its impacts, although digital training for workers is included in programs such as those run by the National Institute for Employment and Vocational Training (INEFOP), or by the National School of Public Administration (ENAP) for public-sector workers.

[78] https://www.boe.es/buscar/doc.php?id=BOE-A-2023-8795 . Last accessed: 31/03/2024.

For these reasons, the existing institutional framework is considered capable of implementing policies and programs related to this issue and exploring alternatives for cooperation between public and private entities.

Making the issue visible, establishing coordinated actions, defining a specific policy, and implementing sustained cooperation among the ecosystem's different stakeholders must be considered in order to carry out a successful strategy in this field.

Civil liability and consumer rights area

Preliminary considerations

AI raises questions that are difficult to resolve for many legal practitioners who, in countries such as ours, seek to interpret rules that—although they clearly provide the necessary legal certainty—were enacted in circumstances very different from today's.

The area addressed here concerns two aspects that are well regulated in law: civil liability and consumer relations.

In analyzing the preventive function of civil liability in our legal system, DE CORES[79] indicates that the concept itself is described as "(…) highly polysemous, but in a broad sense it can be defined as the consequence arising from noncompliance with a rule, so that liability may be not only civil but also criminal, administrative, and even political or moral."

JOSÉ DOS SANTOS[80] states that "(…) civil liability serves to restore the balance compromised by the occurrence of moral or material harm caused by the causal agent," and highlights that Brazilian law recognizes fault-based civil liability—which requires malicious or culpable conduct, or an omission by the person responsible for that conduct—and strict liability—in which proof of the causal link between the conduct and the harm is sufficient, regardless of the intention or fault of the person who caused it.

The author considers what happens with AI civil liability, concluding that it is necessary to consider whether current legal institutions can respond to its evolution.

[79] DE CORES, Carlos. "La denominada función preventiva de la responsabilidad civil. Una crítica a su ubicación dogmática". Available at: https://eva.fder.udelar.edu.uy/mod/resource/view.php?id=49243&redirect=1 . Last accessed: 30/03/2024.

[80] JOSÉ DOS SANTOS, Sonia "Inteligencia Artificial y Responsabilidad Civil" in "Inteligencia Artificial y Derecho" 1st ed. Ed. Hammurabi. 2020. P. 179 et seq.

Within the concept of civil liability, the most common distinction is between contractual liability—arising from breach of a contract between two or more parties—and noncontractual liability—arising from harm caused to someone without such a contractual relationship. The civil liability regime in Uruguay is regulated primarily in our Civil Code.

Consumer relations are defined in Article 4 of Law No. 17.250 of August 11, 2000, as the relationship between a supplier who provides a product or service for consideration and the person who acquires or uses it as the final recipient. From the perspective of the parties involved, there are the figures of supplier and consumer.

ARAMENDIA[81] notes that, regarding AI use and any harm caused through these systems, there are 2 extremes to consider: the uncertainty faced by people harmed by a product or service containing AI about how to proceed to obtain compensation, and the uncertainty faced by designers, developers, producers, financiers, and other members of the chain that brought that product or service to market about their role in causing the harmful event.

The author identifies three challenges: 1) system complexity and the diversity of factors that may cause the error that in turn caused the harm; 2) the number and diversity of actors in the chain, making traceability difficult; 3) the mechanism for continuing to encourage AI investment, research, and development while ensuring that those who suffer harm can obtain fair compensation.

It is precisely the response to these three challenges that we will seek to consider, from a strictly regulatory perspective. The impacts AI may have on consumer relations are outside the scope, since this area will address the problems associated with suppliers' liability and compensation for harm to consumers.

[81] ARAMENDIA, Mercedes. "La Inteligencia Artificial ¿y la responsabilidad?" in "Estudios sobre los Desafíos Jurídicos ante la Digitalización" Volume III. Eds. Mercedes Aramendía and Agustina Pérez Comenale. Ed. UM. Year 2023. Pp. 557 et seq.

Selected international precedents

At this point, it is relevant to consider the proposed European Union AI Liability Directive,[82] which complements the recently approved Regulation.

CASALS[83] notes that “The current proposed Directive, by contrast, refers only to liability based on intent or fault for damage caused by AI systems, which remains subject to national substantive rules. For that reason, it conflicts neither with the application of national rules nor with those arising from the Directive on liability for defective products and, as noted, its substantive scope is much broader.”

On this point, the European Commission[84] has stated: “The Directive simplifies the legal process for victims when proving that someone’s fault led to damage, by introducing two main features: first, in circumstances where relevant fault has been established and a causal link to AI performance seems reasonably likely, the so-called ‘presumption of causality’ will address the difficulties victims experience in having to explain in detail how damage was caused by a specific fault or omission, which can be particularly difficult when trying to understand and navigate complex AI systems. Second, victims will have more tools to seek legal redress through the introduction of a right of access to evidence from companies and suppliers, in cases involving high-risk AI.”[85]

[82] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496 . Last accessed: 30/03/2024.

[83] CASALS, Miguel Martín. “Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial”. Available at: https://indret.com/las-propuestas-de-la-union-europea-para-regular-la-responsabilidad-civil-por-los-danos-causados-por-sistemas-de-inteligencia-artificial/ . Last accessed: 30/03/2024.

[84] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_5807 . Last accessed: 30/03/2024.

[85] A more extensive analysis can be found in La Ley Digital, in the article by Gonzalo ITURMENDI MORALES “Responsabilidad civil por el uso de sistemas de inteligencia artificial” available at https://laleydigital.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAmNDCwsjI7Wy1KLizPw8WyMDIwNDQyMDkEBmWqVLfnJlZUGqbVpiTnEqANKvjtI1AAAAWKE . Last accessed: 30/03/2024.

A bill introduced in the Argentine Republic[86] establishes in Articles 19 to 23 a liability regime for harm or errors in use. The bill proposes liability for developers and suppliers for errors in the use of their systems that cause harm if they have not taken reasonable measures to prevent the error or have failed to comply with established regulations and standards; they must implement security measures and testing. It also provides for users' responsibility to use systems properly and in accordance with the instructions provided, exercising due diligence; otherwise, users will be liable for harm to third parties. It also includes an obligation to maintain adequate civil liability insurance to cover possible harm. Finally, there are rules on transparency and training, and a mechanism for reporting errors in the use of artificial intelligence.

There are also no relevant legislative precedents in this area beyond the provisions of the proposed European Union Directive. This prompts reflection on the need for a specific, multistakeholder analysis of Uruguayan legislation, given the sensitivity of the civil liability structure for legal certainty.

Assessment of civil liability and consumer rights

The first point of the assessment is that the rules do not establish specific regulation for the problems arising from harm that AI systems may potentially cause. Unless the liability regime is clearly established in a contract's terms, the general civil liability rule that might apply by analogy in these cases—which involve great complexity in identifying the members of the chain leading to an AI product or service being put into production—is Article 1330 of the Civil Code, which regulates a form of collective liability associated with objects falling from a building. This general analysis and its

[86] https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/2505-D-2023.pdf . Last accessed: 30/03/2024.

application by analogy were developed at the time by BORDOLI,[87] although not specifically in relation to the issue addressed here, but rather the allocation of liability when there is an identified group comprising several people but it is not possible to determine specifically who caused the harm.

This regime appears insufficient for properly assigning liability to those who caused the harmful event and providing effective compensation for the harm suffered by individuals.

For consumer relations, the aforementioned Article 34 of Law No. 17.250 of August 11, 2000, applies. It provides: “If a defect or risk in the product or the provision of the service results in harm to the consumer, the supplier will be liable in accordance with the regime provided for in the Civil Code.

The retailer or distributor will be liable only when the importer and manufacturer cannot be identified. They will likewise be liable if the harm results from improper storage of the product or when its original conditions are altered.”

Another aspect to consider concerns harm caused when the product or service is offered by the State, in which case Articles 24 and 25 of the Constitution apply, as indicated.

[87] BORDOLI, Carlos Rubens. “Responsabilidad Extracontractual Colectiva por Daño Causado por un Miembro Indeterminado de un Grupo” available in Revista de la FDER (30). Year 2014. Pp. 65 et seq. Available electronically at: https://revista.fder.edu.uy/index.php/rfd/article/view/87 . Last accessed: 30/03/2024.

AI support measures area

Preliminary considerations

The objective of this area is to consider the scope and determination of possible support measures associated with public policy on AI.

Why propose measures to promote AI? The answer lies in the proven benefits this technology can bring to society. Although emphasis is placed on warning about its potential risks for people, it is also important to weigh its many advantages.

In this regard, the December 2023 interim report of the UN AI Advisory Body[88] can be considered. It establishes preliminary recommendations based on 5 principles: 1) inclusive governance, by and for the benefit of all; 2) governance in the public interest; 3) governance built alongside data governance and the promotion of the commons; 4) universal, networked governance rooted in multistakeholder collaboration; 5) governance anchored in the UN Charter, international human rights law, and other agreed international commitments such as the Sustainable Development Goals. Regarding the promotion of AI for Humanity, the document notes, among other things, the need for access and benefits to go together through national investment in talent, data, and computing resources. International cooperation and assistance in the public and private sectors are seen as relevant to this end.

The appropriateness and scope of possible AI support measures must take into account: 1) determining the objectives toward which effective promotion of Artificial Intelligence is directed, placing at the center developments that help build a more just and equitable society; 2) the concrete instruments that could be used to provide benefits that support the development of systems identified as their intended recipients.

[88] https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf . Last accessed: 04/04/2024.

Selected international precedents

Among the most relevant points of the Executive Order on the Safe and Trustworthy Development of Artificial Intelligence applicable to United States government agencies[89] is the promotion of innovation and competition through:

> a) Catalyzing AI research in the United States through a National AI Research Resource pilot.
>
> b) Promoting a fair, open, and competitive ecosystem through technical assistance and resources for small developers.
>
> c) Using existing authorities to expand the ability of highly skilled immigrants and nonimmigrants with expertise in critical areas to study, remain, and work in the United States.

The above is without prejudice to other points such as international cooperation and collaboration among entities within government.

For its part, the proposed European Union "AI Act"[90] expressly notes the link between data governance, open data, and the promotion of AI-driven innovation. Measures to support innovation include developing AI regulatory sandboxes, allowing data processing for certain purposes, and measures for small-scale providers and users ranging from priority access to sandboxes, awareness-raising activities, and dedicated communication channels to, potentially, differentiated fee amounts for certain services.

[89] The Executive Order's content can be consulted at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ Last accessed: 04/04/2024.

[90] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206 . Last accessed: 04/04/2024.

In Brazil, Bill No. 2338/2023 [91] emphasizes promoting research and development to stimulate innovation in productive sectors and the public authorities. Measures also include the creation of regulatory sandboxes and public AI databases.

Other international provisions share the support criteria reflected here, including the concept of developing innovation and thereby emphasizing the role of regulatory sandboxes in that regard.

Preliminary assessment of AI support measures

There are currently some provisions specifically addressing the promotion of innovation in AI. At the time of this document, implementing regulations for Article 75 of Law No. 20.212 are being drafted, so the considerations made in this analysis will be taken into account.

Other types of measures could also be effective in promoting innovation and its developments, such as tax exemptions, and analyzing and promoting seals certifying that audits and assessments have been conducted, which in turn allow access to certain benefits, among others. All these elements require specific analysis.

[91] https://legis.senado.leg.br/sdleggetter/documento?dm=9347622&ts=1702407086098&disposition=inline&_gl=1*1wg6j22*_ga*NTk0MjQwOTMwLjE3MDE3OTA5MTc.*_ga_CW3ZH25XMK*MTcwNjYxODMwOS4yLjEuMTcwNjY0NDgxOC4wLjAuMA . Last accessed: 04/04/2024.

Other thematic areas identified from the contributions received

The use of AI systems for surveillance

Among the concerns and recommendations raised by civil society when responding to the consultation document made available by this Agency were issues associated with the use of AI systems for surveillance by security forces.

Law No. 19.696 of October 29, 2018, implemented by Decree No. 157/022 of May 23, 2022, establishes and regulates the National State Intelligence System (SNIE), requiring its constituent bodies to comply with a set of principles aimed at respecting the Constitution, the principles of the democratic republican system of government, and human rights.

Within this framework, Article 20 of the Law provides that gathering information through special procedures that may affect citizens' freedom and privacy must be authorized by the Judiciary. Regarding controls, Article 25 should be highlighted: it provides for creating, within the General Assembly, a bicameral parliamentary committee tasked with controlling and overseeing the system's activities.

Decree No. 157/022 approves the National Intelligence Policy, specifying a set of actions and measures. However, apart from generic references to compliance with human rights, it makes no provision regarding the application of AI in surveillance of individuals.

In its response to the consultation, civil society offers suggestions such as imposing a moratorium on surveillance software procurement until there is a legal basis adequately regulating the police surveillance ecosystem, or requiring algorithmic auditability and explainability, traceability, access control protocols, and detailed descriptions of responsibilities for those using these surveillance systems.

Civil society also proposes establishing red lines regarding which uses are strictly prohibited for police and which require a court order; prohibiting real-time biometric surveillance without a court order in public spaces; and specifically regulating the admissibility, assessment, and handling of biometric matches as investigative methods and digital evidence, among other measures.

Finally, civil society's recommendations include adequate training for police officers, judges, and prosecutors—through mandatory certification—and urgently regulating the Ministry of the Interior's use of AI for surveillance.

This Agency shares the concern for the proper use of AI systems in security force activities, but also wishes to emphasize the need to establish multisectoral dialogue to ensure an appropriate balance between internal security needs and the protection of people's fundamental rights.

International engagement and cooperation

Another aspect that was not part of the initial thematic areas, but is enormously important, is the country's international engagement. As with other issues on our countries' agendas, AI poses global challenges that motivate us to seek global solutions.

Furthermore, since the AI systems applied in the region are "imported" from other parts of the world, we must make an additional effort to generate regional cooperation mechanisms that address our own needs.

As part of Our Common Agenda[92] presented by the UN Secretary-General in 2021, the organization launched last year the "Global Digital

[92] https://www.un.org/en/content/common-agenda report/assets/pdf/Common_Agenda_Report_English.pdf . Last accessed: 22/06/2024.

Compact – an Open, Free and Secure Digital Future for All"[93]—currently under consultation and expected to be agreed at the Summit of the Future to be held this year—which, under objective 5, includes improving international governance of emerging technologies, including AI, for humanity's benefit. The document proposes agile, multidisciplinary, and multistakeholder international governance, as well as concrete initiatives such as establishing an International Scientific Panel on AI and Emerging Technologies and an International Contact Group on AI Governance.

An interesting aspect of this document is that it also proposes promoting North-South and South-South cooperation on developing datasets, computing capacity, local solutions, use cases, and business ecosystems in developing countries.

At the international level, the AI Framework Convention promoted by the Council of Europe has already been mentioned. It constitutes the first international treaty on this subject, with a perspective based on both principles and risks. Having participated as an observer in the drafting process, our country has the opportunity to become a party to the Convention, which should be assessed with advice from the Ministry of Foreign Affairs. It can already be stated that this Agency shares the Convention's provisions and supports accession.

Finally, at the regional level, special mention should be made of UNESCO and CAF's efforts to incorporate the regional voice into the discussion about AI's future. The First Ministerial and High-Level Authorities Summit on the Ethics of AI in Latin America and the Caribbean, organized by them with the support of the Chilean government, produced the aforementioned Santiago Declaration,[94] which approved establishing a Working Group to create an Intergovernmental AI Council for Latin America and the Caribbean, within the framework of UNESCO's Recommendation on the Ethics of AI, to strengthen regional capacities in this field.

[93] https://www.un.org/techenvoy/global-digital-compact . Last accessed: 22/06/2024.

[94] https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf . Last accessed: 22/06/2024.

Contributions from other public entities identified in the first stage of discussion

In preparing this report, several meetings were held with the entities mentioned in this document, whose contributions can be summarized as follows:

Institutional framework and governance area

- A cross-cutting approach is needed, while it is also important to have a lead body in this field.
- Have an advisory committee to provide advice on specific issues and include different stakeholders according to the topics to be addressed (for example, the private sector, civil society organizations, telecommunications companies, and companies involved in developing AI systems, among others). It is proposed that the Committee form ad hoc groups according to the specific issue to be addressed, or otherwise invite experts in the relevant sector or area.
- Include in the analysis consumer protection, user protection, and consideration of the individual as a digital citizen (AI generator and user)
- Incorporate telecommunications data and consider this a critical service.
- Include the Ministry of National Defense (MDN) in discussions because of defense and the use of AI for that purpose, as well as the Ministry of the Interior (MI) for public security issues.
- Apply public consultation mechanisms to broaden the stakeholders involved, obtaining and/or incorporating other perspectives.
- Include and work to strengthen small and medium-sized enterprises.

Human rights area

- Consider developing policies for AI systems.
- Regarding vulnerable populations, pay particular attention to girls, boys, adolescents, and older adults.

• Specify that the final decision must be made by a human, not the algorithm, and consider incorporating audits to analyze the impact of applying AI, with those audits being institutionalized.

• Analyze the stage in the process cycle at which an audit should take place.
• Designate a body and/or institution to exercise independent oversight in certain cases of risk and/or high impact.

• Analyze the feasibility and/or appropriateness of granting greater powers to the INDDHH or establishing a human rights safeguard mechanism.
• Incorporate a workstream that integrates AI to facilitate access to State services.
• Recognizing the importance of the labor sector, analyze how businesses could play a proactive role by proposing alternatives when human work is replaced by AI, for example through training to undertake other tasks and use new technologies.
• Analyze how to address environmental impacts.
• Consider a risk-based approach.

Work and training for AI area

• Emphasize the impact specifically on employment and, more generally, on the world of work.
• Consider all Labor Legislation in Force (particularly rules on combating discrimination in the workplace).

Intellectual property area

• Generate further discussion about authorship and incorporate the issue of plagiarism.
• Analyze the development of exceptions for using certain data for training, and establish safeguards where copyright is involved, defining their scope and purpose.

