Uruguay
Presidencia

agesic

Report Article 74 Law No. 20,212

Recommendations for an Artificial Intelligence (AI) regulation aimed at ethical development, the protection of human rights and the promotion of technological innovation

Authors: Legal Secretary and Information Society Areas

Version 1
Year: 2024

Content

Presentation.. 7

Background 9

Objectives 9

Report structure.. 10

Guidelines for the preparation of this report 11

The ethical development of AI, the protection of human rights and the democratic system.... 11

The ethical development of AI... 11

The protection of human rights and democracy in the context of AI development 15

Fostering technological innovation and the quest for AI sovereignty 18

Budgets of this report 22

International instruments on AI and lessons learned.. 23

Base definitions for the report.. 27

Entities that contributed to the preparation of the report.. 34

Thematic lines considered.. 35

General aspects 35

Institutional and governance line.. 35

Preliminary considerations 35

Selection of international backgrounds 37

Diagnosis on AI Institutionality and Governance.. 40

Human Rights Line.. 43

Preliminary considerations 43

Selection of international backgrounds 44

Diagnosis on AI and Human Rights 50

Intellectual Property Line 56

Preliminary considerations 56

Selection of international backgrounds 58

Diagnosis on AI and Intellectual Property... 59

Infrastructure and Cybersecurity Line.. 63

Preliminary considerations 63

Selection of international backgrounds 64

Diagnosis on Infrastructure and Cybersecurity for AI.. 65

Line of work and training in AI 68

Preliminary considerations 68

Selection of international backgrounds 69
Diagnosis on work and training for AI........ 69
Civil liability and consumer rights line 71
Preliminary considerations 71
Selection of international backgrounds 73
Diagnosis of civil liability and consumer rights 74
Line of measures for the promotion of AI........ 76
Preliminary considerations 76
Selection of international backgrounds 77
Preliminary diagnosis on AI promotion measures 78
Other thematic lines surveyed based on the contributions received 79
The use of AI systems for surveillance purposes 79
Insertion and international cooperation 80
Institutional and governance line........ 82
Human Rights Line........ 82
Work and training line for AI 83
Intellectual Property Line........ 83
Civil Liability and Consumer Rights Line........ 84
Infrastructure and cybersecurity line 84
Line Promotion measures........ 85
Recommendations 87
Background concepts........ 87
General recommendations........ 88
Specific recommendations........ 93
Institutionality and governance of AI 93
The role of Agesic in the institutionalization of AI 93
Institutionality of AI within organizations 95
Multisectoral and multidisciplinary perspective........ 96
Data governance 97
Ethics, Human Rights and Democracy........ 100
The starting point for the protection of human rights 100
Special measures aimed at the protection of human rights 101
Implementation of rights 104
Equality and non-discrimination........ 104
Addressing the challenges to democracies........ 105

Accessible, appropriate and effective mechanisms and resources 106

Regulation of the development, use and acquisition of AI in the public sector 107

Training and education for AI........ 108

Responsible innovation 111

Legal certainty in the aspects of civil liability and intellectual property.... 111

Infrastructure and cybersecurity........ 113

A comprehensive view of infrastructure and processes for digital transformation 115

Environmental impacts of infrastructure........ 116

Promotional measures 117

Annex 1: National background 121

Mapping of national regulations 121

Institutionality of AI........ 121

Data governance 122

Application of principles in AI 124

Intellectual Property 124

Infrastructure and Cybersecurity 127

Work and training for AI 130

Civil liability and consumer rights........ 131

Promotional 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 Artificial Intelligence 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
United States Executive Order 2023 161
European Union Artificial Intelligence Act.. 165
Annex 3: Contributions received in the consultation process 169

Presentation

The accelerated expansion of Artificial Intelligence (AI) and its potential uses and impacts has generated a deep debate about its ethical, social, economic, political, and other implications. The topic has been part of the discussions on the agendas of international and regional organizations, and national governments.

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

Article 74 of Law No. 20,212, of November 6, 2023, also establishes a deadline for this Agency to submit recommendations with these guidelines, which motivated a development process in which an attempt was made to consider different perspectives and opinions from various sectors of society.

This report and the associated recommendations are the result of this process. We at the Agency hope that they will allow for the initiation of a public debate and collective construction on an issue that undoubtedly has and will have significant and lasting impacts on our society.

Herbert Paguas

Executive Director

Background

Goals

Law No. 20,212, of November 6, 2023, established in its article 74, two major innovations regarding the regulation of Artificial Intelligence (AI) in our country:

With respect**to the National AI Strategy**, highlighted the leadership of the Agency for the Development of Electronic Government Management and the Information and Knowledge Society (Agesic) in its development and implementation, imposed the mandatory action of the Personal Data Regulatory and Control Unit (Urcdp) when personal data is involved, linked the aforementioned strategy with the National Data Strategy, defined its guiding principles, attributed a fundamental role to the participation of multiple interested parties through the potential creation of committees or groups, and established a deadline of 180 days for the preparation of this report.

With respect**to the development and implementation of AI systems**, defined the role of Agesic in the preparation of specific recommendations to public and private sector entities, including recommendations for monitoring compliance, all without prejudice to the powers of the Urcdp and other public entities in their respective areas of action.

This report was prepared based on a predefined methodology and through a process that involved the participation of officials and consultants from various public bodies, with whom, after various meetings, a consultation document was defined that was made available to other previously identified actors (bodies and private entities, academia and civil society), using for this purpose the citizen participation platform managed by Agesic.

Report structure

The report is structured in three chapters and three annexes. The first chapter describes the background of the report, its objectives, budgets, the international background considered, the basic definitions and the entities that made contributions in the first phase of the process.

Chapter two develops the thematic lines considered by this Agency, indicating in each of them some preliminary considerations, a selection of specific international backgrounds and a preliminary diagnosis, which included opinions not only from the Agency but also from the contributions of other entities. Other thematic lines that emerged from the preparation process were also included in this chapter.

Finally, Chapter Three presents the recommendations drawn up by this Agency, divided into general recommendations and specific recommendations, linked to three central aspects: institutionality and governance of AI, ethics, human rights and democracy, and responsible innovation.

Three annexes were also added to the report: the first contains a brief mapping of the most relevant regulations applicable to the thematic lines considered, the second contains a detail of international regulations in different areas, and a third contains the contributions received from the institutions that collaborated in the consultation process carried out through the citizen participation platform.

Guidelines for the generation of this report

Article 74 states that the recommendations generated must be aimed at:

- He**ethical development**of AI.
- The**protection of human rights**.
- He**promoting technological innovation**.

The following chapters will explain how the aforementioned guidelines have been reflected 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.”

Today there are other definitions, which include aspects that were not contemplated at the time of the design of this Strategy. In fact, the report raises the importance of considering definitions recognized and updated by the Organization for Economic Cooperation and Development (OECD). Thus, it is possible to anticipate that this Agency understands an AI system to be: "a system based on a machine that, for explicit or implicit objectives, infers, from the input it receives, how to generate results such as predictions,

---

[1] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-knowledge/comunicacion/publicaciones/estrategia - artificial-intelligence-for-digital-government/strategy-2 . Last accessed on 02/09/2024.

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

SOLOVE affirms[2]When looking at the links between privacy and AI, AI is an "old" technology, not unlike those that began to raise privacy concerns in the second half of the 20th century. But the difference is that today there is a larger amount of data being processed, greater computational power and better analysis mechanisms.

In the document "The governance of artificial intelligence: interim report"[3]The House of Commons Science, Innovation and Technology Committee of the English 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 (Large Language Models or LLMs) that AI became a topic of interest.[4]that AI became a general-purpose technology, accessible to everyone.

The Committee outlines 12 challenges for AI policy and framework makers: 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 of some people that AI is a threat to global life.

---

[2] SOLOVE, Daniel. "Artificial Intelligence and Privacy". 77 Florida Law Review, GWU Legal Studies Research Paper. Available at SSRN: https://ssrn.com/abstract=4713111 orhttp://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-significantopportunities-but-twelve-governance-challenges-must-be-addressed-says-science-innovation-and-technology-committee/ . Last accessed: 20/05/2024.

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

The report cited begins with an AI-generated summary, so, with that inspiration, after considering all the thematic lines and completing the process of preparing this report, ChatGPT –one of the best-known LLMs– was asked to suggest in less than 150 words what to recommend for an AI regulation oriented towards ethical development, the protection of human rights and the promotion of innovation.

Their 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 should include principles of transparency, responsibility and accountability, ensuring that automated decisions are understandable and justifiable. It is essential that AI systems respect data privacy and security, implementing mechanisms to avoid bias and discrimination. In addition, there must be constant monitoring and audit mechanisms to ensure compliance with these regulations, along with appropriate sanctions for violations.

In terms of fostering innovation, regulations must be flexible and adaptable, allowing for experimentation and technological development without imposing excessive burdens. It is crucial to encourage collaboration between public and private sectors, as well as investment in research and development. Policies must foster an inclusive ecosystem, where 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 advancement benefits the whole of society.”

Clearly one can agree with what has been expressed, but reality shows other complexities, especially in the Latin American context.

One of the most important challenges, given the potential of AI to impact how people live and function in society, is to generate an approach that contemplates certain unavoidable principles, which today are reflected in instruments issued by different national, regional and international entities.

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

CRAWFORD points out[5]From a critical perspective, “(...) 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: cleaning data sets, strengthening privacy laws or creating ethics committees. But these will always be partial and incomplete responses in which technology is assumed and everything else has to adapt to it. But what happens if we reverse that polarity and start with the commitment to a more just and sustainable world? How can we intervene to address the interdependent problems of social, economic and climatic injustices? Where does technology serve that vision? Are there places where AI should not be used, where that justice is undermined? ”

The author's questions lead us to think about the search for the underlying motivation for the use of AI, and about collective policies aimed at the conservation of common goods generated from discussion with multiple actors.

As regards the**ethical development**of AI as a guide for the report, this Agency has especially considered the Recommendation on the ethics of artificial intelligence of the United Nations Educational, Scientific and Cultural Organization (UNESCO) adopted on November 23, 2021, and which our country adhered to on June 8, 2023.[6], containing principles, but also highly relevant practical tools.

Within its scope of application, the recommendation details that the approach to AI ethics is carried out "as a systematic normative reflection, based on a comprehensive, global, multicultural and evolutionary framework of values, principles and actions."

---

[5] CRAWFORD, Kate. “Atlas of Artificial Intelligence. Power, Politics and Planetary Costs”. Fondo de Cultura Económica. First Edition. 2022. Page 342 et seq.

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

interdependent, which can guide societies in responsibly addressing the known and unknown effects of AI technologies on humans, societies, and the environment and ecosystems, and provides a basis for accepting or rejecting AI technologies."

Article 74 of Law No. 20,212 enshrines a set of principles aligned with those resulting from the aforementioned recommendation and other international instruments that will be mentioned, namely: equity, non-discrimination, responsibility, accountability, transparency, auditing and safe innovation, respect for human dignity, the democratic system and the republican form of government, and the principles of data protection enshrined in Law No. 18,331 of August 11, 2008 (legality, veracity, purpose, prior informed consent, data security, confidentiality and responsibility).

Given that AI ethics is related to compliance with these principles, which enable the safe and responsible development of systems based on this technology, this Agency believes that we should focus on its effective application, giving concrete examples to do so.

Protecting human rights and democracy in the context of AI development

The second orientation that article 74 raises is the**protection of human rights**. This technology, or any other past or future technology, should not penetrate a legal system that has been built through the recognition of rights inherent to the human person and the republican form of government, enshrined in current national and international instruments.

From this perspective, and as will be mentioned later, this Agency considers it necessary to start by considering the set of obligations derived for States from international human rights law: the duty to respect, the duty to protect and the duty to comply, adopting all measures within their reach to ensure the realization of rights. In line with this approach, it is considered pertinent to highlight the need not only to protect people from possible harmful effects of AI, but also to exploit its potential effects.

potential to promote beneficial effects in the lives of these people and in the development of our societies.

There is a consensus in regional and international instruments to place the human person and the defense of his or her rights at the center of any normative development. PEREZ COMENALE[7]It points out that there is an emphasis on the protection of fundamental rights, with the human being as the center of regulation, and highlights the need to preserve principles linked to the protection of personal data, 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 wants to place special emphasis on the impacts of AI on the democratic system, following the opinion of INNERARITY[8], who seeks to concretize UNESCO's ethics recommendations with this focus. From this perspective, he raises how automatic decision-making systems affect the normative principles of democratic self-government, expressly pointing out that: “The problem is to what extent and in what way algorithmic institutionalism characterized by the use of automated decision-making systems (ADS) is compatible with what we consider a political decision-making system.”

The author provides various recommendations such as education and awareness, regulation and legislation - where he assigns a leading role to future parliamentary commissions to develop prospective work -, public participation and 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 multi-stakeholder approach and the development of global frameworks.

---

7 PEREZ COMENALE, Agustina. “ChatGPT. Challenges and opportunities of Generative Artificial Intelligence. Challenges of its regulation”. Digital book, EPUB. Granero H., et al. 2023. Page 105.