• Discuss a reform of Copyright Law No. 9739 to address AI's impact in this field.

• Regarding patents involving AI, analyze whether or not patent applications need to indicate how AI is involved in the inventive process.

• Encourage actions to develop Intellectual Property.

Civil liability and consumer rights area

• Determine the scope of current legislation to address possible harm caused by the use of AI systems and deepen its analysis before developing regulatory proposals.

• Analyze the possibility of raising public awareness so people can identify when they are in an AI-related consumer relationship, as well as the mechanisms available for making claims and/or complaints.

Infrastructure and cybersecurity area

• Clearly define the concept of AI as applied to infrastructure and cybersecurity.

• Consider issues such as using international data repositories in the public and private spheres.

• Consider and analyze the quality of Software and Hardware in public institutions.

• Identify other types of companies, such as storage service providers.

• Consider AI applied to the standardization of telecommunications infrastructure.

• Analyze the possibility of regional computing capacity centers.

• Assess environmental aspects and natural resource use.

• Assess the country's capabilities in each of the following areas:

- Rules for data management and exchange
- Storage capacity, computing capacity
- Cybersecurity

- Connectivity and infrastructure capacity: scalability, flexibility, and adaptability to change

Support measures area

• Analyze and define national strategic objectives for the use of AI.

• Survey existing support measures in this field and in various AI-related areas.

• Analyze the possibility of having national infrastructure in which to conduct tests (sandboxes and others).

• Analyze the possibility of exemptions and tax incentives associated with promoting AI development and use aimed at the country's strategic objectives in different fields.

Recommendations

Preliminary concepts

The preceding chapters presented an overview of the process and framework applied in preparing the report assigned to this Agency under the aforementioned Article 74 of Law No. 20.212.

The recommendations presented result from the institutional analysis based on the assessment previously developed of the challenges identified for each thematic area, taking into account:

1. the guidelines arising from Article 74 of Law No. 20.212;
2. the national legal framework, including the applicable rules of international law and the resulting legal obligations to respect, protect, guarantee, and promote human rights within and outside the digital environment;
3. the principles and recommendations emerging from international soft law precedents;
4. the review of regulatory precedents developed by other countries;
5. contributions received from public entities, civil society, and the private sector during the work process implemented for this report and during the development of the Strategies led by this Agency;
6. the guidelines established in the country's digital policy, arising from the Digital Government Plan 2025, [95] the Uruguay Digital Agenda 2025, [96] and the AI Strategy for Digital Government.[97]

95 https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/plan-gobierno-digital-2025 . Last accessed: 20/06/2024.

96 https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-actualizacion-medio-termino. Last accessed: 20/06/2024.

97 https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial. Last accessed: 20/06/2024.

Given the cross-cutting nature of AI systems and their current and potential positive and negative impacts across all sectors of society, these recommendations should not be interpreted as an exhaustive list.

They reflect the result of the institutional analysis reached as of the presentation date of this report on general rather than sector-specific aspects, in a context marked by rapid technological development—which requires sustained analysis of the associated potential and risks—ongoing regional and international processes, an ongoing review of the AI Strategy, and the development of the National Data and Cybersecurity Strategies.

All this makes it foreseeable that, in the future, these elements may affect the public challenges addressed by these recommendations and may need attention during the work process that the Legislative Branch may initiate.

The analyses also draw on this Agency's knowledge and experience in digital transformation and policy and on contributions from other public entities in specific fields. However, several of the issues analyzed require in-depth debate with those entities and other stakeholders before any measure is adopted.

General recommendations.

The growing number of international instruments developed in recent years reflects a situation in which there is increasing consensus on the need to regulate activities throughout the lifecycle of AI systems, to ensure that they are fully consistent with human rights, democracy, and the rule of law, while enhancing the opportunities these technologies offer humanity and ensuring equitable access to them between and within countries.

As set out in this report, these instruments include, among others: the OECD Recommendation on AI and its principles adopted in 2019 and updated in 2024; the Recommendation on the Ethics of Artificial Intelligence adopted by UNESCO in 2021; the AI principles and the “International Code of Conduct for Organizations Developing Advanced AI Systems” developed by the G7 in 2023 as part of the Hiroshima AI Process; the European Union AI Act, approved in March 2024; the Framework Convention on Artificial Intelligence adopted by the Council of Europe in May 2024; and the recent Resolution on “Safe, secure and trustworthy artificial intelligence systems for sustainable development,” adopted by the United Nations General Assembly in March 2024.

At the inter-American level, examples include, among others: the Santiago Declaration to promote ethical artificial intelligence in Latin America and the Caribbean, arising in 2023 from the Ministerial and High-Level Authorities Summit of Latin America and the Caribbean, and the Regional Charter on Artificial Intelligence in Administration, adopted within the Latin American Centre for Development Administration (CLAD) in 2023. Uruguay has followed these efforts closely and, in several cases, has participated in their development or adhered to them.

These precedents clearly call on States to respect and act proactively to protect and promote human rights throughout the AI lifecycle by adopting adequate and effective regulatory frameworks, under a balanced approach that integrates AI’s risks and opportunities and promotes responsible and safe innovation.

The precedents presented recognize that AI governance is an evolving field requiring progress in building common frameworks while also allowing each State room to establish national regulatory approaches and instruments according to national contexts and priorities, consistently with its legal framework and the obligations arising from applicable international law.

In light of all the above, this Agency considers it appropriate, first, to affirm the importance of our country maintaining a proactive approach to

regulating AI systems through various public policy instruments:

1. Updating its Artificial Intelligence Strategy under a multistakeholder approach, to respond to the new context generated particularly—but not only—by the expansion of more advanced models such as Generative AI; and with the aim of extending its scope to the private sector, as established by Article 74 of Law 20.212. This process is underway and is expected to be completed in the second half of this year.

2. Reviewing existing legislation, where relevant, in order to:

i) Strengthen the institutional design for AI governance in the country, including mechanisms for multistakeholder participation and collaboration; ii) Ensure that activities throughout the lifecycle of AI systems are fully consistent with human rights, democracy, and the rule of law, through frameworks that enable the identification, prevention, assessment, and mitigation of risks and negative impacts on those rights.

iii) Promote equitable use of AI opportunities and benefits for society and the country's sustainable development in its different dimensions (social, cultural, environmental, and economic), promoting research and safe innovation in the public interest;
iv) Ensure the ethical, human-rights-respecting, responsible, and safe development and use of AI systems in the public sector;

v) Strengthen the country's digital sovereignty and AI sovereignty with a forward-looking vision.

3. Developing, from the public sector, among other possible instruments, agreed protocols, guidelines, and technical recommendations for sectors and areas critical to society and national interests, and promoting, where relevant, the adoption of instruments such as guidelines, codes, and other self-regulatory mechanisms

aligned with national guidelines; and implementing the policies and measures defined under the National Digital Citizenship Strategy, the National Data Strategy, the National AI Strategy, and the National Cybersecurity Strategy.

Second, taking into account the concerns and contributions received from civil society and the private sector during the work process undertaken to prepare this report, this Agency would also like to emphasize, as a general recommendation, the importance of ensuring that regulatory measures adopted:

1. are preceded by and grounded in a public discussion process based on a multistakeholder approach;
2. take into account both the impact of insufficient regulation and the impact of overregulation;
3. are analyzed across disciplines, involving different areas of expert knowledge.

Uruguay has an extensive and sustained track record in international forums such as the Open Government Partnership (OGP), through which it has promoted and implemented various initiatives to integrate open government principles into its digital policy, while also defining the pillars of open government as part of its digital policy objectives.

In this regard, and also in line with other international approaches such as UNESCO's Recommendation on the Ethics of AI, the country is encouraged to continue and deepen its path of participatory and transparent digital policymaking through open government and open parliament policies.

Among the suggestions and contributions received by this Agency during the report's preparation are the following specific proposed measures, which are brought to the Legislative Branch's attention:

- Create a forum for different social stakeholders to identify priorities and formulate recommendations.
- Hold a public hearing before the Legislative Branch involving businesses, academia, and specialized civil society.

• Create advisory groups with participation from all stakeholders that meet regularly.

Finally, third, this Agency would like to highlight, as a general recommendation, the importance of ensuring that any new regulatory instruments provide for periodic review and updating in light of emerging challenges.

Specific recommendations

A summary of recommendations is provided based on the guidelines defined and thematic areas covered.

AI institutional framework and governance

As mentioned above, this is a central aspect of many international instruments, and different jurisdictions apply various arrangements that seek, in one way or another, to establish a specific AI institutional framework, either by drawing on preexisting institutions or creating new ones. Defining the country's institutional framework for AI also affects data governance mechanisms—which must be established—and therefore AI development itself.

The role of Agesic in the AI institutional framework

Regarding Agesic's role, it is proposed that the possibility of enhancing the Agency's current capabilities be assessed by establishing a new internal structure covering Artificial Intelligence and Data, including the roles defined in the final paragraph of Article 74 of Law No. 20.212.

This would clarify the current expansion of the Agency's powers beyond the design and implementation of the National AI Strategy. It would also take advantage of Agesic's potential, since aspects of data management within public entities currently fall within its competence.

It could be appropriate—although not strictly necessary—to establish a statutory provision granting the Agency powers additional to those already existing—indicated in Article 74, final paragraph, and Article 75 of Law No. 20.212—including its role in coordination with other national entities and in representing the country internationally on this issue. Beyond this, it should be recalled that the Agency's leadership in digital transformation and policy arises from several preexisting provisions already reviewed.

Without prejudice to Agesic's leadership in this area, participation by other stakeholders within and outside the public sector is necessary to help design and implement comprehensive public policies. Since its beginnings, Agesic has had a set of Advisory Councils and leads various strategic committees.

Regarding the strategy for adopting an artificial intelligence and data policy, it is proposed that the current Public Sector Strategic Committee for Artificial Intelligence and Data be formally institutionalized through regulation, coordinating with the Agency not only on developing the National AI and Data Strategy but also on planning the action plans that enable its implementation.

Among the Committee's fundamental roles would be to collaborate with Agesic in developing general policies in this field, in addition to working with other competent public entities when developing sector-specific policies. Under this model, sector-specific public entities would undertake the processes of developing sector-specific rules and recommendations, monitoring, and overseeing compliance, alerting Agesic and the Committee in the event of deviations.

Another aspect to consider, which may lead to a different composition of the Committee, is the definition of other issues arising from the participatory process of creating the National AI and Data Strategies that guide public policy in these fields.

Under Article 74, final paragraph, of Law No. 20.212, sector-specific oversight processes assigned to public oversight entities will receive support from Agesic —and possibly the Committee—when AI systems are used.

Beyond particular membership arrangements, this Agency considers that certain entities must be part of this institutional framework (such as ANII, MIEM, URCDP, and INDDHH), to comply with the Legislative Branch's guidelines on developing ethics-based AI that promotes innovation and respects human rights.

The institutional framework for AI within organizations

Two lines of action are suggested within public entities: i. training and strengthening in AI and Data; and ii. structural strengthening to equip each institution with capabilities to manage, monitor, and oversee the policies implemented, as well as carry out strategic and operational plans aligned with those policies.

Several roles currently must be established by public entities and relate to data governance: the personal data protection officer—established by Article 40 of Law No. 19.670 of October 15, 2019—; the transparency officer—established by Articles 41 and 57 of Decree No. 232/010 of August 2, 2010, implementing Law No. 18.381 of October 17, 2008—; and the information security officer—established by law under Article 78, subsection B, of Law No. 20.212 of November 6, 2023.

A particular feature of the data protection officer and information security officer roles is that they extend not only to public entities but also to some private entities:

- the first role extends to those private entities whose main business is processing sensitive data—with sensitive data exhaustively defined in Article 4, subsection E, of Law No. 18.331 of August 11, 2008—and those processing large volumes of data—defined as data relating to more than 35,000 people by Article 10, subsection c, of Decree No. 64/020 of February 17, 2020—;

- the second concerns private entities linked to critical services or sectors of the country—which depends on the definition provided in implementing regulations that have not yet been issued.

To this must be added the need for designated contacts to implement open data policies in public entities, related to compliance with Article 82 of Law No. 19.355 of December 12, 2015.

This Agency considers it possible to adapt the functions of existing roles, particularly that of the data protection officer, through AI and data governance training. It does seem appropriate to create an Internal Data Committee within public organizations, including the data protection officer, information security officer, transparency officer, and open data contact.

A multisectoral and multidisciplinary perspective

Throughout this report, repeated mention has been made of the need for policymaking to adopt a multistakeholder perspective that includes public entities, private entities, academia, and civil society, also taking into account the different productive sectors.

It has also been proposed that organizations have strategic AI and Data roles that enable policy development in these fields and enhance the opportunities both offer.

To this end, it is proposed to build on existing institutional arrangements within Agesic by modifying the powers of the Honorary Advisory Council for the Information Society and potentially incorporating new stakeholders, under a scheme similar to the one currently in place for Cybersecurity. Multidisciplinarity must also be considered.

Agesic currently has two AI-related forums worth maintaining and strengthening: 1) the AI Community in the Public Administration,[98] comprising technical contacts from various public entities; 2) the Observatory on AI Use in the State,[99] created as part of a commitment

[98] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/comunidad-inteligencia-artificial-administracion-publica . Last accessed: 29/03/2023.

[99] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/observatorio-uso-inteligencia-artificial-estado . Last accessed: 29/03/2024.

made under the 5th Open Government Action Plan. Both forums enable participation by different ecosystem stakeholders, with complementary purposes of great value to AI development, notably involving civil society and specialized technical experts.

Data governance

Finally, regarding data governance, progress should continue in public entities' obligations to publish data securely—through the platform provided for in the regulations—and in a manner respectful of personal data protection, going beyond the obligation established in Article 5 of Law No. 18.381 of October 17, 2008.

We must also continue advancing toward a data governance model that makes the policy defined in this field sustainable.

It is also important to continue promoting mandatory information exchange—within the current framework—between public entities (Article 157 et seq. of Law No.18719), to encourage data reuse, and to make progress in designating those responsible for Government master data.

Using data from private entities may also make a difference in this field, for which incentives could be promoted when they decide to share data—not necessarily personal data, but data useful for public policymaking. Such incentives are not present in current legislation, but could include tax exemptions and improvements in service provision, in addition to strictly reputational aspects.

At the international level, Regulation (EU) 2023/2854 (Data Act)[100] establishes certain rights for device users to access and share their data, obligations for private companies to share information when requested by public entities, and compliance with minimum requirements that

[100] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1704709568425 . Last accessed: 21/06/2024.

ensure interoperability—in line with the standardization strategy for a single, resilient, green, and digital market—among other things.

This regulation is also one of the pillars of the European data strategy and digital transformation policy, and is complemented by Regulation (EU) 2022/868 (Data Governance Act),[101] which lays the groundwork for data sharing processes and provides for interesting concepts such as “data altruism,” allowing information to be shared for general-interest objectives with appropriate safeguards.

Regarding data use at market level, the perspectives of the Consumer Protection Unit and the Commission for the Promotion and Defense of Competition, both within the Ministry of Economy and Finance, must be included.

Regarding personal data and system training, it seems necessary to discuss current regulation on lawful grounds for personal data processing. Article 9 of Law No. 18.331 of August 11, 2008, omits processing grounds that do exist internationally, and the existing grounds may create interpretive difficulties when applied to training AI systems. Although this circumstance does not necessarily prevent data use, the lack of a lawful basis such as legitimate interest adds complexity and leads to consideration of whether other grounds can be used for these purposes.

Other instruments, such as the data trusts suggested by the INDDHH, have begun to form part of the discussion. However, the delicate balance in personal data processing provided for in Law No. 18.331 means that this discussion should be led by the Urcdp.

[101] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868 , Last accessed: 21/06/2024.

Summary of recommendations related to the institutional framework and governance	
Recommendations aimed at possible amendments or updates to regulations	- Create Internal Data Committees in public entities, including transparency officers, data protection officers, information officers, and open data contacts. - Promote the use of open and interoperable data, considering new obligations for public entities to publish data in open format, establishing deadlines and conditions for publication
Other recommended initiatives	- Specify Agesic's powers relating to leadership in AI and Data - Create a new institutional structure within Agesic responsible for AI and Data policy. - Institutionalize the Public Sector Strategic Committee for AI and Data. - Reconfigure the Honorary Advisory Council for the Information Society to incorporate new stakeholders and functions. - Define a governance model for government data. - Strengthen public entities' training and equip them with the capabilities needed to ensure they can implement policies, strategies, and operational plans on AI and data

	- Provide data and AI training to data protection officers and other roles related to data management in public entities. - Promote incentives for private entities to share data, respecting personal data protection and intellectual property rules, and through secure mechanisms. - Promote the creation of public databases that contain information reflecting the local language and characteristics and can serve as training data for AI systems. - Enable private entities to use the interoperability platform provided for in Decree No. 178/013 of June 11, 2013.

Ethics, human rights, and democracy

The starting point for protecting human rights

Uruguay maintains close ties with the Inter-American and Universal human rights protection systems, has ratified the human rights treaties arising from these systems, and actively participates in their forums. The recommendations in this section begin by considering the obligations (to respect, protect, and guarantee) that international human rights protection imposes on States.

Along the same lines, the recent UN General Assembly Resolution on AI emphasizes “that human rights and fundamental freedoms must be respected, protected and promoted throughout the lifecycle of artificial intelligence systems” and “calls upon all Member States and, where appropriate,

other stakeholders, to refrain from or cease using artificial intelligence systems that are impossible to operate in compliance with international law or that pose undue risks to the enjoyment of human rights, especially for those in vulnerable situations, and reaffirms that individuals' rights must also be protected online, including throughout the lifecycle of artificial intelligence systems."[102]

The legal protection of human rights in our country is grounded in the Constitution of the Republic, the norms of international human rights law that have been ratified, and a broad and diverse set of laws specifying protection and regulating the exercise of certain rights. Nevertheless, in some cases, the legal protection of human rights in this field would be strengthened by developing rules that specify protection in this area.