[8]INNERARITY, Daniel. “Artificial Intelligence and Democracy”. Year 2024. Available in: https://unesdoc.unesco.org/ark:/48223/pf0000389736_eng

The ability of people to freely participate in democratic life has also been considered when analysing the impact of AI in other areas such as neurotechnology. It is true that the synergy between AI and neuroscience has allowed for substantial advances that must be promoted responsibly, but this has also increased the risks of manipulation of people and their individual autonomy. These reflections are part of the Working Document "Towards a draft text of a recommendation on the ethics of neurotechnology" prepared by the Ad Hoc Group of Experts established within the framework of UNESCO.[9][10].

Focusing on neurotechnology, AI and the impact on the way people analyze and make decisions allows us to visualize that potential uses will leave behind any regulatory attempt that is not based on flexible and adaptable instruments.

The European Parliament[11]It also raises the importance of applying AI tools to improve political engagement and empower people, giving political operators the ability to better understand people's demands through different systems, and provide personalized responses to those demands. It also raises risks, such as disinformation, deepfakes, and other mechanisms that can affect political campaigns and influence public opinion.

The European Parliament thus proposes a set of tools to counteract the negative impacts of AI, including tools for automatic detection of AI-generated content, watermarks,

---

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

[10] Additionally, it should be noted that UNESCO has made available a first version of the recommendation on the ethics of neurotechnology, which is open to 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 in: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf . Last accessed: 15/6/2024.

tools to check information on social networks, and in particular, regulations aimed at mitigating the risks of AI.

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

We agree with the explanatory report, which states that the integrity of democracy and its processes are based on the ability of people to form an opinion and act accordingly, as well as to impact the decisions made by their representatives. Therefore, some recommendations indicated in the report are worthy of consideration, such as the adoption of cybersecurity measures against malicious foreign interference in electoral processes, or against the dissemination of disinformation, all while taking care not to affect pre-existing fundamental rights such as freedom of expression, association and assembly.

It is therefore about having the ability to recognize and assess the impacts of AI on people, on their rights, and on our system in general, promoting the development and application of tools that facilitate democratic discussion without undue influences on people's behavior, and others that**collaborate**with the political spectrum to understand the needs of the community and society, and based on this, make informed and fair decisions.

Fostering technological innovation and the quest for AI sovereignty

Finally, the**promoting technological innovation**It is precisely related to the benefits that this technology can have for economic development, but

---

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

also social of our populations, particularly at the national and regional level in Latin America.

Technological innovation emerges in our country as a basis for the adoption of different strategies and the promotion of different benefits included in current legal and regulatory provisions.

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 in products or processes that result in greater economic value."

At this point, the Agency wishes to focus on some aspects that it considers central to this orientation: institutionality, strategic objectives, instruments or tools, financial support and infrastructure.

In terms of institutionality, it is worth mentioning first of all the National Agency for Research and Innovation, created by article 256 of Law No. 17,930, of December 19, 2005, which saw various aspects of its organization modified by Law No. 18,084, of December 28, 2006, which also created the National Council for Innovation, Science and Technology (CONICyT), made up of various entities linked to science, technology and innovation.

More recently, the aforementioned decree No. 216/023 created the Uruguay Innovation Hub (UIH) program, which includes among its multiple objectives the strengthening of the innovative ecosystem.

This institutionality is complemented by other multiple public entities focused on the development of innovation such as the University of the Republic, the Technological University of Uruguay, the Ceibal Center, the Technological Laboratory of Uruguay, the National Directorate of Innovation, Science and Technology of the Ministry of Education and Culture, the National Development Agency, the Agency for Monitoring and Evaluation of Public Policies, Agesic itself, among others, which in one way or another have among their duties the promotion of innovation within and outside the public sector.

On the other hand, when we talk about strategic objectives, we refer to the intention, preferably expressed in the form of legal regulations, 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.

The indicated 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. The provision of funds for this type of projects is essential and must be part of the discussion when talking about promoting innovation in AI.

Also in regulations subsequent to Law No. 16,906, of January 7, 1998, aspects of technological innovation were included for the granting of the benefits that this law provides, within the scope of investment promotion.

As regards tools for innovation, it is worth highlighting the figure of controlled testing environments - regulatory sandboxes -, through article 75 of Law No. 20,212, in the process of regulation, which will become a fundamental instrument for testing and developing products and services in a controlled manner, before they are put into production.

But the promotion of innovation also comes hand in hand with an adequate infrastructure, which should ensure that the country has the capacity not only to produce technologies but also to maintain and evolve them, generating the necessary technical and educational capabilities internally.

Linked to this, although more broadly, the concept of **AI sovereignty.**This has been described by BELLI[13]as “(...) the ability 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 04/30/2024.

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

The author proposes a framework of interconnected elements (defined as KASE for the acronym in English "Key AI Sovereignty Enablers") that will allow a country to determine its sovereignty in the matter, and which refers to: adequate governance of personal data and algorithms, strong computational capacity, significant connectivity, reliable electrical power, a digitally educated population, solid cybersecurity and an appropriate regulatory framework.

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

The argument of sovereignty in AI should be considered especially when promoting regulatory initiatives. In this regard, the Montevideo Declaration on Artificial Intelligence and its impact on Latin America[16], signed on March 10, 2023 on the occasion of the Khipu event, maintains that it is essential to strengthen the sovereignty of Latin American countries with respect to strategic and regulatory issues of AI, understanding that the training of people at the highest level and the development of critical thinking are crucial.

---

[14] In the aforementioned original, BELLI points out that it 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: 04/30/2024.

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

Budgets of this report

The question that inevitably arises and that this Agency does not intend to avoid is: does our country need an Artificial Intelligence law?

It is the opinion of this Agency that the law is not the only applicable regulatory instrument, and that any eventual legal regulation, if any, should focus not on the regulation of a technology per se, but on the potential and effective positive and negative impacts on people and society, without limiting innovation and technological development.

It must be acknowledged that Uruguay has a regulatory base in several aspects involved in the ethical development of technology, human rights and the promotion of innovation. It is necessary to continue the discussion, and to rely on international provisions and commitments assumed by our country that provide a framework for protection and promotion of innovation and the development of responsible AI. We must think about complementary regulation in aspects that significantly impact people's lives and the development of our societies. Therefore, we will try to provide a proposal for guidelines on how and in what way to carry out this discussion.

DANESI points out[17] that "we need legislation on artificial intelligence, but not just any legislation, because otherwise we run the risk of slowing down innovation and leaving our countries outside of progress", proposing to this end a series of instances of dialogue, analysis and diagnosis with the participation of multiple actors and with a focus on high-risk AI systems.

In the Agency's view, this is not a matter of a dichotomy between regulating or not regulating, but rather of answering the question: what to regulate? On this basis, the recommendations presented in this report are based on three assumptions:

1. **What we understand by "technological regulation" should not be associated with the regulation of a technology in itself but with mitigating impacts**

---

[17] DANESI, Cecilia. "The Empire of Algorithms". Kindle Edition. Pages 215-216.

negative or promote positive impacts on people and/or society. As a corollary to this conception, it must be stated that with regard to the scope of the concept of "regulation", it includes a range of normative instruments in a broad sense, not limited to laws or regulations, but also extends to other "soft" instruments, such as protocols, guides, recommendations, codes, etc.

2. **Any eventual regulation of the negative impacts of technology in general and AI in particular must be human-centred and based on the defence of our society and our democratic system.** Limitations should be expressly legally established, strictly necessary and proportional to ensure legitimate objectives in a democratic society.

3. **Any eventual regulation of positive impacts, on its part, should focus on meeting those objectives that we define as strategic at the country level, in order to be more efficient in the allocation of the limited resources available and to generate and promote the structural conditions necessary for such compliance.** The measures adopted may have different scopes, from general to sectoral, and our level of success will depend on their proper determination.

International instruments on AI and lessons learned

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

In particular, the OECD Council Recommendation on Artificial Intelligence[18] establishes a set of definitions regarding what we should understand by AI System, AI Life Cycle, AI Knowledge and AI Actors - to the

---

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

- which will be referred to in the following chapters - as well as a set of principles applicable to it[19].

This organization also made recommendations for the development of national policies and international cooperation aimed especially at small and medium-sized enterprises (SMEs), namely:

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

2. Promote the digital ecosystem for AI (promoting in particular mechanisms such as data trusts to share information in a legal, ethical and secure manner);

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

4. Building capacity and preparing for the transformation of the labour market (working with various actors to prepare society and the world of work by empowering people, developing training programmes and improving worker safety and promoting entrepreneurship, among others);

5. Cooperate internationally for trustworthy AI (cooperation with other countries and actors, working on common initiatives, using internationally comparable metrics and collecting evidence, among others).

---

[19] At the time of this drafting, Uruguay is in the process of adhering to these principles.

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

Just for reference[21], the Hiroshima AI Process overarching policy framework consists of four pillars: 1. Analysis of 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 in support of the development of responsible AI tools and best practices.

As mentioned, Uruguay recently joined[22]to UNESCO's Recommendation on the Ethics of AI[23], a framework that was adopted by its 193 members, and based on 4 fundamental values: 1. Human rights and human dignity; 2. Living in peaceful, fair and interconnected societies; 3. Ensuring diversity and inclusion; 4. Flourishing of the environment and ecosystems. This recommendation encourages a dynamic understanding of AI, defining it as “those systems with the capacity to process data in a way similar to intelligent behavior.”

For the purposes of the commissioned report, two aspects of the Recommendation are worth highlighting. Firstly, the definition of 11 significant areas for the adoption of relevant actions by governments, in order to move from high-level principles to practical strategies. These areas of action and the strategies proposed by UNESCO help to determine the steps to be taken.

---

[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-knowledge/comunicacion/noticias/uruguayadhiere-recomendacion-etica-inteligencia-artificial-unesco . Last accessed on 02/09/2024.

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

continue to structure a regulatory framework that considers other aspects beyond the institutional ones that are impacted by AI in our societies.

Secondly, it should be noted that the Recommendation proposes two practical methodologies that collaborate in its implementation: the Readiness Assessment Methodology (RAM) and the Ethical Impact Assessment (EIA). In particular, the RAM raises questions on issues such as AI regulations and infrastructure at the country level to enable the accessibility of AI technologies, and aims to collaborate in determining the regulatory and institutional changes necessary to take advantage of and also protect against the use of these technologies.[24].

At the time of writing this report, Uruguay is being evaluated within the framework of the aforementioned methodology, with the collaboration of the Development Bank of Latin America (CAF).[25].

More recently, the adoption of Resolution A/RES/78/265 by the UN General Assembly should be mentioned for its relevance.[26], which calls on all States Parties and other organizations from 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 a number of other initiatives that impact the way AI systems will be treated internationally, and these will be mentioned in more 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-esteano . Last accessed on 02/09/2024.

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

[26] UN – General Assembly. Resolution adopted by the General Assembly on 21 March 2024. 78/265. “Harnessing the opportunities of safe and trusted 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.

Base 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 present some fundamental concepts that contribute to understanding the characteristics and operation of these systems.

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

In response to the need for a technical definition that reflects what AI systems are today, while at the same time ensuring that it is flexible in the face of constant technological advances, on 8 November 2023 the Organisation 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 and agreed definition in this area has formed the technical basis for various processes at the international and regional level.

As noted, for the purposes of this document the revised OECD definition will be adopted, which is as follows: “a machine-based system that, for explicit or implicit purposes, 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 adaptability after deployment.”[27]” (Unofficial translation[28]).

---

[27] OECD, OECD Recommendation on AI, OECD/LEGAL/0449, 2019, as 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 analysed 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 other, simpler software systems that make it possible to execute operations automatically based on rules established by natural persons.[29]. It has formed the basis for the definitions of AI systems established by the European Union's Artificial Intelligence Regulation.[30], and the Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law[31]adopted within the framework of 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 that affect real or virtual environments.

---

[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/artificialintelligence/cai. Last Accessed: 4/16/2024.

[30] Article 3 of the European Union's Artificial Intelligence Regulation sets out the following definition: "'AI system' means a machine-based system, designed to operate with varying levels of autonomy, that can demonstrate adaptability after deployment and which, for explicit or implicit purposes, makes inferences from the input it receives how to generate output information, 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 in:https://rm.coe.int/-1493-10-1b-committeeon-artificial-intelligence-cai-b-draft-framework/1680aee411 . Last accessed: 16/4/2024.

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

AI systems are designed to operate with different levels of autonomy” (unofficial translation[33]).

According to the agency, the modifications 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 received by the system can 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 they are designed and deployed.

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

- While it is always possible to trace the goal setting and development of an AI system back to a human originating the AI system development process, some types of systems may develop implicit subgoals, and sometimes set goals for other systems.
- While human oversight can occur at any stage of the AI system lifecycle, some AI systems may generate results

---

[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 objective of the AI system and without specific instructions from humans.

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

- The reference to "infer" should be understood as "generating outputs" from inputs. Whereas the concept of output(s) refers to the results generated by an AI system that vary depending on the different capabilities and functionalities they perform.