Special measures aimed at protecting human rights

Based on the preceding section, and building on the progress already made through Law No. 20.212, the first recommendation is to broaden the specification of AI Strategy principles in Article 74 of that law, identifying them as guiding principles for AI policies and their various regulatory instruments.

These principles can be complemented by measures that give them substantive content and enable their implementation, taking Articles 6 to 12 of Law No. 18.331 as a basis. These not only enumerate the scope of the principles, but also determine certain practical actions to be carried out by personal data controllers and processors.

In addition, based on the guidance arising from Article 74 of Law No. 20.212 itself, current and potential risks and adverse impacts on human rights throughout the lifecycle of

[102] https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=ZTiBbJsISYXoE5uIOW&fe=true

AI systems in the public and private sectors must be addressed through regulation and other measures.

In light of the need to address these risks and impacts, it is suggested that adopting a risk-based approach be considered in order to:

1. Analyze and define applications of AI systems that are

   unacceptable to society because of their impact on people's rights, assessing bans or moratoria that are appropriate and consistent with the obligation to protect human rights; and

2. Identify and define AI applications that represent a

   high risk to people's rights based on the context and intended use, and the severity and likelihood of possible impacts, in order to define the specific measures that apply.

Various models and approaches have been developed internationally to address risks. For example:

• The European Union AI Act establishes a set of prohibited applications (Title II of the Act), including cognitive behavioral manipulation of people that affects their autonomy and ability to choose freely; biometric categorization systems based on biometric data; and the use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for law enforcement purposes, with exceptions.

• The Executive Order adopted in 2023 by the United States Government directs government entities, within their respective powers, to adopt various measures aimed at providing guidelines and standards for responsible AI development and implementation according to their field of activity, and establishes obligations for companies developing certain AI models to provide information to various national agencies.

• Likewise, Article 16 of the Framework Convention adopted in March by the Council of Europe establishes that each Party shall assess the need for a moratorium, prohibition, or other appropriate measures concerning certain uses of AI systems when it considers those uses incompatible with respect for human rights, the functioning of democracy, or the rule of law.

Thus, for certain types of risk requiring special measures, it is suggested that consideration be given to:

1. Establishing a mandatory ex ante human rights impact assessment;

2. Establishing a duty to register the system in a publicly accessible State Register managed by the entity leading AI policy in the country;

3. Subjecting systems to prior authorization or certification according to the purpose or type of system involved;

4. Providing for periodic system audit mechanisms and possible submission of results to the entity responsible for reviewing them;

5. Complementing the rules ensuring transparency and explainability of AI systems used to make or support decisions, and human oversight of those systems' operation and outputs.

Furthermore, as emphasized by the interim report of the UN High-Level Advisory Body on AI, AI holds significant opportunities for humanity and the realization of people's rights through its potential to improve public service delivery, facilitate access to knowledge, education, healthcare, productive development, agriculture, etc.

Consequently, alongside addressing risks, it is recommended that consideration be given to promoting the development of AI systems aimed at the common good

by identifying purposes deemed to serve that objective and defining support and promotional measures, among others.

Implementing rights

From individuals' perspective, it is suggested that consideration be given to implementing certain rights through legal provisions, such as:

1. The right to know that one is interacting with an AI system;

2. The right to obtain basic information on how the system works and the expected outputs, through a natural person where necessary; and

3. Potentially, the right to appeal when a decision is made on the basis of that system, complementing the right to challenge personal assessments and the right to information provided for in personal data protection Law No. 18.331.

Equality and nondiscrimination

The current National Digital Citizenship Strategy[103] notes that the "impacts that may arise in the context of developing disruptive technologies such as artificial intelligence (AI) go beyond individuals, encompassing collective and social effects. In other words, one can speak of the systemic impacts of many of these digital technologies. For example, those linked to their effects on the future of work and democracy as key elements."

The research paper "Construyendo ciudadanía en entornos digitales. Perspectivas transversales de abordaje[104]," drawing on ECLAC's document "Ciudadanía digital en América Latina. Revisión conceptual de iniciativas,"

[103] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciudadania-digital-para-sociedad-informacion . Last accessed: 20/06/2024.

[104] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/construyendo-ciudadania-entornos-digitales-perspectivas-transversales-3 . Last accessed: 20/04/2024.

argues that the concept of the digital divide is now associated with gaps in the uses and benefits of digital technologies (arising from differences in socioeconomic status, age, gender, cultural capital, and digital skills).

That paper affirms the need to incorporate a perspective of digital inclusion or equality and to develop the skills needed to overcome limitations in access and capabilities, understand the rules of the game, and reflect on our own behavior.

Measures adopted in accordance with this document's recommendations should incorporate an approach that gives special consideration to the greater vulnerability faced by various groups in society, adopting frameworks and policies to address biases that may deepen inequalities, protect people from all forms of discrimination, and ensure that discriminatory outcomes are not carried over into AI systems and, where they occur, are detected and corrected.

Addressing the challenges facing democracies

Globally, concern is increasing about the impacts of disinformation and protecting the integrity of democratic processes and people's ability to form their opinions freely.

For example, in analyzing the impacts and risks involved in Artificial Intelligence, the interim report of the UN High-Level Advisory Body on AI[105] observes that some AI risks originate in the technical limitations of these systems, as with harmful biases or so-called hallucinations in generative AI, while others arise from human use, such as deepfakes, which "can pose a serious risk to social trust and democratic debate."

Resolution AG/RES. 3004 (LIII-O/23) on "Strengthening Democracy,"[106] adopted at the fourth plenary session on June 23, 2023, of the

[105] https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf. Last accessed: 20/06/2024.
[106] https://scm.oas.org/doc_public/SPANISH/HIST_23/AG08884S03.docx . Last accessed: 20/06/2024.

Organization of American States (OAS), resolved to instruct the General Secretariat to develop an inter-American agenda on emerging technologies, particularly concerning the ethical use of AI policies, algorithms, and data governance, within a set of measures aimed precisely at strengthening democracy.

International concern about these challenges was reflected in the latest update of the OECD AI Principles in 2024, one of whose objectives was precisely to reflect the growing importance of addressing these phenomena in the context of generative AI. In this regard, the principles propose "addressing AI-amplified disinformation while respecting freedom of expression and other rights and freedoms protected by applicable international law."[107]

While global efforts continue to understand this phenomenon and how to address it, we must consider measures not only involving restrictions—which are undoubtedly necessary—but also digital and information literacy, developing practical and fundamental skills for people's critical interaction in the digital environment.

As part of these measures, mechanisms can be promoted to identify information manipulation and AI-generated content, as well as policies to strengthen people's digital skills—in the latter case, supported in our country by the National Digital Citizenship Strategy.

Accessible, appropriate, and effective mechanisms and remedies

Our legal system has various public entities with human rights powers outside the justice system, such as the National Human Rights Institution and Ombudsperson's Office, the Personal Data Regulatory and Control Unit, and the Access to Public Information Unit, among others.

[107] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText. Last accessed: 20/06/2024.

To ensure that possible human rights violations arising from AI use are addressed through accessible, appropriate, and effective mechanisms and remedies, it is suggested that current mechanisms be analyzed to identify whether specific powers of existing bodies need strengthening or new necessary mechanisms need to be created, as well as how their powers should be coordinated.

Regulating the development, use, and procurement of AI in the public sector

The Ibero-American Charter on Artificial Intelligence in Public Administration, adopted in 2023 within CLAD, has "as its main objective to promote a shared model for developing Artificial Intelligence from and within public administrations in the Ibero-American sphere."[108] As a basis for this common framework, Chapter 3 proposes general principles for AI in Public Administration: human autonomy; transparency, traceability, and explainability; accountability, responsibility, and auditability; safety and technical robustness; reliability, accuracy, and reproducibility; trust, proportionality, and harm prevention; privacy and personal data protection; data quality and integrity; equity, inclusion, and nondiscrimination; human-centeredness, public value, and social responsibility; and sustainability and environmental protection.

In identifying key dimensions for AI adoption in Public Administration, the Charter proposes, as a component of national strategies, that "national legislation should address issues that ensure algorithmic systems are safe, transparent, traceable, nondiscriminatory, and environmentally sustainable. Personal data protection legislation should also be adapted, as should rules on the use and reuse of public data generally. In addition, it must be ensured that Artificial Intelligence systems are supervised by humans rather than being completely autonomous, minimizing potential harm and eliminating extreme-risk situations. Alongside this, robust cybersecurity mechanisms must be established to maintain data integrity and the

[108] https://clad.org/wp-content/uploads/2023/10/Borrador-CIIA-V1-ES-08-2023.pdf. Last accessed: 20/05/2024.

inviolability of technological infrastructure. Finally, it should be ensured that public algorithms are transparent and nonproprietary or not subject to patents, promoting technological infrastructure based on open architectures."

These principles are shared with the AI Strategy currently under review, which also emphasizes that "every technological solution using AI must respect Human Rights, individual freedoms, and diversity."

In light of the path Uruguay has already followed within its national digital policy, which is human-centered by definition, it is recommended that regulatory instruments for the public sphere continue to be strengthened by incorporating those components of the new AI Strategy to be adopted in 2024 relating specifically to the use and development of these technologies in that sphere.

In this regard, one specific measure to consider is requiring human rights impact assessments before public entities acquire, develop, and/or use AI systems in areas determined to pose a potentially high risk to people's rights. In light of the above, and in particular, it is recommended that regulation of the development, procurement, and application of surveillance systems for public security purposes be analyzed as part of the package of measures under consideration.

In addition, since the Data and Cybersecurity Strategies are being developed, it will also be relevant to consider the guidelines defined in them to identify elements requiring statutory regulation that complements preexisting general frameworks.

Training and education for AI

As mentioned when considering the thematic area of work and training for AI, this report identifies concrete measures specifically aimed at training people and strengthening their skills.

Other aspects of AI's impact on the world of work will require broader developments and an open discussion involving the State, employers, workers, and trade unions, to reach agreements that enhance the benefits of applying this technology and mitigate adverse effects.

Nevertheless, from the perspective of this report, the following recommendations can be made:

1. promote training programs through technical, tertiary, and university educational institutions on AI and data management, in collaboration with business associations, trade unions, and other groups;

2. establish specific support or particular benefits for companies that run AI-oriented courses for their workers and management teams in predefined sectors;

3. assess requiring employers to train workers who must apply or may be affected by AI systems before those systems are implemented, in predefined sectors.

Summary of recommendations on ethics, human rights, and democracy	
Recommendations aimed at possible amendments or regulatory updates	- Explicitly establish the principles enumerated in Article 74 of Law 20.2012 as guiding principles for national AI policy and its implementation. - Define risks that are unacceptable to society; and identify uses that represent a high risk and require special

	measures, also defining those measures. - Assess the adoption of measures aimed at combating disinformation and protecting the integrity of democratic processes and people's ability to form their opinions freely. - Analyze strengthening existing mechanisms or creating new mechanisms to address human rights violations arising from AI systems. - Regulate instrumental rights in favor of transparency, explainability, and the ability to challenge decisions.
Other recommended initiatives	- Establish specific rules on the development, use, and procurement of AI in the Public Sector. - Assess regional and international cooperation instruments in this field. - Analyze adopting measures with the aim of continuing to address digital divides and strengthening the development of digital citizenship.

	- Promote initiatives using AI for the good of society. - Promote training, especially for workers, in collaboration with business associations, trade unions, and other groups, and establish specific support or particular benefits for companies that provide AI-oriented courses in predefined sectors. - Assess requiring employers to train workers who must apply or may be affected by AI systems, before those systems are implemented, in predefined sectors.

Responsible innovation

Legal certainty in matters of civil liability and intellectual property

The analyses conducted show a need to review the national civil liability regime, since it does not seem reasonable to rely on interpretations or gap-filling applications of rules that do not correspond to current reality, so as to provide greater certainty to developers, users, and other system actors.

It is suggested that the following alternatives be considered: i. work with competent entities to determine suggested minimum contents for contracts between those making systems available and those using them. In this regard, personal data protection rules on proactive accountability may be considered as precedents; ii. establish an

analysis committee specifically focused on a possible reform of the civil liability regime in this field.

Legal certainty is also associated with an adequate system for assigning rights in cases of creations involving an AI system in some way.

This Agency suggests:

1. In the case of AI-generated works without direct human intervention, include an indication of this circumstance in the work itself and, in some cases, a reference to the system used to create the work. Exceptions could be proposed for domestic use or other purposes;

2. Initiate a consultation process on how works generated exclusively by AI will be treated. There is currently no consolidated view that these works can be attributed to such systems, so consultation should involve all stakeholders, taking into account not only aspects associated with assigning ownership but also the corresponding economic compensation;

3. Consider defining the system to apply to AI-assisted works, for example by attributing ownership to the person directing the creative process of the completed work;[109]

4. Reaffirm that the scope for processing the data used by these systems to generate new works will depend on current legislation—Article 35 of Law No. 9.376 and Article 9 bis of Law No. 18.331.

Regarding other intellectual property aspects, it is suggested that consideration be given to:

[109] Various alternatives on this subject can be found in MANTEGNA. Op. cit. P. 309.

1. Regarding registration, continuing the process already initiated by Law No. 20.212 and assessing the possibility of communication between this register, other registers, and the publication of public software indicated in Article 7 of Decree No. 44/015 for public entities;

2. Expanding the scope of Article 2 of Law No. 19.179 to computer programs (source or object programs), compilations of data or other materials in any form that, by reason of the selection or arrangement of their contents, constitute intellectual creations, and the expression of ideas, information, and algorithms formulated in original sequences appropriately ordered for use by an information-processing or automatic-control device.

Infrastructure and cybersecurity

This report has already raised the need for adequate infrastructure for AI development and the State's important role in achieving that objective.

Following the OECD report surveyed when analyzing this area, it seems necessary to adopt measures associated with reviewing computing capacity in the public and private sectors; considering the number, capacity, and availability of existing data centers; defining data management standards; analyzing processing capacity and hardware needs in the country; determining potential demand for AI processing; distinguishing AI processing needs; providing education and training; and mapping and analyzing supply chains.

It is considered necessary to create or update regulatory instruments that facilitate the procurement, operation, and maintenance of this infrastructure, to promote capacity management that adapts rapidly to the exponential advances shown by this technology in particular.

For the purposes of this report, whose objective is to provide recommendations to the Legislative Branch, the analyses conducted must also be directed toward determining whether current regulatory provisions are aligned with needs in this field.

From this perspective, this Agency wishes to emphasize that extensive legislation and regulation exists on aspects such as data exchange, cybersecurity, information processing—personal and nonpersonal—telecommunications networks, and public procurement, among others. It is nevertheless possible to recognize the difficulty posed by the existing fragmentation of rules, so organizing these provisions through a consolidated text or similar instruments could be relevant.

Cybersecurity in particular has been regulated since Agesic's creation. Its importance was recently highlighted through the systematization of various provisions and the updating of the Agency's powers and the obligations of public entities generally and certain private entities specifically, in several articles of Law No. 20.212.

The results of the process of developing the National Cybersecurity Strategy, and the strategic objectives arising from that process—as repeatedly mentioned in this report—will be a central input for determining new measures contributing to a secure ecosystem for developing AI and other technologies.

Regarding infrastructure, and considering the contributions received throughout the preparation of this report, Agesic proposes promoting dialogue with other stakeholders on this aspect, suggesting the following alternatives:

1. Add helping to define recommendations as a specific task of the Public Information Technology Advisory Council;

2. Coordinate actions with the Governance Committee for Cross-Cutting Processes and Solutions created by Decree No. 431/022 of December 27, 2022,

3. Define, together with the State Procurement Regulatory Agency (ARCE), specific requirements for procurement associated with AI system development.

Particularly regarding the legal basis for secure data exchange, it is recommended to enable private entities to use the Interoperability Platform created by Decree No. 178/013 to consume services, and to assess amending Decree No. 92/014 to clarify in law the scenarios associated with using cloud provider services.

A comprehensive perspective on infrastructure and processes for digital transformation

A comprehensive perspective is needed, rethinking how the use of State infrastructure and processes is approached and facilitating the deployment of technology such as AI.

In this regard, the aim should be to promote the use of AI as an opportunity to improve public services, State efficiency, and data-based decision-making.

Proposals such as Digital Public Infrastructure (DPI) enable a comprehensive approach to carrying out more efficient digital transformation processes. An initiative called “DPI Safeguards” was recently launched. It aims to share lessons learned by creating a framework to minimize risks at the technical, regulatory, and organizational levels and, ultimately, an environment for the safe, inclusive, practical, and adaptable implementation of DPI.[110]

From this perspective, improving State infrastructure that supports technology such as AI must benefit innovation and

110 The initiative’s interim report can be accessed at: https://safedpi.gitbook.io/safeguards/working-group-documents/reports . Last accessed: 22/06/2024.

research in the public and private sectors, contributing to the country's economic and social development.

Following this logic, the aim should be for infrastructure components, where appropriate, to be used by stakeholders in the innovation, scientific, and entrepreneurial ecosystem, giving special consideration to their different characteristics.

Environmental impacts of infrastructure

Although the environmental aspect was not among this report's central thematic areas, some reference to the environmental impacts of rapid technological development in general and AI in particular is unavoidable.

AI use can generate major benefits in mitigating climate change impacts, and various initiatives, including at the national level, indeed promote developments that tackle this problem.[111]

However, negative impacts are associated with extracting materials to create hardware components, water use, and energy consumption, among other things, making it necessary to bring relevant authorities and stakeholders into this discussion.

UNESCO's Recommendation on the Ethics of AI clearly states the need for everyone involved in the AI system lifecycle to respect national and international norms and practices relating to precaution, designed to protect and restore the environment and ecosystems and support sustainable development.

CLAD includes sustainability and environmental protection among the principles of its Charter, advocating the use of technologies that are environmentally sustainable and nonpolluting in their energy use based on reusable materials and

111 See, for example: https://www.anii.org.uy/apoyos/innovacion/309/fondo-de-investigacion-e-innovacion-en-cambio-climatico/ . Last accessed: 20/06/2024.

devices and renewable energy sources, all in line with the SDGs.