In short,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 purposes, 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 adaptability after deployment.

AI System Life Cycle: The phases of the AI system lifecycle involve: i) "design, data and models"; which is 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 typically occur iteratively and are not necessarily sequential. The decision to decommission an AI system can occur at any time 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 contribute to understanding the characteristics and operation of AI systems are discussed 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), “ML 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 instruct 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 for itself in the data.”[36].

The model is trained from input data that can be labeled (supervised machine learning) or unlabeled (unsupervised machine learning). A third type is called 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_eng . Last accessed: 16/4/2024.

[37] UNESCO (2021). Artificial Intelligence and Education. A Guide for Policymakers, 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.

According to 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, which are usually organized in layers. Each node receives data from nodes in the lower layer and sends data to nodes in the upper layer.[39].

Deep Learning

Deep learning has been defined by UNESCO as a cutting-edge machine learning technique that “allows the machine to recognize complex concepts such as faces, human bodies or images of cats by itself, by scanning millions of images extracted from the Internet, without these images being previously labeled 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 AI is a subset of Deep Learning. Generative AI learns patterns in content in order to generate new content. The output of the AI will be based on the massive data that the model was trained on.

---

[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_eng . 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_eng . Last accessed: 16/4/2024.

[40] UNESCO. Lexicon of Artificial Intelligence. Available at:https://www.unesco.org/es/articles/lexico-de-la-inteligenciaartificial-0 . Last accessed: 16/4/2024.

trained. New content can be presented in different formats, texts written in natural language, images, audio, and software code.

In the words of UNESCO, “Generative AI is an artificial intelligence technology that automatically generates content in response to instructions written in conversational natural language interfaces (prompts).”[41].

The techniques used in generative AI vary.

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

In a similar vein, the October 2023 US Executive Order On Safely and Trustfully Developing and Using Artificial Intelligence states that generative AI “means the class of AI models that emulate the structure and characteristics of input data to generate derived synthetic content. This may include images, videos, audio, text, and other digital content” (unofficial translation)[42].

Foundational or general-use models

They are models with broad capabilities that adapt to different scenarios.

In the European Union AI Regulation they are defined as an AI model trained with a large volume of data using large-scale self-supervision.

---

[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_eng . Last accessed: 16/4/2024.

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

scale, which exhibits a considerable degree of generality and is capable of competently performing a wide variety of different tasks; it can be integrated into various downstream systems or applications[43].

Entities that made contributions to the preparation of the report

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

Likewise, contributions were received in the consultation process from the Association of Notaries of Uruguay (AEU), the Data and Society Laboratory (DATYSOC), DATA Uruguay, the Uruguayan Chamber of Information Technologies (CUTI) and the National Institution of Human Rights and Ombudsman (INDDHH).

Although not all the recommendations of those who responded to the consultation were collected, it was considered necessary to add the documentation submitted to illustrate the different perspectives raised, which is included in the Annex to this report.

---

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

Thematic lines considered

General aspects

In preparing the report, and considering the progress and inputs obtained from the review and creation processes of the National Data and AI Strategies respectively, the following thematic lines were defined:

- Institutionality and governance
- Human Rights
- Work and training
- Intellectual Property
- Civil liability and consumer relations
- Infrastructure and cybersecurity
- Promotional measures

The scope of these lines is reproduced in the following pages.

Institutionality and governance line

Preliminary considerations

The objective of this line is to determine the fundamental aspects to ensure adequate institutionalization of AI in our country.

AI institutionality and data institutionality, as well as AI governance and data governance, are inextricably linked, derived from the dependency relationship that the former has with respect to the latter. In this line, Agesic proposes to raise institutionality from the perspective of the structure necessary for the development, monitoring and auditing of a public policy on AI and data, from the competencies required within public organizations, and from the standards that today already regulate the way in which data is governed at a national level.

With regard to the institutionality for AI, it is important to consider international precedents, but under the prism of local idiosyncrasy, as long as the structures that may be applicable in other countries or regions effective, they may not be efficient or may be directly inappropriate for our country, and vice versa.

An example of dissimilar structures linked to data management, and also to AI, is the way in which the organization of personal data protection has been regulated. In our country, Law No. 18,331, of August 11, 2008, creates a decentralized body of Agesic, called the Personal Data Regulatory and Control Unit (Urcdp), with the authority to determine its own budget and technical autonomy, while remaining under the hierarchical structure of the Presidency of the Republic.

In other Latin American countries, there are autonomous entities –just look at the Agency for Access to Public Information in Argentina, the National Data Protection Authority in Brazil, or the National Institute for Transparency, Access to Information and Protection of Personal Data in Mexico– or entities dependent on Ministries –as in the case of Colombia, where the data protection entity is a delegation of the Superintendency of Industry and Commerce of the Ministry of Commerce, Industry and Tourism–. Some of these entities have shared powers related to data protection and access to public information, some have sanctioning powers for the entire spectrum of those responsible, and others distinguish between public and private entities.

This set of differences does not prevent them from carrying out their activities in their respective national jurisdictions, representing their countries in this area, making recommendations and imposing the corresponding sanctions for non-compliance with the Law.

The objective of this development is to clarify that the institutionality of AI in Uruguay must consider the international and national antecedents associated with the topic, but we reiterate, analyzed in light of the local idiosyncrasy.

Along with AI institutionalization, it is essential to consider data governance, as this is one of the essential elements for the development of AI systems. Data governance includes different types of data.

of data – personal and non-personal –, its management, the entities that generate and manage this data, its reuse, interoperability, and, ultimately, the standards to be met by both the public and private sectors for the use of data when it feeds or is generated by AI systems.

Selection of international backgrounds

The current text of the Council of Europe (CoE) AI Convention[44]Article 1 establishes that the parties must adopt and maintain appropriate legislative, administrative or other measures to give effect to the provisions of the Convention, which must be graded and differentiated based on the severity and probability of occurrence of adverse impacts on human rights, democracy and the rule of law. The Convention raises, with nuances, the applicability of its provisions to the public and private spheres.

In terms of innovation, the Convention provides for the possibility of establishing controlled environments for the development and experimentation of 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 test environments or regulatory sandboxes, which is currently being regulated by Agesic in collaboration with other entities.

Transparency under the Convention is a central principle; that people are effectively aware that they are interacting with an AI system, and oversight mechanisms are an integral part of that transparency.

Regarding the European Regulation on AI[45], its Title VI refers to the governance of AI, creating in the chapters that comprise it the European Committee on Artificial Intelligence (a community body made up of national supervisory authorities), with powers to assist national authorities, coordinate guidelines 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 Regulation refers to the Competent National Authorities, which are responsible for ensuring the application and execution of the Regulation and 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 current legal standards and requirements.

The European AI Regulation or EU AI Law is part of a set of regulations that refer to data governance and that seek – within the framework of the European Data Strategy[46]- create a single market where data flows freely between different sectors of society. This ecosystem is made up of the Digital Services Act, the Digital Governance Act, the Digital Markets Act, the Data Act, the e-Privacy Regulation and the GDPR (European General Data Protection Regulation).

In the United States, we find the Executive Order on the safe, reliable and trustworthy development and use of Artificial Intelligence systems[47]. It emphasizes 8 principles that must be complied with by Federal Government entities to achieve the desired objectives and establishes a set of actions that must be adopted by different federal government agencies in their respective areas of competence, linked to AI. An exclusive central authority with competence in AI is not foreseen, but rather a distribution of issues associated with AI in the institutions that normatively have competence for it.

The influence of the People's Republic of China in this matter cannot be ignored, which, in addition to pre-existing regulations on cybersecurity and personal data protection, has promoted measures for the regulation of AI in general, and generative AI in particular. Specific measures are thus foreseen on transparency in the use of AI systems, safeguards against certain uses, approval

---

[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-andtrustworthy-development-and-use-of-artificial-intelligence/ . Last accessed 19/3/2024.

government for listed uses, prevention of discrimination, exercise of rights by users, and responsibilities punishable by fines[48].

The United Kingdom, for its part, published a document with a pro-innovation approach to AI regulation[49], which emerged after a public consultation carried out over a period of 1 year. Additionally, the United Kingdom created an Office for Artificial Intelligence that is part of the Department of Science, Innovation and Technology, and a Responsible Adoption of Technology Unit. In particular, the latter aims to promote responsible innovation in the public and private sectors, developing tools that allow building trust within organizations in AI and data management systems. Previously and until June 2023, it had an AI Council made up of experts from multiple sectors, which aimed to contribute to the development of the AI strategy.

The UK government now also has a Central Digital and Data Office which leads the digital, data and technology functions for the government and works in particular on developing AI policy and strategy, including standards for government use.

In all these provisions, a particular emphasis is observed on the way data is used and on the principles that should guide regulations. There is also a tendency to generate governance schemes with the participation of multiple actors, without prejudice to the leadership of an organization within the state structure.

---

[48] A summary of what to expect from Chinese regulations can be found in the Parliamentary Observatory, Asia Pacific Program of the National Library of Chile, available athttps://www.bcn.cl/observatorio/asiapacifico/noticias/andamiajeinstitucional-inteligencia-artificial-china . Last accessed: 06/21/2024. Additionally, an English translation of the legislative proposal can 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-proinnovation-approach-to-ai-regulation-government-response . Last accessed 19/3/2024.

There is also a need to place strong emphasis on the innovation component (responsible) and to guarantee the protection of human rights, with the training of technical bodies linked to this regulatory entity being a central element.

Diagnosis on AI Institutionality and Governance

In accordance with the standards surveyed, from an institutional point of view there are two entities with responsibilities for establishing general criteria in this area: Agesic and Urcdp.

Article 74 of Law No. 20,212 provides for the design and implementation of the Data and Artificial Intelligence Strategy, with Agesic in charge of its leadership. Within the framework of these powers, the Agency is given the possibility of creating working groups and other bodies with different actors that collaborate in the implementation of the strategies.

Based on this article, Agesic recently created the**Public Sector Strategic Committee for Artificial Intelligence and Data,**composed of representatives of said 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 Institute of Statistics, the National Institute of Human Rights and Ombudsman, the National Agency for Research and Innovation, and the Personal Data Regulatory and Control Unit.

In addition, the final paragraph of article 74 provides for a task that goes beyond that linked to the strategy, and refers to the development of artificial intelligence systems, for which Agesic may establish criteria and define mechanisms for monitoring compliance. Specifically, this paragraph states: “AGESIC will make specific recommendations to entities in the public and private sectors for the development and implementation of the aforementioned artificial intelligence systems, and for monitoring their compliance, without prejudice to the powers of the URCDP and other public entities in their respective areas of action.”

Consistent with this provision, it is established that this competence is without prejudice, first of all, to the competences of the Urcdp, which can determine criteria for the use of personal data in any processing operation, and especially those established in article 16 of Law No. 18,331 - automated processing that generates, among others, profiles of people -, in accordance with article 34 of the aforementioned Law.

In terms of institutionality, it is appropriate to mention within this diagnosis the reflections emerging from the consultation process. The INDDHH proposes, for its part, that, in light of the powers assigned to Agesic and the Urcdp for establishing general criteria and oversight, its scope of action should be situated outside the Executive Branch, specifically suggesting that it be given the legal form of a decentralized service.

In this regard, it is the opinion of this Agency that, although the proposal is understandable and acceptable, the existing institutional framework would allow for adequate governance of AI, at least at present. Notwithstanding this, the complete proposal of the INDDHH is attached as an annex, for consideration by the Legislative Branch.

In its contributions, CUTI states that the existing institutions in Uruguay would be adequate to address the challenges posed, without prejudice to the need to have advisory groups with the participation of multiple actors and a relevant role in defining policies.

For AI governance and the adoption of this technology to be reliable and responsible, measures for adequate data governance and management must also be considered. Data is one of the main inputs of this technology and its main result. In turn, for data to be reliable and usable, it is important to ensure that it is adequately managed, defining and adopting regulations, policies and guidelines, for which it is relevant to consider national, regional and international standards on the matter.

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

There are certain Agesic competences in this field, such as the rules on information exchange and interoperability, open government and open data, which were compiled in Decree No. 184/015, of July 14, 2015. Likewise, the decentralized units of the aforementioned Agency, the Urcdp and the Public Information Access Unit (Uaip) have competence at the national level with regard to the management of personal information and public information, respectively.

The contributions to the consultation were oriented towards suggesting specific mechanisms for data protection (such as the analysis of data trusts proposed by the INDDHH), the adoption of mechanisms to resolve conflicts between the promotion of innovation in the development of public services and the impact of a possible failure in this area (CUTI) and the generation of standards that allow the evaluation of Uruguayan solutions and their "exportation" (CUTI).

In relation to the way in which AI systems are used, the AEU mentions the importance of considering specific sectors or uses, specifically in the judicial field (proposing "white box" systems based on techniques to make intelligent predictions, classifications and detections), scoring (emphasizing the impossibility of using data that is not part of those used for the specific purpose and the need for explainability) and in the contractual and notarial field (where they advise against the use of synthetic data).

Human Rights Line

Preliminary considerations

The objective of this line is to raise the risks that cannot be ignored in the development of a public policy on AI, and may require - if deemed necessary - special measures, due to their impact on people's rights.

Additionally, the objective is to identify measures to harness AI systems for the benefit of people and their rights, identifying in particular regulatory measures.

For this purpose, the related international standards and obligations of international human rights law ratified by the country, the specific recommendations on AI made by international organizations and the regulations in force or in the process of being developed at the regional and international level will be considered.

The impacts of AI on human rights have been part of the analyses carried out in different forums. The United Nations High Commissioner for Human Rights, Volker Turk, at the High-Level Side Event of the 53rd Session of the Human Rights Council[50]He noted that in our world and at this time, human rights are being put to the test, and that the question of where the limits of AI are is one of “(...) the most pressing issues for our society, for governments and for the private sector.” The High Commissioner points out that there are two schools of thought on the regulation of AI: a) one of them focuses on risks, self-regulation and self-assessment by developers, which places a very large responsibility on the private sector; b) the second is an approach that integrates human rights throughout the entire AI life cycle, incorporating human rights principles from “(...) the collection and selection of data; as well as the design,

---

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

development, implementation and use of the resulting models, instruments and services.”

The High Commissioner makes some proposals in this regard: 1) listening to groups that are most vulnerable to the use of this technology; 2) paying attention to the use of AI in public and private services where there is a greater risk of abuse of power or intrusion into privacy; 3) requiring an assessment of risks and repercussions for human rights before, during and after the use of AI systems (transparency, independent oversight and access to effective remedies); 4) prohibiting or suspending AI technologies that do not comply with international human rights standards; 5) applying data protection regulations and other existing sectoral protection legislation; 6) not allowing an approach based solely on self-regulation; 7) creating an international advisory body.

In our country and in relation to the Human Rights policy, special mention should be made of the National Human Rights Plan 2023-2027, which includes the impact of artificial intelligence, among others, and the need to move towards the ideals of the Universal Declaration of Human Rights. This Plan complements the aforementioned objectives by establishing mechanisms for articulation, regulatory frameworks, and action protocols that allow the incorporation of the human rights approach in public policies such as the one that is intended to be institutionalized in the subject of AI. Based on this, it seems relevant to accompany the development of the proposed guidelines in order to include the subject of AI in the defined objectives.

Selection of international backgrounds

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

Likewise, this recommendation considers the following instruments: the Universal Declaration of Human Rights (1948), the instruments of the international human rights framework, including the Convention on the Rights of the Child (1998), 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. Note is also taken of the Declaration on the Right to Development (1986); of the Declaration on the Responsibilities of 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 Preservation of and Access to Documentary Heritage, including Digital Heritage (2015); the Declaration of Ethical Principles in Relation to Climate Change (2017); the Recommendation concerning Science and Scientific Researchers (2017); of the Internet Universality Indicators (adopted in 2018 by UNESCO’s International Programme for the Development of Communication), including the ROAM principles (adopted by the UNESCO General Conference in 2015); of the Human Rights Council resolution on “The right to privacy in the digital age” (A/HRC/RES/42/15) (2019); and of the Human Rights Council resolution entitled “New and emerging digital technologies and human rights” (A/HRC/RES/41/11) (2019).

Based on this background, UNESCO recommends that member states apply appropriate measures – legislative and others – to give effect to the principles and standards developed in accordance with international law, and in particular international human rights law.

The recommendation makes clear in particular that AI systems should improve the quality of life of human beings, who should not suffer any type of harm at any stage of their life cycle. It also emphasizes the need to have means to promote, defend and exercise human rights. A set of principles are proposed for this purpose: proportionality and harmlessness, security and protection, equity and non-discrimination, sustainability, right to privacy and data protection, human supervision and decision-making, transparency and explainability, responsibility and accountability, awareness and education, and adaptive governance and collaboration of multiple stakeholders. These principles are associated with specific measures that will be analyzed later, highlighting 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 analyse the benefits, challenges and risks of AI systems, as well as appropriate risk prevention, mitigation and monitoring measures, among other safeguards. Such impact assessments should disclose the impacts on human rights and fundamental freedoms, including, but not limited to, the rights of marginalised and vulnerable persons or those in vulnerable situations, labour rights, the environment and ecosystems, as well as the ethical and social consequences, and facilitate citizen participation, in accordance with the values and principles set out in this Recommendation."

As mentioned above, the recent UN General Assembly resolution[51] for the promotion of safe and reliable AI systems that

---

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

enable the Sustainable Development Goals (SDGs) to be achieved, and contains in particular recommendations for measures to be adopted by Member States.

Also within the UN framework, the December 2023 document "Interim Report: Governing AI for Humanity" deserves special mention.[52], which contains, among others, a categorization of risks from the perspective of existing or potential vulnerability for people, groups, the economy, (eco)systems, values and norms, and society. This goes beyond the consideration of a guiding principle of AI governance, which are international human rights standards, and the commitments assumed in the SDGs.

Continuing with international precedents, the community regulation of the European Union, approved by the member countries on March 13, 2024, establishes some relevant aspects highlighted by the organization itself.[53]:

1) Rules for different types of Risks:

   a. Unacceptable risks, prohibited because they constitute a threat to people: cognitive manipulation of the behavior of vulnerable groups of people, social scoring, biometric identification and categorization of people,
   remote and real-time biometric identification – in this case there are exceptions based on police purposes.

   b. High risks, which are divided into two categories and require an assessment prior to their production: i. systems used in products that are covered by EU product safety legislation (toys, aviation, automobiles, medical devices and elevators); ii. Systems for hazardous areas

---

3%20because%20they%20also%20benefit%20sustainable%20development%20for%20all . Last accessed: 25/03/2024.

[52] Available in
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 about this:https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificialintelligence . Last accessed: 24/03/2024.

specific ones that must be registered in an EU database (Management and operation of critical infrastructure, Vocational training and education, Work, management of workers 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 interpretation and legal application of the law)

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

a. Reveal that the content was generated by AI

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

c. Publish summaries of copyrighted data used for training

In the case of high-impact general AI models that may generate a systemic risk, they must be evaluated and, if they suffer serious incidents, they 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 this fact.

3) Support for innovation. This is achieved by creating conditions that encourage the testing of AI models prior to their implementation into production.

In the case of the United Kingdom, the regulatory project presented and put out for public consultation last year aimed to achieve a pro-innovation and pro-security approach.

The project distinguishes 3 categories of risks: 1) social risks; 2) risks of misuse; 3) risks of autonomy. The former include the world of work, innovation and intellectual property, the protection of people from bias and discrimination, the protection of personal data, trust and security in online content, ensuring competition in the digital world, and the protection of the environment.

digital markets, best practices in the public sector. As for the second type of risks, safeguarding democracy from interference in electoral processes and preventing the misuse of technology are mentioned. Finally, as for the last type of risks, the scope of human control over AI systems is mentioned.

The distinction in risks is also present in projects that are being discussed at the South American level, such as project No. 2338[54]of the Federative Republic of Brazil, in which they distinguish high 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 to Parliament on May 7, 2024[55]which also distinguishes between AI systems with unacceptable risk, those with high risk, and adds systems with limited risk.

In October 2023, the United States government issued an Executive Order on the Safe and Trusted Development of Artificial Intelligence to be enforced by government agencies[56]. The measures envisaged in the Executive Order include the creation of security standards, the protection of the privacy of Americans, advancing civil rights and equity, protecting consumers, patients, and students, supporting workers, promoting innovation and competition, advancing U.S. leadership abroad, and ensuring responsible and effective government use of AI (the measures are presented in greater detail in the international regulations annex).

---

[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-andtrustworthy-development-and-use-of-artificial-intelligence/ Last accessed: 24/03/2024.

Diagnosis on AI and Human Rights

The diagnosis in this line focuses on 5 central aspects, linked to the points mentioned by the United Nations High Commissioner for Human Rights, and detailed above.

1. Is it necessary to strengthen the application of pre-existing human rights standards and principles through regulatory instruments that explain and specify their application in the field of AI in a transversal manner and/or as pillars of national policy beyond the provision established in Art. 74 for the National Strategy on AI?

2. Can self-regulation be an effective remedy to guide the actions of public and private entities in the development of AI?
3. Is the risk approach sufficient?,And as a corollary, are there AI systems that, due to their impact on people's rights, should be prohibited or limited, or that require the imposition of special measures?
4. What guarantees of transparency and explainability should be established in the framework of the development of human-centred AI systems?
5. What are the guiding criteria for defining a public policy associated with the development of AI in our country that also allows for enhancing the positive impact on human rights?

Regarding the scope of the application of the principles, currently in accordance with the provisions of article 74 of Law No. 20,212, these are applicable to the design and development of the National Strategy for Artificial Intelligence and Data. Now, and without prejudice to the norms of international human rights law ratified by the country and the derived international obligations are fully applicable, to the extent that these principles were provided for in relation to the development of the aforementioned Strategies, it is appropriate to consider whether it is pertinent to explain them normatively with a broader scope.

broad. That is, specifying its normative content specifically in relation to the AI policy.

As mentioned, the principles included in Article 74 are aligned with those enshrined in the first International Convention on the subject prepared by the CoE. This Convention highlights the principles of human dignity and individual autonomy, transparency and oversight, responsibility and accountability, equity and non-discrimination, privacy and protection of personal data, trust and security, and safe innovation. The aforementioned principles apply, according to the definition of the Convention, to all AI systems throughout their life cycle.

With regard to the risk approach, this perspective is already present in the regulation of personal data protection, which may also be applicable to AI systems when this type of data is used or generated.

Thus, Article 12 of Law No. 18,331, as amended by Article 39 of Law No. 19,670 of October 15, 2018, provides for the performance of impact assessments on the protection of personal data. Article 6 of Decree No. 64/020 of February 17, 2020 provides for the performance of these assessments in the case of processing of personal data that generates greater risks for individuals, and Article 7 indicates the minimum content of the instrument, emphasizing the risk assessment and the security measures to be adopted.

By way of example, Article 6, paragraph c of the aforementioned decree provides for the mandatory performance of impact assessments for processing involving: “(...) an assessment of personal aspects of the data subjects in order to create or use personal profiles, in particular by analysing or predicting aspects relating to their performance at work, economic situation, health, personal preferences or interests, reliability of behaviour and financial solvency and location”. Paragraph d adds that these assessments are mandatory when it comes to “(...) processing of large volumes of personal data”.

The link with AI is undeniable, and the application of these provisions to AI systems that perform profiling of people or that employ large volumes of data

The availability of data for training is indisputable, both in the public and private spheres. It is true that there are certain circumstances in which the scope of application of this law may not cover certain situations, as pointed out by civil society in the response to the consultation and as will be seen later.

As regards self-regulation, there are many examples. Particularly in the area of data, the rules on personal data protection can serve to exemplify how these mechanisms work (see for example the codes of conduct provided for in article 36 of Law No. 18,331).

The adoption of co-regulation schemes that normatively establish certain red lines and monitoring mechanisms seems a more convenient path. These definitions can be observed in the work of MANTELERO[57], who proposes considering the different areas of action of governments and the scope of regulation, comparing the proposals of the Council of Europe and the European Commission, and indicating that in addition to the co-regulatory approach, the proposals put forward by these organisations lean towards a risk-based approach rather than one based on principles.

As regards the possible imposition of special measures, this is also linked to the analysis of the impacts on the rights of individuals, with other measures for more effective supervision of the functioning of the systems. The creation of registers of algorithms, the request for a special prior authorization or even the obligation to carry out tests in controlled environments, can be useful instruments for certain types of systems and in the face of certain special types of risks.

Regarding the principle of transparency and explainability, the European Commission's High Level Expert Group on Artificial Intelligence (AI HLEG), in its “Ethical Guidelines for Trustworthy AI”[58]points out that explainability – a central element of transparency along with traceability and communication – is the

---

[57] MANTELERO, Alessandro. “Beyond Data – Human Rights, Ethical and Social Impact Assessment in AI” in “IT&LAW 36”. Available in: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 the technical processes of an AI system and the human decisions involved. In our law, explainability has express normative enshrining in two provisions of Law No. 18,331: articles 13 and 16.

Article 13 of the aforementioned law provides for the Right to Information, and in its literal G establishes that the obligation to provide information to data holders by those responsible and in charge covers, in the case of "(...) automated data processing regulated by article 16 of this law, the evaluation criteria, the processes applied and the technological solution or program used".

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

The affected party may challenge administrative acts or private decisions that imply an assessment of his or her behaviour, the sole basis of which is the processing of personal data that provides a definition of his or her characteristics or personality.

In this case, the affected party will have the right to obtain information from the person responsible for the database about both the assessment criteria and the program used in the treatment that served to adopt the decision expressed in the act."

Notwithstanding the above, it is necessary to effectively consider broader solutions for AI systems that do not process personal data, or in cases of recipients who must be aware of their interaction with such systems even when their own data is not used by them.