In light of the above, the environmental perspective must be present in every initiative associated with developing AI infrastructure.

Support measures

Support measures are numerous and should focus not on promoting technology itself, but on objectives to be achieved through it. The analysis mentioned some measures arising from current rules and the entities responsible for carrying them out.

In January this year, the European Commission launched a package of measures supporting European startups and small and medium-sized enterprises in developing safe AI. The package includes establishing AI factories with supercomputers accessible to SMEs, support for using general-purpose AI models, creating an AI office within the Commission, financial support through various programs, and developing data spaces, among other measures.

The process of developing the strategies led by this Agency repeatedly identifies the need for infrastructure development to include instruments such as tariff benefits, tax exemptions, and incentives for importing components and exporting services from our country, among others.

Some support measures, such as incentives, exemptions, and other benefits already provided for in current rules, can be directed or redirected toward promoting activities that, thanks to AI, may benefit the economy, society, and ultimately people.

Regarding support for AI in the Public Sector, as early as 2021 the World Bank[112] suggested establishing a central AI innovation hub in government,

[112] https://documents1.worldbank.org/curated/en/746721616045333426/pdf/Artificial-Intelligence-in-the-Public-Sector-Summary-Note.pdf . Last accessed: 21/06/2024.

similar to the UIH program our country currently has. In that document, the World Bank states that investment should be directed toward human capital and digital infrastructure, prioritizing research, entrepreneurship, foundational digital technologies, and digital skills.

The objectives set in this regard are linked, among other things and in this Agency's view, to the objectives already defined in the Uruguay Digital Agenda 2025 and those arising from the development of the National Data and Cybersecurity Strategies and the updating of the National Artificial Intelligence Strategy.

Beyond financial support alternatives grounded in current rules, other measures promote responsible AI use, including regulatory sandboxes and data spaces, which enable safe experimentation, a bounded liability framework, and multistakeholder collaboration (public sector, private sector, academia, and civil society).

International cooperation in this field should also continue, along with signing agreements that improve the country's position in safe AI innovation and research, as with the signing of the recent Patent Cooperation Treaty.

Summary of recommendations for promoting AI innovation	
Recommendations aimed at possible amendments or regulatory updates	- Promote extending the task provided for in Article 74 of Law No. 19.149 of October 24, 2013, to the entire Administration.

	- Expand the scope of Article 2 of Law No. 19.179 of December 27, 2013.
Other recommended initiatives	- Establish an interdisciplinary analysis committee for a possible reform of the civil liability regime in this field. - Analyze, together with competent bodies, proposals for minimum contractual provisions on the scope of liability in agreements between developers, users, and other actors in AI systems. - Regarding Intellectual Property, promote discussion of the alternatives for AI-generated works without direct human intervention and for AI-assisted works. - Continue the registration process initiated by Law No. 20.212 of November 6, 2023, and assess communication between this register, other registers, and the publication of public software. - Assess adding, as a specific task of the Public Information Technology Advisory Council, collaboration with Agesic in defining the recommendations needed for adequate AI infrastructure development at the national level.

	- Consider preparing an analysis of current infrastructure comprehensively in this field, giving particular consideration to public investment measures and the promotion of private investment. - Assess defining a new cloud-use policy in relation to that established in Decree No. 92/014 of April 7, 2014. - Establish collaboration among entities responsible for promoting AI infrastructure initiatives, particularly including the environmental perspective. - Consolidate the tools needed to carry out the actions defined in the National Cybersecurity Strategy. - Finalize the proposed implementing regulations for controlled testing environments and other measures to promote innovation, and implement them. - Assess, together with MEF, MIEM, ANII, and other competent public entities, the necessary support measures.

Annex 1: National background

Mapping national legislation

In preparing this report, a set of statutory and regulatory provisions was taken into account, with a focus strictly on aspects linked to the defined thematic areas and their relationship with AI.

The following table presents the provisions identified, grouped by associated thematic area, with a brief description of each.

AI institutional framework

Applicable provisions	Summary of content
Article 74 of Law No. 20.212 of 6 November 2023	Places Agesic in charge of designing and developing a national data and AI strategy. The final paragraph also expressly establishes that it will make specific recommendations to public- and private-sector entities for the development and implementation of the aforementioned artificial intelligence systems and for overseeing compliance, without prejudice to the powers of the URCDP and other public entities within their respective spheres of action.
Article 34 of Law No. 18.331 of 11 August 2008, as amended by Article 63 of Law No. 20.075 of	Includes among the URCDP's tasks establishing the criteria and procedures to be observed by controllers and processors in the automated processing of personal data indicated in Article 16 of Law No. 18.331.

20 October 2022.	

Data governance

Applicable provisions	Topic	Summary of content
Law No. 18.331 of 11 August 2008, amendments and related provisions, and No. 19.670 of 15 October 2018. Implemented by Decrees No. 414/009 of 31 August 2009 and 64/020 of 17 February 2020.	Personal Data	Establishes the forms of personal data processing in the public and private sectors, associated with a set of principles.
Law No. 18.381 of 17 October 2008. Provision implemented by Decree No. 232/010 of 2 August 2010.	Public Information	Establishes the public nature of information held by the State, as well as the exceptions.
Articles 157 to 160 of Law No. 18.719	Interoperability and exchange	Establishes conditions for interoperability and the exchange of public and private information under the terms of the regulations. Provision implemented

of 27 December 2010		by Decree No. 178/013 of 11 June 2013.
Decree No. 259/012 of 13 August 2012	Open data and Open Government	Uruguay adheres to the “Open Government Declaration” of the “Open Government Partnership,” and the first action plan is established, succeeded by subsequent plans.
Article 82 of Law No. 19.355 of 19 December 2015	Open Data and Open Government	Establishes the obligation of public bodies to publish the information covered by Article 5 of Law No. 18.381 in open data format. Provision implemented by Decree No. 54/017 of February 20, 2017.
Article 76 of Law No. 19.355 of 19 December 2015 as amended by Article 2 of Law No. 19.670 of 15 October 2018	Interoperability and exchange	Establishes the obligation of public bodies not to request certificates, attestations, certified copies, or other documentation of a similar nature issued by another public entity when the information contained in those documents can be accessed through computer systems provided by the competent entities. Provision implemented by Decree No. 353/023 of November 9, 2023.
Decree No. 357/016 of 7 November 2016	Open Data and Open Government	Creates the Open Government Working Group, comprising one representative from each of the following bodies: Agesic, OPP, UAIP. MEF, MRREE, MIEM, and INE. Its tasks are also established.

Applying AI principles

Provisions	Summary of content
Article 74 of Law No. 20.212 of 6 November 2023	Places Agesic in charge of designing and developing a national data and AI strategy. The second paragraph states that “the strategy must be based on principles of equity, nondiscrimination, responsibility, accountability, transparency, auditing, and safe innovation, respecting human dignity, the democratic system, and the republican form of government. The personal data protection principles included in Law No. 18.331 of August 11, 2008, will form part of that strategy.”
Article 5 of Law No. 18.331 of 11 August 2008.	Establishes the following personal data protection principles, which Article 74 incorporates into the AI Strategy: legality, accuracy, purpose, prior informed consent, data security, confidentiality, and (proactive) accountability.

Intellectual property

Applicable provisions	Summary of content
National Constitution, Art. 33	Establishes that intellectual work and the rights of authors, inventors, and artists shall be recognized and protected by law

Law No. 9.739 of 17 December 1937, amended by Laws No. 17.616 of 10 January 2003, 19.857 of 23 December 2019 and 20.212 of 6 November 2023. Implemented by Decrees No. 154/004 of 3 May 2004, 295/017 of 16 October 2017, 404/023 of 12 December 2023	Recognizes authors' ownership rights over the products of their thought, science, and art. The law's protection includes computer programs or software and data compilations whose content constitutes an intellectual creation. It provides for rights, a specified protection term, lawful and unlawful conduct, and possible sanctions. Works are registered at the National Library, except for computer programs, compilations of data or other materials constituting intellectual creations, expressions of ideas, information, and algorithms formulated in original ordered sequences for use by an information-processing or automatic-control device, and transfers of economic rights over these works, which are registered in the DNPI Software Register.
Law No. 14.910 of 19 July 1979	Approves the conventions for the protection of industrial property, for the protection of literary and artistic works, and for intellectual property (Paris and Berne Conventions).
Law No. 16.671 of 13 December 1994	Approves the agreements resulting from the Uruguay Round of Multilateral Trade Negotiations, contained in the Final Act signed in Marrakesh on April 15, 1994, particularly the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).

Law No. 17.011 of 25 September 1998. Implemented by Decree No. 34/999 of 3 February 1999.	Regulates the protection granted to trademarks, defined as signs capable of distinguishing the products or services of one natural person or legal entity from those of another. Establishes types of trademarks, rights, protection terms, registration, and absolute and relative grounds for invalidity regarding certain signs. Also regulates trade names, geographical indications, appellations of origin, and indications of source.
Law No. 17.164 of 2 September 1999. Implemented by Decree No. 11/000 of 13 January 2000.	Regulates rights and obligations concerning invention patents, utility models, and industrial designs. As in the previous case, it establishes rights, grounds for invalidity, protection terms, registration, and possible sanctions.
Law No. 18.036 of 20 October 2006.	Approves the World Intellectual Property Organization (WIPO) Copyright Treaty and the Agreed Statements concerning the WIPO Copyright Treaty.
Law 18.253 of 20 February 2008	Approves the World Intellectual Property Organization Performances and Phonograms Treaty and the agreed statements concerning it.
Law No. 19.179 of 27 December 2013. Implemented by Decree No. 44/015	Regulates the format for processing and storing digital information in certain public and private entities.

of 30 January 2015.	

Infrastructure and cybersecurity

Applicable provisions	Summary of content
Law No. 17.296 of 21 February 2001, Articles 70 to 94 bis, as amended by Articles 143 and 418 of Law No. 18.719 of 27 December 2010 and 256 to 273 of Law No. 19.889 of 9 July 2020, among others. Implemented by Decree No. 212/001 of 4 May 2001.	Establishes the telecommunications powers of the Communications Services Regulatory Unit (URSEC)—currently a decentralized service—the Ministry of Industry, Energy and Mining (MIEM), and particularly the National Directorate of Telecommunications and Audiovisual Communication Services (DINATEL). URSEC's principal tasks were established as regulating and overseeing activities and sectors relating to telecommunications and postal services. Policymaking belongs to MIEM.
Law No. 18.331 of 11 August 2008. Implemented by Decrees No. 414/009 of 31 August 2009 and	Establishes the general framework for communicating personal data between public- and private-sector entities, as well as the basic requirements to be met to ensure the security of personal data processing. Decree No. 64/020 of February 17, 2020, in particular recommends adopting certain security measures in Articles 3 and

64/020 of 17 February 2020.	4, expressly suggesting adoption of Agesic's Cybersecurity Framework.
Law No. 18.719 of 27 December 2010, Article 149, as amended by Article 84 of Law No. 19.924 of 18 December 2020.	Entrusts Agesic with leading policies, methodologies, and best practices and regulating information security and cybersecurity nationally, as well as overseeing and auditing compliance and providing support during their implementation in all public entities and in private entities associated with the country's critical services or sectors.
Law No. 18.719 of 27 December 2010, Articles 157 to 160. Implemented by Decree No. 178/013 of 11 June 2013.	Establishes rules for interoperability between public bodies. Defines Agesic's role and powers in this field. The implementing regulations establish an interoperability platform managed by this agency for information exchange between public entities.
Decree 92/014 of 7 April 2014	For the Central Administration, establishes an obligation for secure data centers to be located within national territory, except those that do not pose a risk to the body. An Annex also establishes physical security conditions that public entities must implement. Exceptions may also be considered, and Agesic is competent to grant them.
Law No. 19.924 of 18 December 2020, Articles 372	Abolishes the National Secretariat for Science and Technology and changes, within the Ministry of Education and Culture, the name and powers of the Directorate

to 375, which abolish the entity created by Law No. 19.355 of 19 December 2015, Article 34, whose powers were regulated by Decree No. 324/017 of 10 November 2017.	for the Development of Science and Knowledge, which is renamed the National Directorate for Innovation, Science and Technology. The aforementioned Secretariat's implementing regulations had included among its powers proposing science, technology, and innovation policies; promoting greater development of connectivity and telecommunications capabilities; and proposing infrastructure in science, technology, and innovation in strategic areas for the country's development.
Law No. 20.075 of 20 October 2022, Article 461, implemented by Decree No. 216/023 of 17 July 2023	Provides a budget allocation for the research, innovation, and experimental development program to promote science, technology, and innovation projects. The cited decree regulates the creation of the Uruguay Innovation Hub Program within the National Research and Innovation Agency (ANII). Its instruments include, for example, establishing open laboratories through financial and operational support.
Law No. 20.212 of 6 November 2023, Articles 78 to 84.	Although many rules regulate cybersecurity aspects, at both statutory and regulatory levels, these articles' contribution to the field stands out: they impose certain statutory obligations on public entities and private entities associated with the country's critical sectors or services, as well as instruments for Agesic to monitor and oversee compliance. They also establish the composition of two

	Agesic advisory bodies on cybersecurity and define the foundations for a National Strategy.

Work and training for AI

Applicable provisions	Summary of content
Law No. 18.046 of 24 October 2008. Implemented by Decree No. 52/021 of 8 February 2021.	Law creating the National Institute for Employment and Vocational Training (INEFOP). Its tasks include advising on the definition of training and education policies to create and improve employment.
Law No. 18.437 of 12 December 2008. Implemented by Decrees No. 334/009 of 20 July 2009 and 294/013 of 11 September 2013.	Declares the promotion of the enjoyment and effective exercise of the right to education as a fundamental human right to be in the general interest.
Law No. 19.121 of 20 August 2013.	Regulates the Public Official Statute of the Central Administration, promoting public officials' training, which is considered fundamental for access to positions and promotion.

Decree No. 340/018 of 22 October 2018.S	Creates the National Occupational Certification Commission within INEFOP.
Law No. 19.973 of 13 August 2021. Implemented by Decree No. 308/021 of 10 September 2021.	Establishes employment policies to encourage paid work for young people, adults, and persons with disabilities, including their training and education.

Civil liability and consumer rights

Applicable provisions	Summary of content
Civil Code	The rules on liability are set out in Articles 1246 et seq. of the Civil Code, providing for contractual and noncontractual liability as mentioned and, with exceptions, a fault-based liability regime for all types. Article 1330 should be considered in particular in this regard.
Law No. 17.250 of 11 August 2000. Implemented by Decree No. 244/000 of 23 August 2000.	In the specific case of consumer relations, a fault-based liability regime is also provided for. Establishes certain specific liability provisions in Articles 34 to 36.

Support measures

Applicable provisions	Summary of content
Law No. 16.906 of 7 January 1998. Implemented by Decree No. 92/998 of 21 April 1998.	Investment and industrial promotion law.
Article 461 of Law No. 20.075 of 20 October 2022	Allocates an annual sum of $400,000,000 (four hundred million Uruguayan pesos), charged to General Revenues, to promote science, technology, and innovation projects approved by the Ministry of Economy and Finance, with advice from the Office of Planning and Budget, upon proposals from the National Research and Innovation Agency.
Decree No. 216/023 of 17 July 2023	Creates the Uruguay Innovation Hub Program to promote the entrepreneurial and innovation ecosystem.
Law No. 20.121 of 23 August 2023. Implemented by Decree No. 360/023 of 14 November 2023.	Law concerning incentives for information technology technicians and professionals to settle in Uruguay

Article 75 of Law No. 20.212 of 6 November 2023	Promotes the creation of controlled testing environments for projects aimed, among other things, at building systems that apply AI.

Annex 2: International background

International principles and recommendations

Attention to artificial intelligence systems has become ubiquitous on the agendas of international organizations and forums, encompassing a wide variety of issues and fields: from how Artificial Intelligence can help achieve the Sustainable Development Goals to debates about its military applications.

Amid this diversity, however, a common starting point can be identified in several completed or ongoing international efforts toward artificial intelligence governance: an emphasis on building governance aimed at enhancing the opportunities and benefits of artificial intelligence for humanity, ensuring equitable access to those benefits, while addressing the challenges and risks arising from these technologies.

To this end, as emerges from the precedents reviewed below, many ongoing efforts emphasize the need for an approach that places people at the center; protects human rights, democracy, and the rule of law; is grounded in international law and international human rights law; promotes safe and trustworthy artificial intelligence systems developed and used ethically; and promotes innovation to harness AI's potential for humanity's benefit and sustainable development.

The objective of this Annex to the Report is to present a summary of guiding principles and recommendations emerging internationally that seek to guide States' actions in formulating their legislation, policies, or other AI-related instruments, based on the review of international precedents conducted in preparing this report. These principles and recommendations must be understood as complementing States' international human rights obligations under current international law.

The precedents reviewed were selected according to their international relevance and impact on Uruguay and are presented chronologically in each subsection.

United Nations

Within the United Nations, a process toward international Artificial Intelligence governance is underway, promoted by the Secretary-General, while negotiations are also underway for the Global Digital Compact, which would include a specific chapter on Artificial Intelligence. The Compact is expected to be adopted at the Summit of the Future to be held next September. The ongoing processes build, among other things, on the milestones within the United Nations indicated below in this section.

UNESCO Recommendation on the Ethics of AI (2021)

The Recommendation on the Ethics of Artificial Intelligence was adopted in November 2021 by the General Conference of the United Nations Educational, Scientific and Cultural Organization (UNESCO).[113] Its purpose is to guide States in formulating laws and policies on artificial intelligence. To this end, the Recommendation promotes a set of values,[114] principles, and policy actions.

The text analyzes “the profound and dynamic positive and negative impacts of artificial intelligence” on societies, the environment, and human life, and states that “taking account of risks and ethical concerns should not impede innovation and development,” but should instead stimulate

[113] UNESCO. Recommendation on the Ethics of Artificial Intelligence, adopted on November 23, 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa . Last accessed:29/4/2024.