Regarding the use of AI systems in Public Administration, it is worth mentioning Law No. 18,381, of October 17, 2008, which aims to:

Promote the transparency of the administrative functions of all public bodies, whether state-owned or not, and guarantee the fundamental right of individuals to access public information (Article 1). Its regulatory decree No. 232/010, dated August 2, 2010, establishes in its Article 6 the principle of maximum publicity, so that the obligated subjects provide the information in the broadest possible way, and its Article 38 includes within the information that the obligated subjects by law must disseminate on their websites, "any other information that could be useful or relevant for the knowledge and evaluation of the functions and public policies that are the responsibility of the obligated subject."

In this way, the obligation to make transparent, but above all to explain, the decisions adopted by public entities when they use AI systems finds its foundation not in one but in two founding laws of the digital environment.

As regards possible guiding criteria for public policy in this area, these could be associated with compliance with principles and the provision of practical tools that allow for innovative development, control of adjustment to human rights standards, and supervisory mechanisms.

At this point, the authority to make recommendations on the matter has been granted by law to the National Human Rights Institution and Ombudsman through article 4 of Law No. 18,446 of 24 December 2008 and to the Secretariat for Human Rights in accordance with article 67 of Law No. 19,149 of 24 October 2013; and in matters of personal data, to the Personal Data Regulatory and Control Unit through article 34 of Law No. 18,331 of 11 August 2008.

We can say that most of the concerns received from the entities that participated in the consultation were focused on this thematic line. Thus, for example, CUTI states that although the current legal and institutional framework would be adequate for the management of potential risks derived from the use of AI - also taking into account the updates made to the personal data protection law - a specific committee or group would be necessary to evaluate the impact on the data.

human rights, and a cautious approach to risk classification, so as not to impact innovation and investment in AI.

The diagnosis issued by civil society institutions regarding the sufficiency or lack thereof of the regulations states that the provisions of the personal data protection law are not sufficient because they are directed, among other things, exclusively to the processing of personal data, and therefore provisions should be included that specify the concept of “significant human supervision”, enable the exercise of collective rights, the publication of impact assessments, the requirements for the explainability, traceability and auditability of algorithms, the guarantee of human and face-to-face interaction with the public administration, and the relationships between copyright, trade secrets and auditability of AI systems (DATYSOC proposals).

In the case of DATA, the importance of the right provided for in article 16 of the personal data protection law is highlighted, but it is clarified that it is necessary to apply these standards to public administration through amendments to Law No. 18,381. They also emphasize the discussion on high-risk systems and the establishment of basic guarantees, and the need to provide support for the work of the INDDHH.

In the case of the AEU, this line raises the question of whether general or sectoral regulations are necessary, and assesses the appropriateness of the risk approach, also taking into account the allocation and distribution of responsibilities for damages. All of this with a focus on the human being and contemplating the obligation for companies to explain where and how they use AI, and also considering the duty to prevent and ensure that discriminatory attitudes are not reflected and to avoid risks. It also proposes the establishment of impact assessments on human rights of AI developments and the strengthening of the role of informed consent and the principle of purpose provided for in Law No. 18,331.

The responses to the queries received from civil society suggest that it is necessary to further analyse the use of AI in the field of surveillance by security forces, which will be considered in another chapter.

Intellectual Property Line

Preliminary considerations

It is pointed out by the World Intellectual Property Organization (WIPO)[59]The concept of Intellectual Property refers to creations of the intellect, from works of art to inventions, computer programs, trademarks and other commercial signs. It is divided into two categories: industrial property (patents for inventions, 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 well as the impacts of Artificial Intelligence on it[61]. The National Artificial Intelligence Plan of the Argentine Republic[62]For example, it has indicated that intellectual property, together with the protection of personal data and consumer rights, are regulations in tension with respect to which a regulatory balance must be sought, due to their importance in the development and application of AI.

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

1) Understand 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-thedirection-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) Analyze whether the current situation allows for incentives, considering the economic and social benefits that may be sought.

It also raises a number of questions about how to respond to AI-generated inventions.

In the first point, WIPO proposes to look beyond the question of who should be the inventor and gives a list of alternatives: 1) recognize only inventions made by humans; 2) allow AI to be named as inventor or co-inventor; 3) require that a legal entity 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 creations generated by AI.

In any case, WIPO's proposal is to work from a multi-stakeholder perspective, which allows different opinions to be considered before making changes to the regulations.

In terms of AI and intellectual creations, following the same WIPO document, a distinction must be made between creations assisted by AI, those based on AI and those generated by AI. MANTEGNA[64]At this point, it proposes different alternatives, in order to regulate creations assisted by AI and those generated by AI, which are in line with the alternatives proposed by WIPO.

Taking into account what was indicated by the aforementioned author, the scope of this line is related to authorship in copyright, industrial property and trade secrets, the link of the latter with measures regarding transparency and explainability - which are part of the principles considered by the law for AI -, the ownership of the databases used for the generation of creations, and the measures to be adopted from the regulatory point of view in the development and implementation stages of generative AI systems.

---

[64] MANTEGNA, Micaela. “ARTEficial: Creativity, Artificial Intelligence and Copyright”. Ed. CDYT, 2022. Pages 299 and following.

For its part, and due to its impact, it is necessary to evaluate the issue of intellectual property in the developments applied by the State when using AI to provide its services and fulfill its duties.

Selection of international backgrounds

A bill to amend intellectual property regulations in France was recently introduced and is currently being considered by its Parliament, linked to the impact of AI.[65]. In this project, some significant provisions are raised in a few articles:

- Article 1 establishes that the integration and subsequent exploitation by an AI system of works protected by copyright is subject to the general provisions regarding the authorization of 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 rights holders of the original works, and adds that their management may be carried out by authors' societies or other collective management organizations;

- Article 3 requires the use of a specific mention in the work created by an AI system stating that said 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 for cases where the origin of the works that served as the basis for the new creation of the AI system cannot be determined, for the benefit of collective management organizations, leaving their determination to the regulations.

In the case of UK legislation, section 9(3) of the Copyright, Designs and Patents Act 1988[66]In terms of authorship, it establishes that when the literary, dramatic, musical or artistic work was generated by

---

[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: 03/27/2024.

computer - defined as one in which there is no human author - the author must be understood as the person through whom the necessary arrangements were made for the realization of said work.

This position is not shared by all jurisdictions, and the difficulty at present is that there is a wealth of proposals on the matter, but the issue has mostly been the subject of different pronouncements by administrative and judicial bodies with different responses depending on the case. The new AI regulation of the European Union, for example, does not address this issue – although it does contain some provisions on data mining.

The aforementioned Resolution of the UN General Assembly A/RES/78/265[67], focuses on Intellectual Property by establishing: “Encouraging, where appropriate and pertinent, the application of adequate safeguards in order to respect intellectual property rights, including copyrighted content, while promoting innovation.”

In light of the above, it seems reasonable in this regard to rely on the opinions of various international and regional organizations regarding the need to explore alternatives from a multi-sectoral and pro-innovation perspective.

Diagnosis on AI and Intellectual Property

As a first point, it should be mentioned that in our country there are indeed regulations that govern the registration of computer programs, data compilations or other materials that constitute intellectual creations, expressions of ideas, information and algorithms formulated in original sequences ordered to be used by an information processing device or automatic control, with the current regulations pronouncing the protection provided through copyright.

On the other hand, the current regulations allow the registration of these rights to be carried out by a natural person or a legal person, including the State. The regulation also provides for the situation of 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.

The provisions of the Berne Convention make the publisher, or the entrepreneur as the case may be, the owner of the copyright, as long as the latter does not reveal his identity. But even in that case, it is not a question of the originality or the presumed authorship by a person of that work, but of the lack of knowledge of the details of his identity.

As Alexander CUNTZ and others point out,[68], it is not only a question of determining who created the work, but how creations generated entirely by AI change the nature of the innovation process and how that change affects the balance of the need for resources and incentives in the innovation ecosystem.

However, even though it may be prudent to ask whether it is possible to attribute ownership of the rights to the AI system – through a kind of electronic personality – to a particular natural or legal person – developer, user or others – to a group of people, or to understand that this should be in the public domain, the conditions do not seem to be in place to give an answer at this time.

The use of training data in AI models is another point to be clarified, in order to determine whether current regulations – both for the potential use of data protected by intellectual property rights and for the use of personal information protected by personal data protection regulations – are sufficient to meet the needs of these systems, or whether special exceptions are required – as can be found in Brazil's AI bill.[69]-.

Furthermore, it is important to determine how the requirements of transparency and explainability operate with intellectual property rights.

---

[68] CUNTZ, Alexander et al. “Artificial Intelligence and Intellectual Property: An Economic Perspective”. Edited by WIPO in the framework of the Working Papers in Economic Research. 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 in particular article 42. Last accessed: 27/03/2024.

As regards trade secrets, there are different rules linked to the subject.[70]-as Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)-.

In terms of personal data, the scope of the information that companies and organizations must disclose in certain types of automated processing of personal data is contemplated in articles 13 and 16 of Law No. 18,331.

Finally, it is relevant to determine whether the rules on intellectual property in the use of applications by the State reflected indirectly in the provisions on Public Software should be applied in the field of AI systems.

In the context of the discussion on the scope of this line, the DNPI raised some aspects that should be mentioned. Thus, it was pointed out that the intellectual property system implies an incentive mechanism to capture value, allowing creators to negotiate and avoid the undue use of their creations. It is indicated in particular that it is not possible, in this instance, to transfer this basis to AI creations.

The Directorate also maintains that, in our country, in accordance with continental European tradition, the copyright is seen as an extension of the rights of personality, establishing inalienable and non-waivable moral rights in favor of the author; in turn, with respect to originality, this is understood as an expression of the author's personality. In the case of patents, inalienable rights refer to recognition as an inventor, in accordance with the provisions of Article 2 of Law No. 17,164 of September 2, 1999.

Thus, and in accordance with current regulations, in order to grant exclusive rights over the invention to the inventor, he must provide a clear, detailed and complete description.

---

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

completeness of the invention; with the intervention of algorithms or other AI mechanisms, the issue is in the possibility of effectively providing a complete description of the way in which said algorithms arrive at one result or another, or generating a “black box” effect.

Considerations regarding intellectual property were also raised in the responses to the consultation carried out by DATYSOC, which mentioned the omission of the current legislation on the use of works for the purposes of computational analysis (including the restriction of the condition that the uses cited do not compete with the normal exploitation of the works and do not unjustifiably harm the interests of the authors, for which they also propose a wording), in addition to the need to regulate the relationships between copyright, trade secrets and auditability of systems (which in the specific aspect of intellectual property would imply exceptions enabling the entry, copying and analysis of systems to audit them at the request of a Judge or when the law so provides), and to establish prohibitions linked to competitive uses, or those that harm the author or owner of the rights to the works in an unjustified manner.

In the case of DATA, it is aligned with the need to provide greater support in the decision-making process for the acquisition of software or AI-based solutions by the Public Administration, pointing out the possibility of making adaptations to Law No. 19,179, of December 27, 2014, and its regulatory decree No. 44/015, of January 30, 2015. This, in addition to considering the possibility of creating an intervention mechanism so that Agesic can determine the risk and advise public entities on carrying out impact assessments prior to the acquisition of AI-based solutions for some sectors.

Infrastructure and Cybersecurity Line

Preliminary considerations

The development of AI depends on several factors. One of them is adequate infrastructure, in which the State plays a central role.

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

The OECD published its 350th report in February 2023[72] of the digital economy series, putting forward recommendations for building computational capacities for Artificial Intelligence, recognizing in this line of action a central element for the development and evolution of this technology. This document highlights the need for countries that develop AI plans to carry out an adequate analysis of domestic computational capacities to achieve the designed objectives.

Based on the analysis carried out by the OECD, it is appropriate at this point to: 1) evaluate the review of computational capacities especially for AI in public and private sector actors, considering the use of cloud services in the country or abroad; 2) consider the number of existing data centers, define data standards, analyze processing capacities and hardware needs in the country, among others; 3) determine the demand

---

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

[72] https://www.oecd-ilibrary.org/science-and-technology/a-blueprint-for-building-national-compute-capacity-for-artificialintelligence_876367e3-en . Last accessed: 03/28/2024.

AI processing potential to anticipate needs and plan accordingly; 4) distinguish AI processing needs from others; 5) provide capabilities and training for workers; 6) map and analyze the necessary supply chains to build contingency and resilience plans.

The alternatives handled by the OECD are undoubtedly worthy of consideration in order to ensure the effectiveness of the strategy designed. However, the scope of this document is related to possible normative recommendations, and in this sense, it is appropriate to consider the existence and sufficiency or not of standards associated with:

1) Infrastructure for data management and exchange

2) information storage

3) cybersecurity

4) telecommunications networks

Selection of international backgrounds

There are no regulatory precedents that expressly contemplate this circumstance at an international level, beyond the mention of specific and isolated aspects in existing regulations and draft standards, and it is not present in the different AI strategies surveyed. To this extent, what is expressed in OECD report No. 350 is confirmed, which states that many countries have developed national AI strategies without having fully analyzed whether they have sufficient computing infrastructure and software for AI to achieve their objectives.

The initiative of**Digital Public Infrastructure**promoted by UNDP[73], mentioned above, is linked according to this entity to a combination of open standards built with a public interest purpose, enabling governance and a community of competitive and innovative market actors to foster innovation, especially 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 highlighted in different documents and can help determine the direction that efforts should take for an AI supported by a secure, sovereign and pro-innovation infrastructure.

Diagnosis on Infrastructure and Cybersecurity for AI

In our country, there is a strong institutional framework in terms of telecommunications, cybersecurity, interoperability and data policies. The distribution of powers between the different public entities involved is seen as adequate, although greater coordination between them is necessary.

On the other hand, no current analyses have been found related to purchases in terms of physical infrastructure, nor regulations that specifically regulate the requirements for the acquisition of AI systems by public entities, nor AI adoption plans from the perspective of this document, nor objective information associated with the use of physical infrastructures for these activities by public or private entities.[74].

And here, the planned purchasing processes and the determination of the needs of the entities are seen as a central point that must be considered. In this regard, two regulations could be of importance at this point: a) Article 74 of Law No. 19,149, of October 24, 2013, which assigns Agesic the task of mandatorily reporting on the development and IT acquisition plans of the Central Administration departments, and proposing to the Executive Branch general technical requirements to be required in the acquisition of IT goods and services; and b) Decree No. 431/022, of December 27, 2022, which creates the Governance Committee for Processes and Cross-Cutting Solutions - made up of several public entities and including Agesic - in order to exercise the functional and technological leadership of the information systems.

---

[74] This is without prejudice to sectoral information that can help define policies such as the “Uruguay Telecommunications Market Report” published periodically by URSEC, available at:https://www.gub.uy/unidadreguladora-servicios-comunicaciones/datos-y-estadisticas/estadisticas/informes-mercado-del-sector-telecomunicaciones . Last accessed: 03/29/2024.

cross-cutting information and technological platforms for shared use, linked to the internal management of the sections of the Central Administration.

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

With regard to the storage of information, Decree No. 92/014 of 7 April 2014 has been applied by public entities in general – not only those belonging to the Central Administration, either by express reference to its provisions or by the adoption of similar regulations in their respective areas – as an argument to avoid contracting cloud data processing services. Agesic has sought to provide greater clarity regarding the scope of the decree.[75], but the possibility of an update should be considered, in line with the criteria defined by the Agency[76].

As regards the infrastructure enabling the exchange of information, Agesic has at its disposal the Interoperability Platform, created by article 17 of decree No. 178/013, of June 11, 2013, in order to guarantee the exchange of information in electronic format, in a safe and reliable manner. Although this platform is aimed at public entities, it could also be used by private entities, in which case the conditions established by Agesic and by the entities that display their services on it for the consumption of information must be met.

Finally, in terms of cybersecurity, the development of the National Strategy is in process, so it must be in accordance with what is defined therein. Yes, it can

---

[75] “Guide to the interpretation of Decree 92/014 on Cybersecurity” available athttps://www.gub.uy/agencia-gobiernoelectronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-interpretacion-decreto-92014- ciberseguridad/guia-interpretacion and document “Use of the Cloud in Public Administration” available at https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-knowledge/comunicacion/publicaciones/uso-nubeadministracion-publica/uso-nube-administracion-publica . Last accessed: 03/30/2024.

[76] “General Principles of Public Cloud in the State”. Available at:https://www.gub.uy/agencia-gobierno-electronicosociedad-informacion-knowledge/comunicacion/publicaciones/principios-generales-nube-publicaestado#:~:text=Con%20el%20fin%20de%20guiar%20a%20las%20entidades,este%20documento%20principios%20generales%20to%20have%20on%20account . Last accessed: 03/30/2024.

It should be noted that, in addition to extensive and pre-existing regulation on the matter, there was a recent update by articles 78 and following of Law No. 20,212.

In the context of the discussions regarding the preparation of the report, DINATEL submitted proposals related to the scope and diagnosis carried out in this thematic line.

Thus, it was proposed to consider the status of current regulations in the field of infrastructure for data management and exchange, information storage, cybersecurity obligations, telecommunications networks (robustness and quality of service), identification of critical infrastructure, international agreements on data exchange and those associated with civil liabilities, in addition to the topic of cloud infrastructure and the update of current cloud data regulations.

DINATEL pointed out that the development of AI at this point must incorporate infrastructure needs outside the telecommunications sector, a vision of social impact and non-restrictive regulation or laws promoting the installation in the country and use of public and private data centers for public purposes. This in addition to other contributions that are attached in the annex of this document.

Line of work and training in AI

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 address emerging challenges.

This report, in this specific line, sought to identify measures to promote the strengthening of people's skills in the field of AI, aimed at preventing and mitigating negative impacts on employment and the labor market and enhancing the use of AI for the benefit of society.

In the report prepared by the OECD entitled “OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market”[77]It is indicated that the impact of AI will generate changes in the needs for skills, which are currently lacking, so public policies will play an important role in encouraging training by employers, as part of formal education.

This is shared by UNESCO in its Recommendation on the Ethics of Artificial Intelligence, which, within scope 10, establishes the need to expand basic and interdisciplinary skills at all educational levels associated with the ethical use of AI, support collaboration agreements with educational institutions, industry, civil society, and workers' organizations to reduce gaps and generate training strategies in medium-sized companies, among others. It also proposes working with companies to collaborate on equitable transitions for at-risk employees through training and job retraining programs, among others. Other measures linked to research, market competitiveness and consumer protection, the provision of financing when necessary, etc. are included.

---

[77] See in particular Chapter 5 on skills, available at:https://www.oecd-ilibrary.org/sites/638df49aen/index.html?itemId=/content/component/638df49a-en . Last accessed: 03/31/2024.

Selection of international backgrounds

The Spanish government, through Decree-Law No. 2/2023, of March 8, 2023, established some urgent measures to promote AI in the autonomous community of Extremadura[78]. In its first article, it establishes as its main and general objective, to increase the technical capacity in AI through the literacy of the population, including the training of the active population and public employees. To this end, it proposes promoting the development of entrepreneurial, creative, social and cultural capacities, the promotion of support measures for companies that carry out training and capacity building plans in the field, and the inclusion of this training for unemployed people and public officials.

The Executive Order for the Safe and Trusted Development of AI of the United States government, within Section 10 (Advancing the use of AI in the Federal Government) proposes at the highest level of federal government agencies, the implementation of training and familiarization programs in AI for employees, managers and leaders, among others. These programs should empower employees and others to develop and maintain operational knowledge in emerging AI technologies. It also proposes that agencies provide professional development opportunities, scholarships, and funds for their staff.

Diagnosis on work and training for AI

There are various provisions at the national level that provide for the promotion of training among workers. However, the regulations analysed do not initially show a particular emphasis on aspects related to AI and the way of managing its impacts, beyond the fact that training for workers in the digital field is present in programs such as those carried out by the National Institute of Employment and Vocational Training (INEFOP), or by the National School of Public Administration (ENAP) in the case of public sector workers.

---

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

Based on the above, it is estimated that the existing institutional framework would allow for the implementation of policies and programs related to this topic, and for the exploration of alternatives for cooperation between public and private entities.

Making the problem visible, establishing coordinated actions, defining a specific policy and implementing sustained cooperation between the different actors in the ecosystem must be considered in order to carry out a successful strategy in this area.

Civil liability and consumer rights line

Preliminary considerations

AI raises questions that are difficult to resolve for many legal operators who, in countries like ours, try to interpret regulations that - although they clearly provide the necessary legal security - were sanctioned in a reality very different from the current one.

The line raised at this point refers to two aspects that are well regulated by law, such as civil liability and consumer relations.

OF CORES[79], when analyzing the preventive function of civil liability in our law, indicates that the concept itself is considered to be "(...) highly polysemous, but that in a broad sense, it can be defined as the consequence that arises from the non-compliance with a rule, thus allowing for not only civil liability but also criminal, administrative, and even political or moral liability."

JOSE DOS SANTOS[80]states that “(...) civil liability has the function of restoring the balance, compromised by the occurrence of moral or material damages caused by the causal agent” and highlights that in Brazilian law, there is subjective civil liability – which requires malicious or culpable conduct or an omission by the author of such conduct – and objective liability – in which proof of the causal link between the conduct and the damage is sufficient, without considering the intention or fault of the person who caused it.

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

---

[79] DE CORES, Carlos. “The so-called preventive function of civil liability. A critique of its dogmatic position”. Available in:https://eva.fder.udelar.edu.uy/mod/resource/view.php?id=49243&redirect=1 . Last accessed: 03/30/2024.

[80] JOSÉ DOS SANTOS, Sonia “Artificial Intelligence and Civil Liability” in “Artificial Intelligence and Law” 1st. Ed. Hammurabi. 2020. Page 179 et seq.

Within the concept of civil liability, the most common distinction is between contractual liability –derived from the breach of a contract between two or more parties- or non-contractual liability –derived from damage caused to someone, without such contractual link existing-. The civil liability regime is regulated in Uruguay primarily in our Civil Code.

In the case of consumer relations, these are defined in article 4 of Law No. 17,250, of August 11, 2000, as the link between the supplier who, for a fee, provides a product or renders a service and the person who acquires or uses it as the final recipient. From a subjective point of view, there are the figures of supplier and consumer.

ARMENDIA[81]points out that in the use of AI and the possible damages that may be caused by the use of these systems, there are two extremes to consider: the insecurity of the people who are harmed by the product or service that contains AI regarding how to proceed to be compensated, and the insecurity of the designers, developers, producers, financiers, and other members of the chain that brought that product or service to the market regarding their role in producing the harmful event.

The author poses three challenges: 1) the complexity of the systems and the diversity of factors that can cause the error that in turn caused the damage; 2) the multiplicity and diversity of actors in the chain, making traceability difficult; 3) the mechanism to continue promoting investment, research and development in AI and in turn ensure that those who suffer damage will be able to access fair compensation.

It is precisely the response to these three challenges that will be considered from a strictly normative perspective. The impacts that AI may have on consumer relations are outside the scope, since what will be referred to in this line is the problem associated with the responsibility of suppliers and the reparation of damages to consumers.

---

[81] ARAMENDIA, Mercedes. “Artificial Intelligence and Responsibility?” in “Studies on the Legal Challenges of Digitalization” Volume III. Coord. Mercedes Aramendía and Agustina Pérez Comenale. Ed. UM. Year 2023. Pages 557 et seq.

Selection of international backgrounds

At this point it is relevant to consider the proposal for a Directive on AI Responsibility of the European Union[82], which complements the recently approved Regulation.

CASALS points out[83]“The current Proposal for a Directive, on the other hand, refers only to liability for intent or negligence for damage caused by AI systems, which remains subject to national substantive rules. For this reason, it does not conflict with the application of national rules or with those arising from the Directive on liability for damage caused by defective products and, as noted, its objective scope is much broader.”

At this point, the European Commission[84]The EU Commission has noted that: “The Directive simplifies the legal process for victims in proving that a person’s fault has caused the damage by introducing two key features: first, in circumstances where relevant fault has been proven and a causal link with the AI’s performance appears reasonably likely, the so-called ‘presumption of causation’ will address the difficulties experienced by victims in having to explain in detail how the damage was caused by a particular fault or omission, which can be particularly difficult when trying to understand and deal with complex AI systems. Second, victims will be given more tools to seek legal redress thanks to the introduction of a right of access to evidence submitted by companies and suppliers, in cases where high-risk AI is involved.”[85]

---

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

[83] CASALS, Miguel Martín. “The European Union’s proposals to regulate civil liability for damages caused by artificial intelligence systems”. Available in:https://indret.com/las-propuestas-de-la-union-europea-para-regular-laresponsibilidad-civil-por-los-danos-causados-por-sistemas-de-inteligencia-artificial/ . Last accessed: 03/30/2024.

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

[85] A more extensive analysis can be seen in La Ley Digital, article by Gonzalo ITURMENDI MORALES “Civil liability for the use of artificial intelligence systems” available at https://laleydigital.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAmNDCwsjI7Wy1KLizPw8WyMDIwNDQyMDkEBmWqVLfnJIZUGqbVpiTnEqANKvjtI1AAAAWKE . Last accessed: 03/30/2024.

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

There are no relevant regulatory precedents on this issue, beyond the provisions of the draft European Union directive. This motivates us to reflect on the need for a specific and multi-actor analysis of Uruguayan legislation, given the sensitivity of the civil liability structure to legal certainty.

Diagnosis of civil liability and consumer rights

The first point of the diagnosis is that the rules do not establish a specific regulation for the problems arising from the damages that AI systems can potentially cause. Unless the liability regime is clearly established in the terms of a contract, the general regulation on civil liability that could be applied by analogy in these cases - in which there is great complexity in determining the members of the chain that leads to the production of an AI product or service - is article 1330 of the Civil Code, which regulates a type of collective liability associated with something that falls from a building. This analysis in general terms, and its

---

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

application in analogue way was duly prepared by BORDOLI[87], although not specifically related to the topic at hand but to the assignment of responsibility in the event that there is an individual group made up of several people but where it is not possible to specifically identify who caused the damage.