[114] The values listed are: Respect, protection, and promotion of human rights, fundamental freedoms, and human dignity. The flourishing of the environment and ecosystems. Ensuring diversity and inclusiveness. Living in peaceful, just, and interconnected societies.

research and innovation conducted ethically and based on human rights.[115]

In 2023 Uruguay endorsed UNESCO's Recommendation, thereby reinforcing the country's commitment to its implementation within the new Artificial Intelligence Strategy and the first National Data Strategy.116 For these reasons, and given its importance as a reference framework in preparing this Report, a summary of the Recommendation's 10 guiding principles follows.

UNESCO principles[117]

Principle	Scope
Proportionality and do no harm.	The Recommendation proposes ensuring the application of risk assessment procedures and measures to prevent harm to human beings, the environment, and ecosystems. It should also be ensured that processes related to the lifecycle of AI systems are confined to legitimate purposes or objectives. The Recommendation states that AI systems should not be used for social scoring or mass surveillance.
Safety and security.	The Recommendation indicates that safety and security risks should be identified,

[115] Ibid. Preamble.

[116] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-recomendacion-etica-inteligencia-artificial-unesco . Last accessed 09/02/2024.

[117] Based on paragraphs 25 to 47 of UNESCO's Recommendation on the Ethics of AI.

	prevented, and eliminated throughout the AI lifecycle.
Fairness and nondiscrimination	The Recommendation emphasizes that an inclusive approach should be adopted to ensure that the benefits of AI technologies are available and accessible to everyone, taking into account the specific needs of different groups. It also maintains that digital divides within and between countries, and biases throughout the lifecycle of AI systems, should be addressed.
Sustainability	The Recommendation emphasizes the need to assess the impacts of AI technologies on sustainability, that is, to continuously assess the human, social, cultural, economic, and environmental effects involved in this technology.
Right to privacy and data protection.	The Recommendation proposes that privacy must be respected, protected, and promoted throughout the lifecycle of AI systems. It maintains that algorithmic systems require adequate privacy impact assessments and indicates that appropriate data protection frameworks and data governance mechanisms should be established in accordance with a multistakeholder approach.
Human oversight and determination	The Recommendation maintains that Member States should ensure that, at any stage in the AI system lifecycle, it is always

	possible to attribute ethical and legal responsibility to natural persons or existing legal entities.
Transparency and explainability	The Recommendation affirms that people should be fully informed when a decision is based on AI algorithms or made from their outputs, particularly when it affects their rights, and proposes that adequate mechanisms should exist to review and amend the decision. It maintains that AI actors should inform users adequately and in a timely manner when a product or service is provided directly by, or with the help of, an AI system. The Recommendation defines explainability as making AI system outputs intelligible and providing information about them. It also refers to the intelligibility of the input, output, and operation of each algorithmic component and how it contributes to system outcomes (traceability).
Responsibility and accountability	The Recommendation proposes that AI actors and Member States should respect, protect, and promote human rights and foster the protection of the environment and ecosystems, assuming their respective ethical and legal responsibility. To this end, appropriate oversight, impact assessment, auditing, and due diligence mechanisms should be developed, including protection for

	whistleblowers, to ensure accountability for AI systems and their impacts throughout their lifecycle.
Awareness and literacy.	The Recommendation emphasizes that public awareness and understanding of AI technologies, their operation, and impacts should be promoted through open and accessible education, civic engagement, digital skills, AI ethics training, and media and information literacy.
Adaptive and multistakeholder governance and collaboration.	The Recommendation proposes that ensuring an inclusive approach to AI governance requires guaranteeing the participation of different stakeholders (governments, intergovernmental organizations, academia, civil society, the private sector, and human rights institutions, among others).

To implement these principles, UNESCO's Recommendation promotes specific actions for States and other actors. Based on this report's purpose, the following stand out:

- Ensure that AI governance mechanisms are inclusive, transparent, multidisciplinary, and involve multiple stakeholders.

- Ensure that AI system legislation complies with Member States' human rights obligations

and promotes human rights and fundamental freedoms throughout these systems' lifecycle.

• Develop or adapt, as appropriate, regulatory frameworks to achieve accountability and responsibility for the content and outputs of AI systems at different stages of their lifecycle. These frameworks should take into account that responsibility and accountability must ultimately always rest with natural persons or legal entities, that AI systems themselves should not be granted legal personality, and should incorporate the principle of human oversight.

• Have frameworks to protect personal data and ensure effective and independent oversight within a data governance mechanism.

• Establish clear transparency and explainability requirements for AI systems to help ensure their trustworthiness throughout their lifecycle. These requirements should encompass the design and implementation of impact assessment mechanisms that take into account the nature of the application domain, intended use, recipients, and feasibility of each particular AI system.

• Ensure compliance with environmental laws, policies, and practices by all AI actors.

• Allocate specific public budget funds to finance gender-responsive plans, ensure that national digital policies include a gender action plan, and develop relevant policies.

• Promote general awareness programs on AI advances, particularly data and the opportunities and challenges presented by AI technologies, AI systems' impacts on human rights, including children's rights, and their implications. These programs should be accessible to both technical and nontechnical groups.

• Promote research and encourage private-sector companies to facilitate the scientific community's access to their data for research.

• Ensure that AI actors respect and promote freedom of expression and access to information regarding automatic content generation, moderation, and preservation, through appropriate frameworks, including regulatory ones, that foster transparency, ensure users have access to diverse viewpoints, and provide processes for promptly notifying users of the reasons for content removal or other treatment, as well as appeal mechanisms allowing users to seek redress.

• Assess and address AI systems' impact on labor markets and the implications for each country's educational needs.
• Promote and support other actors' efforts to adapt training programs and strategies to future implications for work and industry needs, including those of small and medium-sized enterprises, and implement upskilling and reskilling programs and explore social protection programs for those unable to retrain.

• Adopt appropriate measures to ensure market competitiveness and consumer protection, considering possible measures and mechanisms at national, regional, and international levels to prevent abuses of dominant market positions, including monopolies, in relation to AI systems throughout their lifecycle.

Preliminary principles and recommendations of the High-level Advisory Body on Artificial Intelligence (2023).

This precedent arises from the "Interim Report: Governing AI for Humanity" prepared by the United Nations Advisory Body on Artificial Intelligence and published in December

2023. [118] The body was created that same year at the Secretary-General's initiative to address AI risks, opportunities, and international governance, and consists of independent experts.[119]

The advisory body's report describes a set of opportunities and risks involved in AI systems and analyzes how the global governance deficit results in benefits and risks being distributed unequally around the world. It emphasizes the need to identify and address AI risks, including building consensus on which risks are unacceptable and how they can be prevented or anticipated.

The Advisory Body's recommendations emphasize the need for global international AI governance based on five guiding principles, summarized below.

Principles for international AI governance promoted by the UN AI Advisory Body

Principle	Scope
AI should be governed inclusively, by and for the benefit of all.	The report proposes that AI should be governed so that all people and all countries, regardless of their level of development, can benefit from it.
AI should be governed in the public interest.	The report maintains that binding rules consistently applied by

[118] https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf . Last accessed:29/4/2024.

[119] The full membership list is available at the following link: https://www.un.org/en/ai-advisory-body/members Last accessed:29/4/2024.

	Member States are needed to ensure that public interests prevail.
AI governance should be built alongside data governance and the promotion of data commons.	The report proposes considering how data are collected, stored, and shared to ensure that data are shared and used in a way that benefits society as a whole.
Artificial intelligence governance should be universal, networked, and rooted in adaptive multistakeholder collaboration.	The report emphasizes that any artificial intelligence governance effort should prioritize universal endorsement by different Member States and stakeholders and inclusive participation by the Global South, considering different cultural contexts.
AI governance should be anchored in international norms and commitments.	The report advocates that AI governance should be grounded in the UN Charter, international human rights law, and other agreed international commitments such as the Sustainable Development Goals.

It has been announced that the Advisory Body's final report would be presented in mid-2024 and would constitute a fundamental input for defining the specific Artificial Intelligence commitments and actions that Member States will undertake under the Global Digital Compact in September

2024. Uruguay has participated in the consultations promoted by the AI Advisory Body and is participating in the ongoing negotiations on the Global Digital Compact.

UN General Assembly Resolution A/RES/78/265 (2024)

UN General Assembly Resolution 78/265, “Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development,” [120] was adopted on March 21 this year after being co-sponsored by more than 120 States, including Uruguay.

The Resolution covers “artificial intelligence systems in the nonmilitary domain, whose lifecycle includes predesign, design, development, evaluation, testing, deployment, use, sale, procurement, operation and decommissioning.”

The text defines the characteristics distinguishing safe and trustworthy AI systems as follows: “(…) human-centric, reliable, explainable, ethical, inclusive, fully respecting the promotion and protection of human rights and international law, privacy-preserving, sustainable-development-oriented and responsible.”[121]

The Resolution affirms[122] “that human rights and fundamental freedoms must be respected, protected and promoted throughout the lifecycle of artificial intelligence systems,” and “calls upon all Member States and, where appropriate, other stakeholders, to refrain from or cease using artificial intelligence systems that are impossible to operate in compliance with international law or that pose undue risks to the enjoyment of human rights.”

[120] UN – General Assembly. Resolution adopted by the General Assembly on March 21, 2024. 78/265. Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development. A/RES/78/265. Available at: https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=hxXvAKO8RS5xFkIlcb&fe=true . Last accessed:29/4/2024.

[121] Ibid. Recitals.

[122] Ibid. Paragraph 5.

The UN resolution encourages Member States to promote safe and trustworthy artificial intelligence systems through various means, including:

• Promoting the development and implementation of national regulatory and governance approaches and frameworks, consistent with their respective policies and priorities and their obligations under international law, to support responsible and inclusive artificial intelligence innovation and investment while promoting safe and trustworthy AI systems.[123]

• Encouraging the development, implementation, and dissemination of risk monitoring and management mechanisms, mechanisms for data protection, including personal data protection and privacy policies, and impact assessments as appropriate, throughout the lifecycle of artificial intelligence systems.[124]

• Encouraging the development and deployment of effective, accessible, adaptable, and internationally interoperable technical tools, standards, or practices, including reliable content and provenance authentication mechanisms such as watermarking or labeling, where technically feasible or appropriate, that enable users to identify instances of information manipulation, distinguish or determine the origin of authentic digital content and AI-generated or manipulated content, and enhance media and information literacy.[125]

• Facilitating the development and implementation of effective and internationally interoperable frameworks, practices, and standards for training and testing artificial intelligence systems to improve policymaking and help protect people from all forms of discrimination, bias, misuse, or other harm, and avoid reinforcing or perpetuating discriminatory or

[123] Ibid. Paragraph 6. Subparagraph a)
[124] Ibid. Paragraph 6. Subparagraph e)
[125] Ibid. Paragraph 6. Subparagraph g).

biased applications and outcomes throughout the lifecycle of artificial intelligence systems.[126]

• Encouraging, where appropriate and relevant, the implementation of appropriate safeguards to respect intellectual property rights, including copyright-protected content, while promoting innovation.[127]

• Promoting transparency, predictability, reliability, and understandability throughout the lifecycle of artificial intelligence systems used to make or support decisions affecting end users, including by providing information and explanations and promoting human oversight, for example through review of automated decisions and associated processes or, where appropriate and relevant, by providing alternatives for human decision-making or effective remedies and accountability for those adversely affected by automatic decisions of artificial intelligence systems.[128]

• Strengthening investment in the development and implementation of effective safeguards, including risk and impact assessments, throughout the lifecycle of artificial intelligence systems to protect and mitigate possible impacts on the full and effective enjoyment of human rights and fundamental freedoms.[129]

[126] Ibid. Paragraph 6. Subparagraph h).
[127] Ibid. Paragraph 6. Subparagraph i).
[128] Ibid. Paragraph 6. Subparagraph k).
[129] Ibid. Paragraph 6. Subparagraph l).

Other intergovernmental processes

Various processes aimed at promoting a common AI governance framework have taken place in recent years within the Organization for Economic Co-operation and Development (OECD), the Council of Europe, the G7, and the G20. This section presents a summary of the principles and policy guidelines emerging from these efforts.

OECD Recommendation on Artificial Intelligence (2019)

The OECD Council Recommendation on AI[130] was originally adopted by the Council of the Organization for Economic Co-operation and Development (OECD) in May 2019. To respond to advances in Artificial Intelligence technologies, particularly generative AI, it has since been amended twice: in 2023 and, recently, in 2024.

The principles seek to facilitate interoperability among global policies and advocate AI that is innovative and trustworthy and protects human rights and democratic values. In 2024 Uruguay formally requested adherence to the OECD Principles, and the process is currently underway.

OECD Principles on Artificial Intelligence

Principle	Scope
Inclusive growth, sustainable development, and well-being	The Recommendation proposes that stakeholders[131] proactively engage in responsible stewardship of AI for the benefit of people and the planet, advancing inclusive

[130] OECD. Recommendation of the Council on Artificial Intelligence. OCDE/LEGAL/0449. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 Last accessed, 13/05/2024.

[131] The Recommendation defines stakeholders as “all organizations and individuals involved in or affected by AI systems, directly or indirectly.”

	growth, well-being, sustainable development, and environmental sustainability.
Respect for the rule of law, human rights, and democratic values, including fairness and privacy.	The Recommendation maintains that AI actors[132] should respect the rule of law, human rights, and democratic values throughout the AI system lifecycle, for which they should implement mechanisms and safeguards to address risks arising from uses outside the intended purpose, intentional misuse, or unintentional misuse, in a manner appropriate to the context. This also includes addressing AI-amplified disinformation while respecting freedom of expression and other rights and freedoms protected by applicable international law.
Transparency and explainability	The Recommendation emphasizes that AI actors should commit to transparency and responsible disclosure regarding AI systems, providing meaningful information that is appropriate to the context and consistent with the state of the art. This information should enable a general understanding of AI systems, including their capabilities and limitations, awareness when interacting with AI systems, and, where feasible and useful, simple and easily understood information about data sources/inputs, factors,

[132] The Recommendation defines “AI actors as those who play an active role in the AI system lifecycle, including organizations and individuals that deploy or operate AI.”

	processes and/or logic that enable understanding of the outcome and, where applicable, allow those adversely affected by the outcome to challenge it.
Robustness, safety, and security	The Recommendation proposes that AI systems should be robust, safe, and secure throughout their lifecycle, so that they do not pose unreasonable safety risks under any conditions of use. Where technically feasible, to reinforce information integrity while ensuring respect for freedom of expression.
Accountability	The Recommendation proposes that AI actors should be accountable for the proper functioning of AI systems and respect for the preceding principles. To this end, they should ensure traceability, including in relation to datasets, processes, and decisions made during the AI system lifecycle, apply a systematic risk management approach to each phase of the lifecycle on an ongoing basis, and adopt responsible business conduct to address risks related to AI systems.

G20 AI Principles (2019)

In 2019, through a resolution, the Group of Twenty (G20) expressly supported the OECD Principles and took note of its recommendations.[133] The resolution reproduces the principles already discussed in the preceding section.

International Guiding Principles for Organizations Developing Advanced AI Systems, Hiroshima Principles (2023)

The OECD Principles have also served as the basis for other developments, such as the International Guiding Principles for Organizations Developing Advanced AI Systems adopted by the G7, known as the Hiroshima Principles.[134] They were adopted in 2023 under the Hiroshima Process[135] and seek to address recent advances in the most advanced AI systems, including generative AI, offering guidance to organizations that develop and use the most advanced AI systems. The concept of organizations in the context of the Principles includes, among others, entities from academia, civil society, the private sector, and the public sector.

The Hiroshima Principles gave rise to a code of conduct for developers.

[133] https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf Last accessed 2/5/2024.
[134] G7 Leaders' Statement on the Hiroshima AI Process. October 30, 2023. Available at: https://digital-strategy.ec.europa.eu/es/library/hiroshima-process-international-guiding-principles-advanced-ai-system . Last accessed, 02/05/2024.
[135] The Hiroshima AI Process consists of four pillars: 1. Analysis of the priority risks, challenges, and opportunities of generative AI. 2. The Hiroshima Process International Guiding Principles for all AI actors in the AI ecosystem. 3. The Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. 4. Project-based cooperation to support the development of responsible AI tools and best practices (Cf. (https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process),

Hiroshima Principles

Principle	Scope
Identification, assessment, and mitigation of risks throughout the AI lifecycle.	Take appropriate measures throughout the development of advanced AI systems, including before and during deployment, to identify, assess, and mitigate risks throughout the AI lifecycle.
Identification and mitigation of vulnerabilities and, where appropriate, incidents and misuse.	Monitor vulnerabilities, incidents, emerging risks, and misuse after deployment, and take appropriate measures to address them. Mechanisms for reporting vulnerabilities, where appropriate, should be accessible to a diverse set of stakeholders.
Transparency.	Publicly report through clear and accurate information on the capabilities, limitations, and areas of appropriate and inappropriate use of advanced AI systems, to help ensure sufficient transparency and increase accountability.
Information sharing.	Work toward responsible information sharing and incident reporting among organizations developing advanced systems, including industry, governments, civil society, and academia.

AI risk management and governance policies.	Develop, implement, and disclose artificial intelligence governance and risk management policies founded on a risk-based approach, including privacy policies and mitigation measures. This should include accountability and governance processes to assess and mitigate risks, where feasible, throughout the AI lifecycle.
Security	Invest in and implement robust security controls, including physical security, cybersecurity, and protection against insider threats throughout the AI lifecycle.
Content authentication mechanisms	Develop and implement reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other techniques enabling users to identify AI-generated content.
Research to mitigate societal and security risks and investment in effective mitigation measures.	Conduct, collaborate on, and invest in research supporting advances in AI safety and trustworthiness, and address key risks, as well as invest in developing appropriate mitigation tools.
Develop advanced AI systems centered on humans and global challenges and supporting achievement of the SDGs.	Prioritize the development of advanced AI systems to address the world's greatest challenges, particularly, among others, the climate crisis, global health, and education. Support progress on the United Nations Sustainable Development Goals. Organizations should prioritize responsible stewardship of trustworthy and

	human-centered AI and also support digital literacy initiatives.
Development and adoption of international technical standards and norms relating to AI.	Contribute to developing and, where appropriate, using international technical standards and best practices, including watermarking, and work with standards development organizations.
Implementation of measures for personal data and intellectual property protection	Implement appropriate data input measures and protections for personal data and intellectual property. Manage data quality, including training data and data collection, to mitigate bias. Support appropriate transparency of training datasets and compliance with applicable legal frameworks.