This regime appears to be insufficient to properly assign liability to those who caused the damaging event and to effectively repair the damage to people.

In the case of consumer relations, the aforementioned article 34 of Law No. 17,250 of August 11, 2000, will apply, which provides: “If the defect or risk of the thing or the provision of the service results in damage to the consumer, the provider will be liable in accordance with the regime established in the Civil Code.

The trader or distributor will only be liable when the importer and manufacturer cannot be identified. They will also be liable if the damage occurs as a result of inadequate storage of the product or when its original condition is altered.

Another aspect to consider concerns the damage caused when the product or service is offered by the State, and in such a situation the provisions of articles 24 and 25 of the Constitution apply, as indicated.

---

[87] BORDOLI, Carlos Rubens. “Collective Extracontractual Liability for Damage Caused by an Undetermined Member of a Group” available in the FDER Journal (30). Year 2014. Pages 65 and following. Available in electronic format at: https://revista.fder.edu.uy/index.php/rfd/article/view/87 . Last accessed: 03/30/2024.

Line of measures to promote AI

Preliminary considerations

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

Why propose measures to promote AI? The answer lies in the proven benefits that this technology can have for society. While there is an emphasis on warning about the potential risks that it poses for people, it is also relevant to consider its multiple advantages.

The interim report of the UN Advisory Body on Artificial Intelligence of December 2023 can be considered in this regard.[88], which establishes a set of preliminary recommendations based on 5 principles: 1) inclusive governance, by and for the benefit of all; 2) governance for the public interest; 3) governance built in conjunction with data governance and the promotion of common goods; 4) universal governance, networked and rooted in multi-stakeholder collaboration; 5) governance anchored in the United Nations Charter, international human rights law and other agreed international commitments such as the Sustainable Development Goals. This document, regarding the promotion of AI for Humanity, points out, among others, the need for access and benefits to go hand in hand, through national investment in talent, data and computing resources. To this end, international cooperation and assistance in the public and private sectors are seen as relevant.

The relevance and scope of possible AI promotion measures must take into account: 1) the determination of the objectives towards which the effective promotion of Artificial Intelligence is directed, focusing on developments that contribute to the construction of a more just and equitable society; 2) the specific instruments that could be used to provide benefits that contribute to the development of the systems that are seen as recipients of these.

---

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

Selection of international backgrounds

Among the most relevant points of the Executive Order on the Safe and Reliable Development of Artificial Intelligence to be applied by the United States government agencies[89]the promotion of innovation and competition is found, through:

a) Catalyze AI research in the United States through a National AI Research Resource pilot.

b) Promote a fair, open and competitive ecosystem through technical assistance and resources for small developers.

c) Use existing authorities to expand the skills of highly specialized 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 between entities within the government.

For its part, the proposal for the European Union's "AI Law"[90]The document expressly points out the link between data governance, open data and the promotion of AI-driven innovation. Measures to support innovation include the development of controlled test spaces for AI, the enabling of data processing for certain purposes, and some measures for suppliers and small-scale users ranging from priority access to controlled test spaces, awareness-raising activities, specific communication channels and, eventually, differential rates for certain services.

---

[89] The content of the Executive Order can be consulted at:https://www.whitehouse.gov/briefing-room/presidentialactions/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]The plan places emphasis on promoting research and development in order to stimulate innovation in productive sectors and in public power. The measures envisaged also include the creation of regulatory sandboxes and public AI databases.

There are other provisions at the international level that share the criteria regarding promotion reflected in this document, which include the concept of innovation development, thus highlighting the role of controlled testing environments in this regard.

Preliminary diagnosis on AI promotion measures

There are currently some provisions that specifically refer to the promotion of innovation in the field of AI. At the time of writing this document, the regulations for Article 75 of Law No. 20,212 are being drafted, so the considerations made in the framework of this analysis will be taken into account.

On the other hand, there are other types of measures that could be efficient in promoting innovation and its development, such as tax exemptions, analysis and promotion of seals that certify the performance of audits and evaluations that in turn allow access to certain benefits, among others, all of these elements that require a particular 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 lines highlighted based on the contributions received

The use of AI systems for surveillance purposes

Among the concerns and recommendations raised by civil society when responding to the consultation document made available by this Agency, questions are raised regarding the use of AI systems for surveillance purposes by security forces.

Law No. 19,696, of October 29, 2018, regulated by Decree No. 157/022, of May 23, 2022, establishes and regulates the National State Intelligence System (SNIE), imposing on the bodies that comprise it compliance with a set of principles with the objective of respecting the Constitution, and the principles of the democratic republican regime of government and respect for human rights.

In this context, Article 20 of the Law provides that the search for information through special procedures that may affect the freedom and privacy of citizens must be authorized by the Judiciary. Regarding controls, it is worth highlighting Article 25, which provides for the creation within the framework of the General Assembly of a bicameral parliamentary commission with the task of controlling and supervising the performance of the system.

Decree No. 157/022 approves the National Intelligence Policy, specifying a set of actions and measures, but without prejudice to generic references to compliance with human rights, no provision is made regarding the application of AI in surveillance activities of people.

Civil society, in response to the consultation, puts forward suggestions such as imposing a moratorium on the acquisition of surveillance software until there is a legal basis that adequately regulates the police surveillance ecosystem, or the possibility of requiring algorithmic auditability and explainability, traceability, access control protocols and a description of detailed responsibilities for those who use these surveillance systems.

Civil society is also proposing the establishment of red lines regarding which uses are strictly prohibited for the police and which require a court order, the prohibition of the use of biometric surveillance in real time and without a court order in public spaces and a specific regulation of the admissibility, assessment and processing of biometric matches as investigation methods and as digital evidence, among others.

Finally, civil society recommendations include adequate training for police officers, judges and prosecutors - through mandatory certification - and urgent regulation of the use of AI for surveillance purposes by the Ministry of the Interior.

This Agency shares the concern for the proper use of AI systems in the framework of the activities of the security forces, but also wishes to emphasize the need to establish a multi-sector dialogue in order to contemplate an appropriate balance between the needs associated with internal security and the protection of the fundamental rights of individuals.

International insertion and cooperation

Another aspect that was not part of the initial lines, but which is of enormous relevance, is the international insertion of the country. As with other issues on the agenda of our countries, AI poses global challenges that motivate us to seek global solutions.

Furthermore, since the development of AI systems applied by the region is “imported” from other parts of the world, we must make an additional effort to generate regional cooperation mechanisms that take into account our own needs.

As part of the Common Agenda[92]Presented by the UN Secretary General in 2021, the organization launched the “Global Digital” initiative last year

---

[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 in the consultation process and expected to be agreed upon at the Future Summit to be held this year– which, within its objective 5, includes improving the international governance of emerging technologies, including AI, for the benefit of humanity. The document proposes agile, multidisciplinary and multi-stakeholder international governance, and some specific 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 the promotion of North-South and South-South cooperation in the development of data sets, computational capacity, local solutions, use cases and business ecosystems in developing countries.

At the international level, the Framework Convention on AI promoted by the Council of Europe has already been mentioned, which is the first international treaty on the subject, with a vision of principles and also of risks. As our country participated as an observer in the drafting process, it has the possibility of becoming a member of the Convention, which should be assessed with the advice of the Ministry of Foreign Affairs. It is already announced that this Agency shares the provisions of the Convention and supports the accession.

Finally, at the regional level, the efforts of UNESCO and CAF to incorporate the regional voice in the discussion on the future of AI should be especially highlighted. The aforementioned Santiago Declaration emerged from the First Ministerial and High-Level Summit on the Ethics of AI in Latin America and the Caribbean, organized by them with the support of the Chilean government.[94], which approved the establishment of a Working Group for the constitution of an Intergovernmental Council on AI for Latin America and the Caribbean, within the framework of the UNESCO Recommendation on the Ethics of AI, with the purpose of strengthening regional capacities in the matter.

---

[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 collected from other public entities in the first stage of discussion

In the context of the process of preparing this report, several meetings were held with the entities mentioned in this document, from which the following contributions can be summarized:

Institutionality and governance line

- There is a need for a cross-cutting approach, although it is important to have a leading organisation in this area.
- Having an advisory committee, with the role of advisor on specific topics and with the integration of different actors according to the topics to be addressed (for example, the private sector, civil society organizations, telecommunications companies, companies linked to the development of AI systems, among others). It is proposed that the Committee integrate ad hoc groups, according to the specific topic to be addressed or otherwise convene experts in the sector or area to be considered.
- Involve consumer protection, user protection, and the consideration of the person as a digital citizen (generator and user of AI) as aspects to be integrated into the analysis.
- Integrate telecommunications data and consider this point as a critical service.
- Include the Ministry of National Defense (MDN) in the discussions for defense and the use of AI for this purpose, as well as the Ministry of the Interior (MI) for public security aspects.
- Apply the mechanism of public consultations, in order to broaden the number of actors involved, obtaining and/or integrating other visions.
- Include and work on strengthening small and medium-sized businesses.

Human Rights Line

- Consider generating policies for AI systems.
- Regarding the vulnerable population, pay special attention to girls, boys, adolescents and older adults.

- Specification that the final decision is made by a human, not by an algorithm, and the possibility of incorporating audits to analyze the impact of the application of AI, and that these be institutionalized.

- Analyze the stage of the process cycle at which a potential audit should occur.
- Determine an organization and/or institution that independently controls certain cases of risk and/or high impact.
- Analyze the feasibility and/or relevance of providing the INDDHH with greater powers or establishing some guarantee mechanism in the area of human rights.
- Incorporate a line of work that integrates AI to facilitate access to State services.
- Identifying the importance of the work sector, analyzing how companies could play a proactive role, proposing alternatives to the replacement of human work by AI, for example, through training to address other tasks and the use of new technologies.
- Analyze the approach to environmental impacts.
- Consider the risk approach.

Line of work and training for AI

- Emphasize the impact on employment specifically and the world of work generally.
- Consider all current labor regulations (particularly regulations on combating discrimination in the workplace).

Intellectual Property Line

- Generate further discussion on the topic of authorship and incorporate the topic of plagiarism.
- Analyze the development of exceptions for the use of certain data for training purposes, and create safeguards when it comes to copyright, defining their scope and purpose.

- Discuss a reform to the Copyright Law No. 9739 in order to consider the impact of AI on the matter.
- In the area of patents involving AI, analyze whether or not it is necessary to indicate in the patent application how AI intervenes in the inventive process.
- Encourage actions for the development of intellectual property.

Civil Liability and Consumer Rights Line

- Determine the scope of current regulations in order to consider potential damages caused by the use of AI systems and further analyze them prior to making regulatory proposals.

- Analyze the possibility of raising awareness among citizens, so that people can identify when they are in a consumer relationship linked to AI, as well as what mechanisms exist to make claims and/or complaints.

Infrastructure and cybersecurity line

- Clearly define the concept of AI applied to infrastructure and cybersecurity.
- Consider issues such as the use of data repositories at an international level, 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 services.

- Consider AI applied to the standardization of telecommunications infrastructure.
- Analyze the possibility of computing capacity centers by region.
- Evaluate environmental aspects and use of natural resources.
- Evaluate the country's capabilities in each of the following points:
    - Standards for data management and exchange
    - Storage capacity, computing capacity
    - Cybersecurity

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

Line Promotion Measures

- Analyze and define strategic objectives at the national level for the use of AI.
- To identify existing promotional measures in this area and in different aspects related to AI.
- Analyze the possibility of having infrastructure at a national level where tests can be carried out (sandboxes and others).
- Analyze the possibility of exemptions and tax incentives associated with promoting the development and use of AI aimed at the country's strategic objectives in different areas.

Recommendations

Previous concepts

In the previous chapters, an overview was presented of the process and framework applied in the preparation of the report committed to this Agency in accordance with the aforementioned article 74 of Law No. 20,212.

The recommendations presented are the result of the institutional analysis carried out based on the diagnosis that was previously developed on the challenges identified for each thematic line, based on:

1. the guidelines resulting from Article 74 of Law No. 20,212; the
2. national legal framework, including applicable international law standards and legal obligations resulting from respecting, protecting, guaranteeing and promoting human rights in the digital environment and beyond;
3. the principles and recommendations emerging from the international background of soft law;
4. the review of regulatory background generated by other countries;
5. the contributions received from public entities, civil society and the private sector, in the work process implemented for this report, and in the construction of the Strategies led by this Agency;

6. the guidelines established in the country's digital policy emerging 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-knowledge/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-informaciontrabajo/comunicacion/publicaciones/estrategia-inteligencia-artificial. Last accessed: 20/06/2024.

Given the transversality of AI systems and their current and potential positive and negative impacts on all sectors of society, these recommendations should not be interpreted as an exhaustive list.