Council of Europe Framework Convention (2024)

The Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law[136] was formally adopted by the Committee of Ministers of the Council of Europe (COE) in May 2024 and will open for signature by member and nonmember States of the Council next September. The Convention's text was negotiated within the COE's Committee on Artificial Intelligence in a process extending from 2021 to March 2024. In October 2023, Uruguay joined the Committee as an observer, a status enabling nonmember States to accede to the treaty.

[136] Available at: https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411

This precedent is a legally binding instrument for States that sign and ratify it.

The Framework Convention aims to ensure that activities throughout the lifecycle of artificial intelligence systems comply with and are consistent with States' international human rights obligations, standards, and commitments, and are fully consistent with democracy and the rule of law.

The treaty obliges all parties to address risks arising from activities related to the AI lifecycle in both the public and private sectors, establishing nuances regarding the scope of States' obligations toward the private sector in the Convention's context.

The Explanatory Report accompanying the Treaty maintains that it ensures each Party's existing applicable obligations on human rights, democracy, and the rule of law also apply to activities throughout the artificial intelligence lifecycle. In this regard, the Framework Convention is aligned with each Party's applicable human rights protection system and mechanisms, including its international law obligations and other international commitments and its applicable domestic law.

As such, no provision of this Framework Convention aims to create new human rights or human rights obligations or undermine the scope and content of existing applicable protections. Rather, by establishing various legally binding obligations contained in Chapters II to VI, it facilitates effective implementation of each Party's applicable human rights obligations in the context of new challenges posed by artificial intelligence.[137]

Regarding the private sector, the Report explains that the treaty obliges all Parties to address risks and impacts on human rights, democracy, and the rule of law in the private sector, and clarifies that addressing risks is not

[137] COE – CAI. Explanatory Report. Para. 13 (unofficial translation). Available at: https://www.coe.int/en/web/artificial-intelligence/cai . Last accessed. 2/5/2024.

simply acknowledging those risks, but requires adopting or maintaining appropriate legislative, administrative, or other measures to give effect to this provision, as well as cooperation between Parties as set out in the provisions on the follow-up mechanism and international cooperation. It clarifies, however, that the obligation does not necessarily require additional legislation, and Parties may use other appropriate measures, including administrative and voluntary measures. Thus, although the obligation is binding and all Parties must comply with it, the nature of the measures adopted may vary.[138]

Activities within the lifecycle of artificial intelligence systems related to protecting national security interests are excluded from the Convention's scope. The Explanatory Report specifies that this exception applies only if and insofar as the activities concern protecting national security interests, so that all regular law enforcement activities for preventing, detecting, investigating, and prosecuting crimes, including threats to public security, also remain within the Framework Convention's scope as long as Parties' national security interests are not at stake.

The Framework Convention consists of 36 articles and 8 chapters.

Chapter II establishes States Parties' general obligations to adopt or maintain measures ensuring that activities within the lifecycle of artificial intelligence systems are consistent with obligations to protect human rights, as enshrined in applicable international law and domestic law (Article 4), and to adopt or maintain measures seeking to ensure the integrity, independence, and effectiveness of democratic institutions and processes (Article 5). Chapter III, in turn, stipulates common principles that will guide implementation of the Convention.

As indicated, Parties are required to apply existing national and international frameworks to the context of activities within the lifecycle of

[138] Ibid. Para. 29.

artificial intelligence systems, adopting or maintaining, consistently with those frameworks, measures to ensure accessible and effective remedies are available for human rights violations resulting from activities within the lifecycle of artificial intelligence systems (Article 14).

The Convention also provides that States Parties must adopt or maintain measures ex ante and, as appropriate, iteratively throughout the artificial intelligence system lifecycle, to identify, assess, prevent, and mitigate risks, considering actual and potential impacts on human rights, democracy, and the rule of law. It indicates that these measures must be graduated and differentiated, appropriate to the context and use.

In this regard, the Explanatory Report specifies that this provision gives Parties flexibility in assessment approaches and methodologies. It notes that “in particular, Parties may choose to implement this assessment at different levels, such as at the regulatory level by prescribing different risk classification categories and/or at the operational level by relevant actors assigned responsibilities for activities within the artificial intelligence system lifecycle. Likewise, each party will assess the need for a moratorium, prohibition, or other appropriate measures regarding certain uses of artificial intelligence systems when it considers those uses incompatible with respect for human rights, the functioning of democracy, or the rule of law (Article 15).

Principles set out in the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law

Principle	Scope
Human dignity and individual autonomy	Adopt or maintain measures to respect human dignity and individual autonomy

	in relation to activities within the lifecycle of artificial intelligence systems.
Transparency and oversight	Adopt or maintain measures ensuring that appropriate transparency and oversight requirements, adapted to specific contexts and risks, exist regarding activities within the lifecycle of artificial intelligence systems, including the identification of content generated by artificial intelligence systems.
Accountability and responsibility	Adopt or maintain measures ensuring accountability and responsibility for adverse impacts on human rights, democracy, and the rule of law resulting from activities within the lifecycle of artificial intelligence systems.
Equality and nondiscrimination	Adopt or maintain measures ensuring that activities related to the lifecycle of artificial intelligence systems respect equality, including gender equality, and the prohibition of discrimination, and adopt or maintain measures aimed at overcoming inequalities.
Privacy and personal data protection	Adopt or maintain measures ensuring the protection of individuals' privacy and personal data within the AI system lifecycle, including through national and international laws, standards, and frameworks, and establish effective guarantees and safeguards for individuals.

Reliability	Adopt measures to promote the reliability of artificial intelligence systems, which may include requirements relating to adequate quality and security throughout the lifecycle of artificial intelligence systems.
Safe innovation	Establish, where appropriate, controlled environments to develop, experiment with, and test AI systems under the supervision of competent authorities to foster innovation while avoiding adverse impacts on human rights, democracy, and the rule of law.

Processes in Latin America and the Caribbean

Digital Agenda for Latin America and the Caribbean, e-LAC (2022)

The Digital Agenda for Latin America and the Caribbean (e-LAC 2024) was adopted at the Eighth Ministerial Conference on the Information Society in Latin America and the Caribbean, held from November 16 to 18, 2022, and jointly organized by the Economic Commission for Latin America and the Caribbean (ECLAC) and the Government of Uruguay. It sets out regional policy priorities and strategic actions under four pillars.

The instrument's pillar 3 addresses productive and sustainable digital transformation and establishes as one regional agenda objective "promoting the effective use of emerging digital technologies to enhance productivity, foster innovation and entrepreneurship, with particular provision for Internet of Things solutions, artificial intelligence and environmentally friendly

technologies, safeguarding human rights and the ethical use of technology."[139]

Working groups have been established to implement the Agenda's objectives. These groups are a cooperation forum within eLAC2024, aimed at achieving a specific goal under the leadership of a coordinating country.

The Working Group on Artificial Intelligence is one of the groups established for the 2023–2024 period, coordinated by Chile's Centro Nacional de Inteligencia Artificial and Uruguay's Agency for Electronic Government and the Information and Knowledge Society (AGESIC).

Santiago Declaration (2023)

The Santiago Declaration "To promote ethical artificial intelligence in Latin America and the Caribbean"[140] was adopted in October 2023 by participating governments —including the Government of Uruguay—during the Forum on the Ethics of Artificial Intelligence in Latin America and the Caribbean and the Ministerial and High-Level Authorities Summit of Latin America and the Caribbean, organized by UNESCO, CAF, and the Government of Chile.

The Declaration approves creating a Working Group to establish an Intergovernmental Artificial Intelligence Council for Latin America and the Caribbean, to strengthen regional capacities in AI ethics and governance within UNESCO's Recommendation on the Ethics of AI.

Through this instrument, signatory countries agreed to "begin an analysis of the need to develop and adopt new legal frameworks and regulatory agendas for the responsible design, development and use of AI. The analysis

[139] ECLAC (2022). Digital Agenda for Latin America and the Caribbean, e-LAC 2024, Objective 13. Available at: https://repositorio.cepal.org/server/api/core/bitstreams/1fae5881-feba-42b4-a0b0-53ba8fa1f679/content . Last accessed, 15/5/2024.
[140] Available at: https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf .

should consider all cross-cutting human rights principles, particularly proportionality and do no harm; safety and security; fairness and nondiscrimination; inclusion; gender diversity; cultural diversity; accessibility; sustainability—social, cultural, economic, and environmental—; the right to privacy and personal data protection; human oversight and determination; transparency and explainability; responsibility and accountability; awareness and education; and intelligent governance and adaptive multistakeholder collaboration."[141]

The Declaration maintains that it is urgent to integrate the distinctive features of Latin American and Caribbean cultures into the creation of AI technologies for the region, and states that encouraging greater investment in the region is fundamental to comprehensively harnessing AI to solve its various problems and promoting innovative use of this technology by developing the necessary incentives.

Recent regulations in the United States and the European Union

2023 United States Executive Order

In October 2023, the United States government issued an Executive Order on the Safe and Trustworthy Development and Use of Artificial Intelligence,[142] expressly stating the purpose of promoting an "approach that addresses AI's risks without unduly reducing its benefits."[143]

[141] Ministerial and High-Level Authorities Summit of Latin America and the Caribbean (2023). Santiago Declaration, "To promote ethical artificial intelligence in Latin America and the Caribbean," operative paragraph 2. Available at: https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf Last accessed. 16/5/2024.

[142] The Executive Order's content can be consulted at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ Last accessed: 24/03/2024.

[143] Article 2, subsection (a).

The regulation directs various federal entities to take numerous measures to establish safeguards around artificial intelligence technologies and imposes new rules on certain AI system developers. The Executive Order sets out eight guiding principles and priorities for artificial intelligence policy, summarized below:

1. Safety and security: The Executive Order promotes ensuring robust, reliable, repeatable, and standardized assessments of AI systems, as well as policies, institutions, and, where appropriate, other mechanisms to test, understand, and mitigate their risks before they are used.
2. Responsible innovation and competition: The Executive Order promotes a set of measures to attract talent to the country, investments in AI-related education, training, development, research, and capacity, and the need to address intellectual property (IP) issues to protect inventors and creators.

3. Support for workers: The Executive Order considers the need to adapt workforce training and education to support a diverse workforce and help facilitate access to AI-created opportunities, and to ensure that AI is not deployed in ways that undermine workers' rights.
4. Equity and civil rights protection: The Executive Order proposes that Artificial Intelligence policies must be consistent with equity promotion policies and civil rights.
5. Consumer protection: The Executive Order proposes protecting the interests of consumers interacting with AI systems, particularly in critical areas, while promoting responsible use of AI.

6. Privacy: The Executive Order raises the need to protect privacy as AI continues to advance.
7. Managing risks from federal entities' use of AI: The Executive Order proposes increasing internal capacity to regulate, govern, and support responsible AI use to deliver better outcomes.
8. International leadership and cooperation: The Executive Order proposes that the United States should be a global AI leader and pioneer the systems and safeguards needed to deploy the technology responsibly, and proposes leading

regulatory efforts toward establishing common frameworks for assurance and risk management, and promoting global technical standards for AI.

Specific measures provided for in the Executive Order to achieve these objectives include:

1. Safety standards.

    • Require developers of certain systems to share information with the United States government.

    • Develop standards, tools, and tests to ensure that systems are safe and trustworthy before they are put into production.

    • Protect against the risks of using AI with dangerous biological materials.

    • Protect against AI-enabled fraud and deception. To this end, content authentication and watermarking guidelines will be developed to identify AI-generated content.

    • Establish an advanced cybersecurity program to develop AI tools and help detect and resolve vulnerabilities in critical software.

    • Direct the development of a National Security Memorandum to guide future actions on AI and security.

2. Privacy protection.

    • Prioritize federal support to accelerate the development of privacy-preserving technologies.

    • Strengthen privacy-preserving research and technologies.

• Assess how agencies collect and use available information and strengthen privacy guidelines for federal agencies.

• Develop guidelines for federal agencies to assess the effectiveness of privacy-preserving techniques.

3. Advance civil rights and equity

• Provide guidelines for landlords, federal benefit programs, and federal contractors to avoid using discriminatory algorithms.

• Tackle algorithmic discrimination through technical assistance, coordination, and best practices.

• Ensure fairness in the criminal justice system

4. Protect consumers, patients, and students.

• Advance responsible AI use in healthcare

• Design resources to support educational transformation through AI tools.

5. Support for workers.

• Develop principles and best practices to mitigate harms and maximize AI's benefits for workers

• Prepare a report on AI's potential impact on the labor market and study and identify options to strengthen federal support for workers affected by AI

6. Promote innovation and competition.

• Catalyze AI research in the United States through a National AI Research Resource pilot.

• Promote a fair, open, and competitive ecosystem through technical assistance and resources for small developers.

• Use existing authorities to expand the ability of highly skilled immigrants and nonimmigrants with expertise in critical areas to study, remain, and work in the United States.

7. Advance United States leadership abroad

• Expand bilateral, multilateral, and multistakeholder engagement to collaborate on AI.

• Accelerate the development and implementation of vital AI standards

• Promote safe, responsible, and rights-centered development and implementation abroad to address global challenges.

8. Ensure responsible and effective government use of AI.

• Establish guidelines for government offices' use of AI.

• Support government agencies in procuring AI products and services.

• Accelerate the rapid hiring of AI professionals in government.

European Union Artificial Intelligence Act

The European Artificial Intelligence Act[144] was approved by European Union countries on March 13, 2024. Under the provisions

[144] Artificial Intelligence Act, March 13, 2024. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.html

of Article 1, its purpose is to protect fundamental rights, democracy, the rule of law, and environmental sustainability from high-risk AI while promoting innovation.

The European Union instrument adopts a risk-based approach, under which it establishes prohibited applications and high-risk systems for which it regulates a set of requirements and obligations:

a) Unacceptable risk (Title II).

This classification includes the following prohibited applications:

• Cognitive behavioral manipulation of people that affects their autonomy and ability to choose freely, or exploits their vulnerabilities arising from age, disability, or other circumstances. The prohibition does not affect lawful practices related to medical treatments.[145]

• Biometric categorization systems based on biometric data.[146]

• AI systems enabling public or private actors to carry out social scoring of natural persons based on multiple data points relating to their social behavior across multiple contexts, or known, inferred, or predicted personal or personality characteristics over certain periods of time.[147]

• Use of AI systems for “real-time” remote biometric identification of natural persons in publicly accessible spaces for law enforcement purposes (exceptions are established).[148]

b) High-risk AI systems (Title III).

This classification covers systems whose outputs are relevant to an action or decision potentially posing significant risk to people’s

[145] Para. 29.
[146] Para. 30.
[147] Para. 31.
[148] Paras. 32 and 33.

health, safety, or fundamental rights. The regulation indicates that classification must take into account both the severity of possible harm and the likelihood of its occurrence. It provides that putting high-risk AI systems into service or using them must be subject to compliance with certain mandatory requirements.

This classification includes, among others:

- Various use cases of biometric identification systems.
- AI systems intended to be used as safety components in the management and operation of critical infrastructure.
- AI systems used in education or vocational training.
- AI systems used in employment and worker management, particularly recruitment and personnel selection.
- AI systems used to assess natural persons' credit ratings or creditworthiness, since they determine whether those individuals can access financial resources or essential services.
- AI systems intended to be used for law enforcement purposes
- AI systems used in migration, asylum, and border control management.
- AI systems intended for the administration of justice.
- AI implementations in products or product safety components already covered by European legislation (such as medical devices, railways, aircraft, or machinery).

The Regulation defines several supervisory authorities. It also establishes requirements that high-risk system providers must meet. These include Article 9, which indicates that a risk management system must be established, implemented, documented, and maintained. It also

provides that, where relevant, providers must ensure natural persons are informed that they are interacting with an AI system.

Annex 3: Contributions received during the consultation process

Institución Nacional de Derechos Humanos y Defensoría del Pueblo

Montevideo, June 11, 2024.

Re: Report on the application of Article 74 of Law No. 20.212

i. Background

Under Article 74 of Law No. 20.212 of November 6, 2023, AGESIC is entrusted with designing and developing a national data and artificial intelligence strategy based on international standards in the public and private spheres. Within this framework and as part of that strategy, a 180-day deadline has been established for submitting to the Legislative Branch a report and recommendations for its statutory regulation, aimed at its ethical development, the protection of human rights, and, at the same time, the promotion of technological innovation. To that end, the provision allows AGESIC to establish working groups, advisory committees, and other participation mechanisms that include perspectives from the public and private sectors, academia, and organized civil society.

On April 30, 2024, AGESIC prepared the document setting out the basis for developing the report provided for in Art. 74 of Law No. 20.212, inviting various public entities to participate, including the National Human Rights Institution and Ombudsperson's Office.

Within this framework, the INDDHH will make the following contributions to the document in question, within its institutional tasks and powers to defend, promote, and protect human rights, and with the aim of contributing to the issue and responding to the questions raised in the report as points for contributions from participating entities.

This does not constitute an analysis of every point mentioned in the extensive report referred to, but rather certain issues that the INDDHH Governing Board considers most relevant to address, without prejudice to the importance of all the aspects mentioned in the document and the possibility of addressing, on future occasions, other issues not covered here.

ii. On the institutional framework and governance

As indicated in the document submitted, one of the first aspects to analyze concerns the institutional framework and governance of AI, particularly the issue of the lead entity's organizational and institutional position in this field.

In this regard, AGESIC itself is cited as an example, created under Law No. 17.930 as a deconcentrated body of the Office of the President of the Republic, followed by Law No. 18.331, which created the Personal Data Regulatory and Control Unit (URCDP) as a deconcentrated body within AGESIC, still within the Office of the President of the Republic.

Examples from comparative law, both in Latin America and Europe, are also given, showing the existence of self-governing entities

(which in our legal system would correspond to what the framers of the Constitution regarded as
Autonomous Entities or Decentralized Services) and entities under
Ministries, operating as a kind of technical secretariat, through a sort of mechanism comparable to the one in our country (with the qualification that in our case the link is with the Presidency). Finally, reference is made on this point to the European Regulation, the United States case, and the regulation currently in force in the United Kingdom.

On this point, considering the provisions of Law No. 20.212, which entrusts AGESIC and the URCDP with establishing general criteria on the subject (including oversight), their
sphere of action should ideally be situated outside the
Office of the President of the Republic (setting aside doctrinal discussions about the Presidency's role under our Constitution and the enormous expansion of that organizational system's subject areas and tasks) and, generally, outside the Executive Branch itself, since the latter is in fact the largest producer and user of information and data in our country.

Given the growing daily importance of handling
data, information, and AI, the ideal would be a completely autonomous oversight entity, as our Constitution recognizes for
the three oversight bodies, which also have autonomous regulatory powers, as is particularly the case with the Court of Auditors and the Electoral Court.

Since this scenario is unlikely, given that it entails a constitutional reform, two possible institutional paths are proposed for potential institutionalization.

First, one option is to place this agency within the Legislative Branch's sphere of action as an autonomous and independent entity, as with the INDDHH, created under Law No. 18.446. Although the Parliamentary Commissioner for the Prison System also belongs to the legislative sphere, it has a role of reporting directly to Parliament, which is not the case for the INDDHH and should likewise not apply to an agency such as the one proposed for AI. A clear strength of this option is the representative nature of the legislative sphere of action and, particularly, the clear separation of its activities from the Executive Branch, with the particular features noted above.

The second feasible option, with strong precedents in our legal system, would be to follow the path of other oversight entities such as URSEC, URSEA, and JUTEP, which recently (in institutional terms) have become what comparative law calls self-governing entities and adopted—in all three cases—the form of decentralized services, although they could potentially also adopt the form of Autonomous Entities, given that they are not limited by Art. 186 of the Constitution, as is the case with the BCU's oversight role.

The Decentralized Service form, which, as indicated, appears to be the path adopted for oversight entities, given the specificity of their tasks and the proper application of the principles of specialty and specialization for public bodies, particularly this type of entity, removes them from the hierarchical sphere of action of the Executive Branch (or the Office of the President of the Republic), and even adopts a form of appointment of leadership that exceeds the government's five-year terms.

Nevertheless, oversight of the system will naturally continue, given the characteristics of how decentralized services operate and the aspects relating to administrative supervision, staff status, and budgetary provision under Art. 220 of the Constitution. This last point undoubtedly poses one of the most substantial challenges, since an appropriate budget allocation, as recognized in the report, is essential for the proper functioning of this type of oversight agency.

iii. Another aspect reviewed in the report concerns the example of data trusts. Although the trust instrument—recognized in our country in Law No. 17.703—is clearly geared toward assets and finance (whether testamentary, management, guarantee, or financial trusts), its application to data appears clearly innovative.

Considering examples from comparative law—particularly the trust in common law—and the substantive foundations of the trust instrument, particularly the existence of settlors, a trustee, and beneficiaries and, on the other hand, a set of assets or rights held in trust and a mandate, it is essential that regulation enabling these instruments have a statutory basis to protect data subjects' rights and regulate the roles of each party, particularly the trustee, which should preferably be a State entity (for example, the oversight agency).

Alongside this, a significant set of regulatory and oversight aspects must be clearly established by law, particularly the trustee's powers regarding the data managed and the potential beneficiaries of those collected data.

Within this framework, the trust option, although not to be ruled out, undoubtedly entails extensive regulatory development to ensure information security and proper protection of people's rights.

iv. (…..)

Contributions from Data Uruguay for developing the report provided for in Art. 74 of Law No. 20.212

Daniel Carranza Secretary
of Data Uruguay

1. What specific recommendations could you make, based on your experience, to promote the areas defined in this document?

At Data Uruguay, we analyzed the document “Basis for developing the report provided for in Art. 74 of Law No. 20.212” and emphasize the importance of adapting national legislation to regulate artificial intelligence (AI) in Uruguay according to the latest international human rights standards.

We emphasize the importance of Agesic’s work in establishing ethical frameworks and soft law rules through the AI Strategy for the public sphere, although we consider that this work must be complemented by updating national legislation. The aspects requiring the most urgent regulation relate to automated decision-making through artificial intelligence systems, particularly in the public administration. These situations include not only fully automated decisions, but also human-machine interaction and the concept of meaningful oversight (when operators act with awareness of the system’s biases or limitations).

To promote the areas defined in this document, we believe that, following this consultation, the Uruguayan Parliament should consider opening a public hearing where our legislators can interact with businesses, academia, and specialized civil society, since legislation on these issues is currently being enacted on the basis of very superficial understandings of some challenges of regulating this subject and its consequences..

We suggest a list of possible issues to discuss at the proposed public hearings on AI regulation, including:

- Determining which uses pose a high risk of violating individual rights and would warrant specific regulation.

- Establishing basic safeguards such as the right to explainability, traceability, transparency, and algorithmic auditability in high-risk systems, even if they do not process personal data or are not covered by the Personal Data Protection Law.

- Mandatory application of risk assessment instruments in certain critical scenarios that do not involve personal data use or where personal data protection obligations do not apply (such as public security or defense).

- Mandatory labeling of synthetic content.

- Defining the principle of meaningful human oversight.

Finally, we understand that, although the National Human Rights Institution and Ombudsperson's Office is the body mandated to make human rights public policy recommendations and provide guidance to Parliament, its members lack a sufficient critical mass of knowledge to fulfill this recommendation function on AI. It would therefore be desirable to suggest some form of support for the INDDHH to establish agreements with academia and civil society specialized in digital rights.

2. Are there regulatory deficiencies or inconsistencies affecting the aspects assessed in the areas defined in this document that have not been considered?

Regarding the analysis of Articles 13 and 16 of the Personal Data Protection Law in section "3.3 Preliminary assessment of AI and Human Rights" of the document, we highlight the importance of the right to challenge automated decisions and obtain information on "the assessment criteria, the processes applied, and the technological solution or program used." Nevertheless, these rules are insufficient and need updating to include modern standards, such as standards

on algorithmic transparency[1] and meaningful human oversight.[2] These same standards could also be included through obligations imposed on the public administration by amending the Access to Public Information Law.

3. Have you identified potential improvements or amendments to current legislation that could support AI development in Uruguay?

Reform of Law No. 19.179 on open formats and free software and its implementing decree (Decree No. 44/015)

Following the same logic of updating existing legislation proposed by Agesic in the draft document, we suggest implementing a support system for public administration decisions on procuring software or AI-based solutions by amending Law No. 19.179 on open formats and free software and its implementing decree (Decree No. 44/015). This law is an instrument that has existed in our legal system since before the rise of AI and could be reviewed to prioritize open AI solutions, avoiding black boxes and encouraging guarantees of transparency and explainability. We believe that, in addition to reviewing Law No. 19.179 and its decree to promote preferential use of open AI models, an intervention mechanism should be included through which Agesic determines risk and advises public entities on conducting impact assessments before acquiring AI-based solutions, at least for certain key sectors or uses (health, public security, or education, for example).

4. Are there other aspects you find have not been considered and should be analyzed?

Urgent regulation of the Ministry of the Interior's procurement and use of surveillance software

A search of the press is enough to establish that, in recent years, the Ministry of the Interior has steadily procured new technologies to combat crime. Many of these acquisitions use powerful AI systems, whether to detect gunshots

[1] IDB (2022), "Auditoría algorítmica para sistemas de toma o soporte de decisiones". See: https://publications.iadb.org/publications/spanish/document/Auditoria-algoritmica-para-sistemas-de-toma-o-soporte-de-decisiones.pdf

[2] EU AI Act. See: https://www.euaiact.com/key-issue/4

by placing microphones in public streets or to identify people based on biometric patterns. None of these technologies is adequately regulated by law under the standards called for by the various Special Rapporteurships of the international human rights system.

The UN Human Rights Committee's criteria for adopting surveillance measures are as follows: governments may establish such measures for their citizens provided that 1) they are authorized by an accessible and precise national law, 2) they pursue a legitimate objective, and 3) they meet the criteria of necessity and proportionality. As far back as 10 years ago, the UN High Commissioner for Human Rights warned that these requirements were not being met,[3] and that States often use surveillance systems without adequate national laws, procedural safeguards, or sufficient oversight. The High Commissioner notes "the disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hampers any attempt to assess their compatibility with international human rights law and ensure accountability."

We share the High Commissioner's concern and believe that the report Agesic submits to Parliament should recommend urgently regulating the Ministry of the Interior's use of AI for surveillance.

[3] "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" A/HRC/27/37, para. 48. See: https://documents.un.org/doc/undoc/gen/g14/068/74/pdf/g1406874.pdf?token=BBP8Fg822XkzlZAS4c&fe=true

Datysoc
LABORATORIO DE
DATOS Y SOCIEDAD

Consultation for developing the report provided for in Art. 74 of Law No. 20.212

Document prepared by Patricia Díaz Co-coordinator of the
Laboratorio de Datos y Sociedad | Datysoc

Preliminary matters

We offer several suggestions regarding the document's structure:

- Since this will be a lengthy document, we suggest generating a hyperlinked table of contents to improve navigation and usability.
- We suggest placing at the end of each area a bullet-point summary specifically and clearly stating the regulatory recommendations.

Authorization: the Agesic team is authorized to copy, adapt, and/or incorporate any part of this document into the final version submitted to Parliament, without citation.

1. What specific recommendations could you make, based on your experience, to promote the areas defined in this document?

We state that, generally, we agree with both the analysis presented and the aspects prioritized, as well as the broad guidelines of the proposal presented in the draft "Basis for developing the report provided for in Art. 74 of Law No. 20.212." However, there is a central aspect the document fails to address explicitly and clearly: a question that several legislators surely have in mind. Do we need general AI regulation, or should we regulate certain AI uses or its use in certain sectors?

We believe the conditions are not yet in place for general regulation based on determining different risk levels, assigning differentiated obligations for each level, and creating new specialized AI institutions. A better understanding of the landscape is needed before regulating, so we propose recommending to

parliamentarians the creation of a forum to promote the areas defined in this document, identify other national priorities, and formulate recommendations from different social stakeholders for adequate and sustainable regulation.

In parallel with this discussion, we suggest focusing current regulatory **efforts on updating the existing national body of law and regulating current high-risk government uses of AI.**

Thus, without ruling out other emerging issues, we highlight police use of AI as a high-risk emerging issue warranting urgent regulation and propose creating a new area: “AI use for police surveillance and as evidence in criminal proceedings” (see question 4).

2. Are there regulatory deficiencies or inconsistencies affecting the aspects assessed in the areas defined in this document that have not been considered?

Below we present several aspects not considered in the document that we believe should be added:

Section “3. Human Rights area”

We propose adding the following considerations to section “3.3 **Preliminary assessment of AI and Human Rights”:**

On Personal Data Protection Law 18331 (LPDP) and Decree 64/020.

We agree with the draft document’s observations that Arts. 13 and 16 of the LPDP should be reviewed. We consider these provisions insufficient for the following reasons:

1) The right to challenge personal assessments based on automated data processing (Art. 16) applies only in the context of personal data, although there are countless contexts in which it does not apply. An illustrative example: the mechanism provided for in Art. 16 could not be used to challenge and obtain information about an AI system that analyzes water and air pollution data where the health of a group of citizens is considered at risk.
2) Art. 16 only allows challenges to decisions “whose sole basis is personal data processing.” It is enough to “put a human in the middle” and say that the system “advises” but the human makes the decision for the article’s application to fall away. In light of the well-known “automation biases,”[1] consideration should be given to including a provision defining the concept of “meaningful human oversight,”

[1] Report “Hacia una supervisión significativa de los sistemas automatizados de toma de decisiones” (2022). Digital Future Society. Available at: https://digitalfuturesociety.com/es/report/hacia-una-supervision-significativa-de-los-sistemas-automatizados-de-toma-de-decisiones/

including minimum requirements such as training for actors who operate the system, among other factors.
3) We must not forget that the mechanisms of the LPDP and Decree 64/020 do not regard personal data protection as a collective right, so these provisions likewise cannot be used to require any public or private institution to account for basic explainability parameters of its automated systems in the face of a potential risk to fundamental rights.
4) Under Decree 64/020, obligated entities are not required to publish their impact assessments; they must only share them with the URCDP if the assessment identifies a potential and significant risk (Art. 7).
5) Arts. 13 and 16 of the LPDP do not specify the requirements for explainability and do not require traceability or auditability, so the obligation is satisfied when the administration itself unilaterally presents explanations.
6) Rules are needed to guarantee a minimum level of transparency,

interpretability, and algorithmic auditability (Stoyanovich, Julia 2020)[2] on the understanding that:

- **Algorithmic transparency is not synonymous with releasing source code.** Publishing source code helps, but is sometimes unnecessary and often insufficient. In some cases, requiring source code release may be excessive or infringe rights.
- **Algorithmic transparency requires data transparency. Explainability** can only be achieved in a data context: the data used for training and testing, the data to be used for system deployment and validation (reference datasets), and data on system performance and accuracy. Data transparency is necessary for all automated systems, not only Machine Learning-based systems.

- **Data transparency is not synonymous with making all data public.** Data should be released whenever possible; where this is not possible (for data protection, confidentiality, or intellectual property reasons, for example), alternatives include publishing selection or collection methodologies, using synthetic datasets, publishing statistical summaries or samples, the data used for preprocessing, data provenance and information on quality/representativeness, and the known sources of bias identified.

[2] Stoyanovich, Julia (2020). TransFAT. Translating fairness, accountability, and transparency into data science practice. Available at: https://pdfs.semanticscholar.org/061f/de41f92e6bd408b5722428bdcc8b2a7d0858.pdf

- **Actionable transparency requires interpretability or comprehensibility.** Ultimately, this means explaining the system's assumptions and effects (not just operational details) and involving the public—technical and nontechnical.

On Access to Public Information Law 18381 (LAIP).

The LAIP should include a provision introducing the right to be **informed about which decisions are made automatically or with support from an automated system by the public administration, and about** how those systems work (taking into account the preceding section's observations on transparency, interpretability, and algorithmic auditability and the definition of "meaningful human intervention"). A provision guaranteeing the right to human and in-person interaction with the public administration should also be included.

Section "4. Intellectual Property area"

We propose adding the following considerations to section "4.1 **Preliminary considerations":**

Most AI development activities currently require large-scale use of substantial data volumes and often involve thousands of copyrighted images, audio recordings, texts, etc., for computational analysis or model training. Such uses include text and data mining techniques (such as crowling, scraping, and parsing), and creating technical or ephemeral copies for model training, among others. Thus, to encourage innovation and create a secure legal environment for local researchers and developers, copyright laws need to include an exception allowing works to be used for computational analysis. This exception should include the restriction that those uses must not conflict with the normal exploitation of works or unreasonably harm authors' interests.

Given that software and databases are also protected by copyright and technological protection measures, the relationships between copyright, trade secrecy, and system auditability will need clear regulation. AI system auditability is of particular public interest for both cybersecurity and transparency and explainability reasons, and often requires circumventing technological protection measures to access

systems, make test copies, or carry out reverse engineering.

We propose adding the following considerations to section “4.2 Selected **international precedents”:**

Regarding copyright exceptions for computational analysis, the most recent precedent within WIPO is the report on “Los retos de los centros de investigación y los fines de la investigación en relación con los derechos de autor” (2023).[3] This report was commissioned from Raquel Xalabarder by the Standing Committee on Copyright and Related Rights (SCCR/WIPO), and the author states: “The role of nonhuman (machine) reading, such as artificial intelligence (AI) analysis, is becoming increasingly important within research methodologies. Text and data mining (TDM) has gained prominence thanks to digital technologies. Using TDM tools, researchers extract information from a wide variety of protected works, from scholarly works to music and press publications.” (our translation) The same report contains an Annex with examples of national rules providing these copyright exceptions for research activities involving computational analysis, which are already present in almost all Global North legislation. Regarding exceptions to copyright and technological protection measures for system auditability, there is the 2022 report of the OECD Working Party on Security in the Digital Economy.[4] It states that “copyright law may be infringed when disclosed information contains portions of copyrighted software code. Such copyright protection could restrict vulnerability information sharing with the original vendor, making CVD—Coordinated Vulnerability Disclosure—difficult to implement in many cases.” The document explains that the failure to update exceptions to copyright and technological protection measures entails legal risks for auditors and digital security researchers, and also states that these rules are used by the owners of software under investigation to threaten legal proceedings.

[3] Xalabarder, Raquel (2023). “Los retos de los centros de investigación y los fines de la investigación en relación con los derechos de autor”. Available at: https://www.wipo.int/meetings/es/doc_details.jsp?doc_id=621815

[4] OECD (2022). OECD Policy Framework on Digital Security. Available at: https://www.oecd.org/publications/oecd-policy-framework-on-digital-security-a69df866-en.htm

We propose adding the following considerations to section “4.3 **Preliminary assessment of AI and Intellectual Property”:**

> Uruguay’s Copyright Law (Law 9.739) does not provide exceptions to copyright (or to the technological protection measures regime) that enable proper development of computational analysis or auditing activities, whether for security or explainability purposes. A new exception therefore needs to be included in Art. 45 of the Copyright Law (Law 9739) to allow works to be used for computational analysis. It is also suggested that an exception to copyright (and technological protection measures) be added to enable systems to be accessed, copied, and analyzed exclusively to allow auditing when required by a judge or another law. These exceptions must expressly state that competitive uses, or uses that unreasonably harm the author or right holder of the works, are strictly prohibited.

3. Have you identified potential improvements or amendments to current legislation that could support AI development in Uruguay?

---

4. Are there other aspects you find have not been considered and should be analyzed?

Below, we propose including a new area constituting the **most significant emerging use of AI with a high risk of violating fundamental** rights in Uruguay, which should therefore be analyzed independently and warrants urgent regulation:

AI use for police surveillance and as evidence in criminal proceedings area.

Preliminary considerations:

AI use for crime prevention and public security puts citizens’ rights at risk because of its potential for discrimination and its highly intrusive nature, beyond any biases or failures entailing discrimination risks. Some of the main concerns

regarding the use of these systems by police and in criminal justice are:[5] Violating the presumption of innocence. The right to be presumed innocent in criminal proceedings is a fundamental human right. However, the growing use of AI in criminal justice, particularly remote biometric surveillance and certain types of predictive policing software, raises questions about the scope of this right and how AI systems must be built and used to protect it.

Preserving equality of arms and due process. One of the main concerns raised in studies of certain AI systems is that they are inaccessible to proper scrutiny by defendants and their lawyers. This has serious implications for the principle of equality of arms and the right to adversarial proceedings, because without information about how a decision is made, it is difficult to envisage how defendants can challenge its accuracy and lawfulness. In this regard, one of the principal problems preventing sufficient contestability of AI systems in criminal proceedings is the lack of notification. If a person is not notified that they have been subject to an automated decision by an AI system, they will have no opportunity to challenge either the decision or the information on which it was based. The black-box phenomenon is another risk factor in AI application, since preserving due process and equality of arms necessarily requires the system and its results to be explainable and demonstrably free from bias.

The lack of mandatory training for justice system actors: training justice system actors is essential to determine admissibility and properly assess digital evidence, as well as to give meaning to the concept of “meaningful human intervention” in the judicial context. Training is needed not only for primary users of AI systems, such as judges and police officers who use them to support their own decisions. It must also be available to criminal defense lawyers, so they are better positioned to challenge AI systems when necessary.

Selected international precedents

In the report “Surveillance and human rights” (2019),[6] the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression proposes drastic measures. The report urgently calls for

[5] Policy Paper: Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU (2022). Fair Trials. Available at: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf

[6] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. “Report on surveillance and human rights”, A/HRC/41/35. (United Nations General

"an immediate moratorium on the global sale and transfer of the tools used by the private surveillance industry until rigorous human rights safeguards are established in regulating these practices and it can be guaranteed that governments and non-State actors will use those tools legitimately." It also calls for "stricter regulation of surveillance equipment exports and stronger restrictions on their use."

The "EU Artificial Intelligence Act" (Art. 5 of Chapter II, "Prohibited Artificial Intelligence Practices")[7] prohibits law enforcement and security forces from using real-time biometric identification in publicly accessible places for policing or public order applications, except to search for potential crime victims, prevent specific and substantial threats to critical infrastructure or natural persons, prevent terrorist attacks, and pursue crimes punishable by more than five years' imprisonment. Beforehand, it is mandatory to assess the likelihood and scale of possible harm without such systems and the harm those systems might cause; binding judicial or administrative authorization must be obtained; and temporal, geographical, and personal limitations will be imposed.

Another important precedent is the "European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters."[8] This resolution addresses artificial intelligence (AI) use in criminal law, focusing on its application by police and judicial authorities. The document emphasizes the need for a robust regulatory framework ensuring respect for fundamental rights, privacy, and data protection. It also emphasizes the importance of transparency, human oversight, and accountability in AI system use to prevent bias and discrimination. The resolution also calls for impact assessments and regular audits of these systems to ensure compliance with the European Union's ethical and legal standards.

In this Resolution, the European Parliament highlights AI's potential to improve efficiency and effectiveness in combating crime, but also warns of associated risks, such as miscarriages of justice and

Assembly, May 28, 2019). Available at:.
https://www.undocs.org/es/A/HRC/41/35

[7] European Union Artificial Intelligence Act approved by the European Parliament legislative resolution of March 13, 2024. Available at:
https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

[8] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). Available at:

https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

human rights violations. The resolution proposes creating a specific legal framework for AI use in criminal matters, including clear guidelines on data collection and processing and measures to ensure fairness and nondiscrimination. It also recommends that authorities and legal professionals receive adequate training on AI use and implications, thereby ensuring fair and safe application of these technologies in the judicial system.

Preliminary assessment

The Ministry of the Interior has been building an automated surveillance ecosystem to support its responsibilities, based both on AI and other systems. This ecosystem has not been accompanied by adequate regulation or proactive transparency criteria that build confidence in its operation. There is no regulation regarding police use of systems recently acquired by the Ministry of the Interior. Examples include automated facial recognition; UCINET software (intelligence software using open sources such as social networks); the ShotSpotter system (which involves placing microphones in streets so AI can detect gunshots); and even camera analytics software to "determine suspicious behaviors that may alert police before a crime occurs." In Uruguay, oversight of the use of personal databases employed in "public security, defense, State security, and activities in criminal matters, investigation, and suppression of crime" is not covered by the obligations established by Personal Data Protection Law 18331 (LPDP Art. 3, Subsection B, and Art. 25).[9]

Regarding the Automated Facial Recognition (RFA) software acquired by the Ministry of the Interior in February 2020 through public tender, we emphasize that this procurement is related to approval of the creation of a facial identification database for processing for public security purposes, under the Secretariat of the Ministry of the Interior (Arts. 191 and 192 of the 2020 Budget Law). This permits the use of facial photographs (and associated information) from identity cards and passports in the National Directorate of Civil Identification (DNIC) database to create a biometric database for a purpose other than identification. Many questions arise from this procurement and blanket authorization to use

[9] "However, it should be noted that, even in the cases indicated in the preceding paragraph, the URCDP has interpreted that personal data protection principles remain generally applicable." See the consultation to the URCDP Executive Council published in: Report "Fuera de Control. Uso policial del reconocimiento facial automatizado en Uruguay". Datysoc (2022), p. 49. Available at:

https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf

the entire population's biometric data. For exactly what purposes was the system procured? Who authorizes use of the RFA system? How will its use be audited? How will access be controlled? How should an officer proceed following a biometric match in different use contexts? When can a biometric match be admitted as evidence? How will this evidence be assessed? How will potential system biases be addressed? When and how will the accused be informed that this type of evidence exists? How will differences between a biometric match in a controlled and an uncontrolled environment be addressed? How will these personal data be deleted when no longer needed? None of this has yet been defined, and most of these

decisions should be established through precise and publicly accessible statutory provisions.

It is also worth noting that neither the Criminal Procedure Code nor the Police Procedure Law contains any regulation on digital evidence admissibility or assessment, nor are there public protocols on the Ministry of the Interior's acquired AI or training for judicial actors on how this AI works.

Regulatory recommendations on police use of AI

Following the recommendations of the UN Special Rapporteur on Freedom of Expression, it is suggested that a moratorium be imposed on surveillance software procurement until there is a legal basis adequately regulating the police surveillance ecosystem.

To establish strict regulation of its use and provide safeguards against discriminatory acts and abusive or arbitrary use, the necessary amendments should be made to the Criminal Procedure Code and Police Procedure Law to regulate the issue adequately, including:

- A requirement to conduct a fundamental rights impact assessment (public where possible) before acquiring AI surveillance solutions, and to know and declare in advance the exact purposes for which they are procured.
- Establishing red lines on which uses are strictly prohibited for police and which require a court order.
- The possibility of requiring algorithmic auditability and explainability, traceability, access control protocols, and detailed descriptions of responsibilities for those using these surveillance systems.
- Adequate training for police officers, judges, and prosecutors on system operation and limitations through mandatory certification.

Specific recommendations relating to biometric surveillance and facial recognition:

- Prohibit blanket enrollment of the entire population in the facial recognition system acquired by the Ministry of the Interior. This entails repealing Arts. 191 and 192 of the 2020 Budget Law, as these articles violate the presumption of innocence principle.
- Prohibit real-time biometric surveillance without a court order in public spaces.
- Mandatory impact analysis and risk assessment mechanisms together with accountability and monitoring mechanisms.
- Specific regulation of the admissibility, assessment, and handling of biometric matches as investigative methods and digital evidence.

CONTRIBUTION FROM THE COMPUTER AND TECHNOLOGY LAW COMMITTEE OF THE ASOCIACIÓN DE ESCRIBANOS DEL URUGUAY.

Consultation: Basis for discussing the contents of the preliminary report provided for in Art. 74 of Law No. 20212 (AGESIC)

1. What specific recommendations could you make, based on your experience, to promote the areas defined in this document?

Regarding governance, an initial determination should be whether general or sector-specific regulation is needed, since certain sectors are highly sensitive institutionally, socially, and economically. In both cases, as with the European Union Artificial Intelligence Act, it would be appropriate to focus on the risks it might pose and on assigning and distributing liability for harm (given the many actors who may participate) to ensure equitable compensation for those harmed.

Resolving the allocation of liability for AI use will be a challenge in a system that may not be based in Uruguay, but whose consequences will be borne in our country.

In the judicial field, we believe it may be advisable to “use ‘white-box’ AI systems based on techniques that serve to make predictions, classifications, and intelligent detections that offer

enormous benefits for judicial work and organizations' digital transformation, without the risk of black-box inexplicability."[1]

The "PretorIA" system, created by the Innovation and Artificial Intelligence Laboratory of the Universidad de Buenos Aires Law School (UBA IALAB), a predictive system developed for use by Colombia's Constitutional Court, may be highly advisable

"PretorIA combines features based on expert systems and white-box machine learning techniques."[2]

2. Are there regulatory deficiencies or inconsistencies affecting the aspects assessed in the areas defined in this document that have not been considered?

To determine these criteria and through them place AI at the service of citizens and achieve greater social well-being, we should consider, as a country, what limits we are prepared to establish for different AI developments and regulate them accordingly.

Establish the corresponding impact assessments for an AI development to minimize human rights risks.

[1] Tratado de inteligencia artificial y derecho : tomo II / Juan Gustavo Corvalan... [et al.] ; edited by Juan Gustavo Corvalan. - 2nd ed. - Ciudad Autónoma de Buenos Aires : La Ley, 2023. Digital book, Book "app" for Android Digital File: download and online ISBN 978-987-03-4642-5 [2] Work cited

For these issues, consideration will be given to using the recent EU AI Act as a basis

3. Have you identified potential improvements or amendments to current legislation that could support AI development in Uruguay?

Section 3.3, "Preliminary assessment of AI and Human

Rights," of the document submitted for consultation highlights "7 central aspects linked to the points mentioned by the United Nations High Commissioner for Human Rights and detailed above…"

In this report, we will focus on two of the questions set out there:

1.- What is the scope of transparency and explainability to be guaranteed in the development of human-centered AI systems?

In response, we say that although under our current legislation we could apply Law No. 18331 regarding personal data, using the principles of purpose limitation and prior informed consent, given AI's impact, both in development and application, on individuals and society, these principles should be strengthened in their definition and application. Prior informed consent should clearly establish the information to be provided either to the consumer of an AI service or the purchaser of an AI product. (children's games, glasses, chat GPT) The provisions of Art. 9 of Law No. 18331 are insufficient.

This conclusion is reached because of the type of personal data that may be used in AI training, which may include biometric and sensitive data that may be compromised during processing. Regarding the purpose limitation principle, a more explicit definition focused on AI development would help achieve greater transparency.

“We consider it essential for a regulatory framework” to place human beings at its center and “require companies to state explicitly where and how artificial intelligence technologies and automated techniques are used in their platforms, services, and applications, as well as the duty to prevent discrimination and ensure that AI equipment and systems reflect nondiscriminatory attitudes and avoid bias.”[3]

“In AI-based scoring, personal data may not be considered unless they form part of the set of data for whose purpose the study is conducted.

The scoring outcome must meet all AI principles so that it can be properly explained by a human being to the person affected

Synthetic data may not be used in notarial or contractual matters.

[3] Tratado de inteligencia artificial y derecho : tomo II / Juan Gustavo Corvalan... [et al.] ; edited by Juan Gustavo Corvalan. - 2nd ed. - Ciudad Autónoma de Buenos Aires : La Ley, 2023. Digital book, Book “app” for Android Digital File: download and online ISBN 978-987-03-4642-5 1. Artificial Intelligence. 2. Law. I. Corvalan, Juan Gustavo, ed. CDD 346.002

Privacy policies must explicitly state whether synthetic data are used and how they are used."[4]

4. Are there other aspects that have not been considered and should be analyzed?

A new technological divide must be anticipated, much deeper than previous ones, in which many people will be left behind, at risk of becoming vulnerable.

Furthermore, "adaptability and acquiring new skills have always been imperative in the changing world of law. However, in the digital and artificial intelligence era, these skills evolve and must adapt to the challenges and opportunities offered by new technologies

"One example is legal prompt engineering, an emerging skill that refers to the ability to interact and communicate effectively with AI-based conversational agents, such as ChatGPT.

In this sense, we will see that legal prompt engineering is a crucial skill encompassing and improving various aspects of legal practice in the digital era, not only in searching for information but also in drafting legal documents, arguing cases effectively, and designing improved legal strategies through precise and effective interaction with sophisticated conversational agents. This adaptation

[4] Work cited

is not only necessary but may offer great opportunities to

advance the path of professional retraining, optimize legal practice, and

develop intelligent justice in the age of machines."[5]

Notary Elisabeth Bouvier Villa
Notary Javier Wortman

[5] Work cited

This document brings together the AI Advisory Group's contributions for submission to the Legislative Branch, as provided for in Art. 74 of Law No. 20.212, under Agesic's responsibility.

The contributions are made by the Artificial Intelligence Advisory Group of the Cámara Uruguaya de Tecnologías de la Información

Institutional Framework and Governance (Ref. Chapter 2 of the document)
The objective of this area is to determine the fundamental aspects needed to ensure an adequate institutional framework for Artificial Intelligence in our country.
Comments
The document shows that the existing institutional framework is adequate for addressing the challenges raised. It is indeed essential to have advisory groups involving all stakeholders that operate regularly.
The concept of working groups is clear, but they should have greater involvement in defining policies, which are coordinated, managed, and led by AGESIC. It would be good to give them greater significance and decision-making power than a working group. We agree with the role of the URDCDP. Agesic must encourage the development of artificial intelligence systems, but it would not be advisable for it to develop them itself. I also consider it appropriate to define criteria and oversight mechanisms to ensure the criteria are properly applied.
Incorporating AI as a central aspect of creating innovative solutions is a path that involves taking risks (as all innovation does). When a solution is developed to provide a public service (often in sensitive fields), the impact of failure is greater, and this may slow innovation because such risks are not taken. Governance must incorporate mechanisms to resolve these "conflicts."
Seek to assess solutions developed by the Uruguayan ecosystem under international standards concerning solution impact, data quality, etc., so that solutions assessed locally under this standard can be "exported" to other countries using the same standard.

Human Rights (Ref. Chapter 3 of the document)
The objective of this area is to identify risks that cannot be overlooked in developing public policy on Artificial Intelligence and that must require—if considered necessary—special measures because of their impact on people's rights, and which measures might be appropriate for harnessing AI systems for the benefit of people and their rights, identifying regulatory measures.
Comments

It is important to identify the cases to which it is being applied. Different disciplines should be considered to assess human rights impacts. It would be advisable to create a committee or working group specifically for this issue and its possible long-term implications.

The risk-classification approach, although appropriate, requires great caution so that it does not become a barrier to AI innovation and investment. Definitions must be precise enough to provide legal certainty and flexible enough to adapt to context. For example, a facial recognition system for monitoring citizens is not the same as one for finding missing children.

As described in Agesic's document, the current legal and institutional framework is already appropriate for managing most potential risks. Updates to the personal data protection law already prevent some potential problems.

Intellectual Property (Ref. Chapter 4 of the document)

The World Intellectual Property Organization (WIPO)27 notes that Intellectual Property refers to creations of the mind, from works of art to inventions, computer programs, trademarks, and other commercial signs.

NO COMMENTS.

Infrastructure and Cybersecurity (Ref. Chapter 5 of the document)

Artificial Intelligence development depends on several factors. One of the most important is adequate infrastructure, with the State playing a central role in this regard.

Comments

Infrastructure and technological architecture must accompany the country's AI policy strategy. Processing algorithms and maintaining control over it are key to building national capabilities and having the independence to advance this technology.

Infrastructure must be differentiated between what is available for service provision and what is intended for research and Innovation.

It is important to further develop a national strategy on what may be moved to the cloud and use its algorithms, and what may not.

Finally, interoperability platforms are needed to improve data quality and thereby system interoperability.

Work and AI Training area (Ref. Chapter 6 of the document)

The impacts of Artificial Intelligence on the world of work and on workers need to be assessed and addressed from different perspectives to take advantage of opportunities and tackle emerging challenges.

Comments

In this field, there are three main groups to train:
• Regarding retraining, workers need to be familiarized with these technologies so they incorporate them into their workplaces. This is needed for more competitive businesses and industry.
• Personnel who will develop the models need not come from technical areas.
• Raise public awareness of the strengths offered by proper use and the threats that may arise from misuse.

Civil liability and consumer rights area (Ref. Chapter 7 of the document)

The area addressed here concerns two aspects that are well regulated in law: civil liability and consumer relations.

Comments

In a technology-producing country such as Uruguay, which is committed to increasing this industry's share of the economy, it is important to provide adequate protection for AI application developers and manufacturers. Liability must be linked to noncompliance with current legal rules and cases of proven negligence. Overregulation in this field can create liabilities that impose a high barrier on entrepreneurs.

AI support measures area (Ref. Chapter 8 of the document)

The objective of this area is to consider the scope and determination of possible support measures associated with public policy on AI.

Comments

It is considered important to create spaces through public policies that encourage including this technology in industries we want to strengthen nationally. Agriculture, for example. Define policies and practices for the proper use of data and training. Create seals validating companies that apply them. These seals may

be recognized globally, improving the quality of services provided by companies, while also assuring the public that good practices are being applied.