These reflect the results of the institutional analysis achieved at the date of submission of this report on general and non-sectoral aspects, and in a context marked by the rapid development of technologies - which determines the need for a sustained analysis of the potential and risks involved -, the existence of ongoing processes at regional and international level, the existence of an ongoing process of review of the AI Strategy and the construction of the National Data and Cybersecurity Strategies.

All of this makes it foreseeable that in the future these elements may have an impact on the public challenges referred to in these recommendations, which need to be addressed during the work process that the Legislative Branch may eventually initiate.

Furthermore, the analyses carried out are based on the knowledge and experience of this Agency in matters of transformation and digital policy and on the contributions made by other public entities in specific areas, but in several of the topics analysed it is necessary to generate an in-depth debate with these and other actors, before adopting any type of measure.

General recommendations.

The growing number of international instruments that have been developed in recent years reflect a scenario in which there is increasing consensus on the need to regulate activities within the life cycle of AI systems, in order to ensure that they are fully consistent with human rights, democracy and the rule of law, and at the same time, enhance the opportunities that these technologies offer for humanity and ensure equitable access between and within countries.

As outlined in this report, these instruments include, inter alia: the OECD Recommendation on AI and its principles adopted in 2019 that were updated in 2024; the Recommendation on the Ethics of Artificial Intelligence adopted in 2021 by UNESCO; the AI principles and the “International Code of Conduct for Organizations Developing Advanced AI Systems” developed by the G7 in 2023 within the framework of the Hiroshima AI Process; the European Union AI Regulation, adopted in March 2024; the Framework Convention on Artificial Intelligence adopted by the Council of Europe, adopted in May 2024; and the recent Resolution “Safe and Trustworthy Artificial Intelligence Systems for Sustainable Development”, adopted by the United Nations General Assembly in March 2024.

At the inter-American level, the following can be cited as examples, among others: the Santiago Declaration to promote ethical artificial intelligence in Latin America and the emerging Caribbean in 2023 of the Ministerial and High-Level Summit of Latin America and the Caribbean, and the Regional Charter on Artificial Intelligence in Administration, adopted within the framework of the Latin American Center for Administration for Development (CLAD) in 2023..Uruguay has been attentive to these efforts, and in several cases has participated in their creation or has even adhered to them.

From this background, there arises a clear call for States to respect and act proactively to protect and promote human rights throughout the entire AI life cycle, adopting appropriate and effective regulatory frameworks, under a balanced approach that integrates the risks and opportunities that AI offers and promotes responsible and safe innovation.

It is recognized in the background presented that AI governance is an evolving field, which requires progress in the construction of common frameworks, and at the same time considering the scope of each State to establish regulatory approaches and instruments at the national level based on national contexts and priorities, in a manner consistent with its regulatory framework and the obligations emerging from applicable international law.

Based on all of the above, this Agency considers it pertinent, first of all, to support the importance of our country maintaining a proactive approach to the regulation of AI systems through different public policy instruments:

1. Updating, under a multi-stakeholder approach, its Artificial Intelligence Strategy, to respond to the new context generated particularly - and not only - by the expansion of the most advanced models such as Generative AI; and with the aim of expanding the scope to the private sector, as provided for by article 74 of Law 20.212.
   This process is currently underway and is expected to be completed in the second half of this year.
2. Reviewing, where appropriate, the current regulations, in order to:
   (i) Strengthen the institutional design for AI governance in the country, including mechanisms for multi-stakeholder participation and collaboration;
   (ii) Ensure that activities throughout the life cycle of AI systems are fully consistent with human rights, democracy and the rule of law, through frameworks that allow for the identification, prevention, assessment and mitigation of risks and negative impacts on such rights.
   iii) Promote the equitable use of the opportunities and benefits of AI for the benefit of society and the sustainable development of the country in its different dimensions (social, cultural, environmental and economic) by promoting safe research and innovation based on the public interest;
   iv) Ensure the ethical, human rights-respecting, responsible and secure 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, guides and technical recommendations for the sectors and areas that are critical for society and national interests, and promoting, where appropriate, the adoption of instruments such as guidelines, codes and other self-regulation mechanisms.

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

Secondly, taking into account the concerns and contributions received from civil society and the private sector during the work process developed for the preparation of this report, this Agency would also like to underline, as a general recommendation, the importance of the regulatory measures that are adopted**:**

1. are preceded and supported by a process of public discussion based on a multi-stakeholder approach;
2. take into account both the impact of under-regulation and the impact of over-regulation;
3. are analyzed interdisciplinarily involving different expert knowledge.

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

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

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

- Creation of a forum to identify priorities and formulate recommendations by different social actors.
- Holding a public hearing before the Legislative Branch in which companies, academia and specialized civil society participate.

- Creation of advisory groups with the participation of all stakeholders, which function on a regular basis.

Finally, thirdly, this Agency would like to highlight as a general recommendation the importance of ensuring that, in the event of the creation of new regulatory instruments, these include a process of periodic review and updating, based on the challenges that emerge.

Specific recommendations

A summary of recommendations is made based on the defined guidelines and thematic lines covered.

Institutionality and governance of AI

As mentioned above, this is a central aspect in many of the international instruments, and there are various formulas applied in different jurisdictions that seek, in one way or another, to establish a specific institutional framework for AI, either by relying on pre-existing institutions, or by generating new ones. Likewise, the definition of the institutional framework for AI in the country impacts the data governance mechanisms – which must be established – and therefore the development of AI itself.

Agesic's role in the institutionalization of AI

Regarding the role of Agesic, it is proposed to evaluate the possibility of enhancing the Agency's current capabilities by establishing a new internal structure that includes the Artificial Intelligence and Data line, 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. Agesic's potential would also be leveraged, since it is currently responsible for aspects of data management within public entities.

It may be appropriate – although not strictly necessary – to establish a legal regulatory provision in which the Agency is given additional powers to those already existing – indicated in article 74 in fine and in article 75 of Law No. 20,212 – including its role in coordination with other entities at the national level and the representation of the country at the international level on this issue. Beyond the above, it should be remembered that the Agency's leadership in matters of transformation and digital policy results from several pre-existing provisions that have already been outlined.

Without prejudice to Agesic's leadership in the matter, it is observed that the participation of other actors inside and outside the public sector is necessary, in order to collaborate in the design and implementation of comprehensive public policies. Since its beginnings, Agesic has had a set of Advisory Boards and leads various strategic committees.

In terms of the strategy for adopting an artificial intelligence and data policy, the normative institutionalization of the current Strategic Committee of the Public Sector for Artificial Intelligence and Data is proposed, which coordinates with the Agency not only the development of the National Strategy for AI and Data but also the planning of the action plans that allow its implementation.

The Committee's fundamental roles include collaboration with Agesic in the development of general policies on the matter, in addition to working with other competent public entities when developing sectoral policies. In this model, the sectoral public entities would be the ones to carry out the processes of developing sectoral regulations and recommendations, monitoring and supervising compliance, alerting Agesic and the Committee in the event of deviations.

Another aspect to consider and which may motivate a different integration of the Committee is the definition of other issues that arise from the participatory process of creating the National AI and Data Strategies and that guide public policy on these issues.

In accordance with the provisions of Article 74 in fine of Law No. 20,212, the sectoral oversight processes that correspond to public oversight entities will have the collaboration of Agesic - and eventually of the Committee - when AI systems are used.

Beyond specific integrations, this Agency understands that there are entities that must be part of this institutionality (such as ANII, MIEM, URCDP, INDDHH), in order to comply with the guidelines given by the Legislative Branch regarding the development of an AI based on ethics, which promotes innovation and respects human rights.

Institutionality of AI within organizations

Two lines of action are suggested with respect to the internal affairs of public entities: i. a line of training and strengthening in AI and Data, and, ii. a line of structural strengthening to provide each institution with capacities that allow the management, monitoring and control of the policies that are implemented, as well as to carry out strategic and operational plans aligned with said policies.

To date, there are a set of figures that must be established by public entities and that are related to data governance: the figure of the personal data protection delegate - established by article 40 of Law No. 19,670, of October 15, 2019 -, the figure of the person responsible for transparency - established by articles 41 and 57 of decree No. 232/010, of August 2, 2010, regulating Law No. 18,381, of October 17, 2008 - and the figure of the person responsible for information security - legally established by article 78, letter B of Law No. 20,212, of November 6, 2023 -.

The particularity of the figures of the data protection officer and the information security officer is that they extend not only to public entities but also to some private entities:

- In the case of the first of the indicated figures, it extends to those private entities that process sensitive data as their main business - the definition of sensitive data being exhaustive and provided for in article 4, letter E of Law No. 18,331, of August 11, 2008 - and those that process large volumes of data - defined as data of more than 35,000 people by article 10, letter c of decree No. 64/020, of February 17, 2020 -;

- In the case of the second, it refers to private entities linked to critical services or sectors of the country - which depends on the definition given by the regulations that to date have not yet been issued.

Added to this is the need to have referents who implement open data policies in public entities, linked to compliance with the provisions of Article 82 of Law No. 19,355, of December 12, 2015.

This Agency believes that it is possible to reconvert the functions of existing figures, especially that of the data protection officer, through training in AI and data governance. It does seem appropriate to create an Internal Data Committee within public organizations that includes the figure of the data protection officer, the person responsible for information security, the person responsible for transparency and the person responsible for open data.

Multisectoral and multidisciplinary perspective

The need for policy definition to take into account a multi-stakeholder perspective, including public and private entities, academia and civil society, as well as the different productive sectors, has been mentioned repeatedly throughout this report. It has also been suggested that organizations have strategic roles in AI and Data that enable the development of policies in this area and enhance the opportunities that both topics offer.

To this end, it is proposed to base itself on existing Agesic institutions, modifying the powers of the Honorary Advisory Council on the Information Society, and eventually incorporating new actors, in a scheme similar to the one currently existing in the field of Cybersecurity. In addition, multidisciplinarity must be considered.

There are currently two areas linked to AI in Agesic that should be maintained and strengthened: 1) the AI Community in Public Administration[98], made up of technical representatives from different public entities; 2) the Observatory of the use of AI in the State[99], created as part of a commitment

---

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

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

assumed in the 5th Open Government Action Plan. Both spaces enable the participation of different actors in the ecosystem, with complementary purposes and of great value for the development of AI, highlighting the participation of civil society and specialized technicians in the field.

Data governance

Finally, and with regard to data governance, progress should continue to be made in the obligations of public entities to publish data in a secure manner – through the platform provided for by the regulations – and in a manner that respects the protection of personal data, going beyond the obligation established in Article 5 of Law No. 18,381, of October 17, 2008.

We must also continue to move towards a data governance model that provides sustainability to the policy defined in this area.

It is also important to continue promoting the mandatory exchange of information – within the current framework – between public entities (article 157 and following of Law No. 18719), in order to promote the reuse of data, and to move forward in establishing those responsible for the Government's master data.

The use of data from private entities can also make a difference in this area, for which incentive measures could be promoted in the event that it is decided to share data – not necessarily personal, but useful for defining public policies. These incentive measures are not present in the current regulations, but could include tax exemptions and improvements in the provision of services, in addition to strictly reputational aspects.

At international level, Regulation (EU) 2023/2854 (Data Act)[100], establishes certain rights for users of devices to access and share their data, obligations of private companies to share information in the event that it is required by public entities and to comply 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 standardisation strategy for a single, resilient, green and digital market – among others.

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

In the aspects of data use at market level, the perspective of the Consumer Protection Unit and the Commission for the Promotion and Defense of Competition, both of the Ministry of Economy and Finance, should be included.

Regarding personal data and system training, it seems necessary to discuss the current regulation regarding legitimate bases for processing personal data. Thus, Article 9 of Law No. 18,331 of August 11, 2008, omits the inclusion of treatment bases that do exist at an international level, and the existing ones may generate some interpretative difficulties when they are applied to train AI systems. Although this circumstance does not necessarily prevent the use of data, the lack of a basis for legitimation such as legitimate interest adds complexity to the issue and leads to considering whether it is possible to use other bases for these purposes.

Other instruments such as the one suggested by the INDDHH for data trusts have begun to form part of the discussion. However, the delicate balance in the treatment of personal data provided for in Law No. 18,331 motivates this discussion to 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 institutionality and governance	
Recommendations oriented to eventual modifications or updates regulations	- Create Internal Data Committees in public entities, including transparency officers, data protection officers, information officers, and open data referents. - Promote the use of open and interoperable data, considering including new obligations for public entities associated with the publication of data in open format, establishing deadlines and conditions for such publication
Other initiatives recommended	- Specify Agesic's responsibilities related to leadership in AI and Data - Create a new institution within Agesic in charge of AI and Data policy. - Institutionalize the Public Sector Strategic Committee for AI and Data. - Reformulate the Honorary Advisory Council on Information Society to incorporate new actors and functions. - Define a data governance model. - Strengthen the training of public entities and provide them with the necessary capabilities to ensure that they can carry out the implementation of policies, strategies and operational plans on AI and data

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

Ethics, Human Rights and Democracy

The starting point for the protection of human rights

Uruguay maintains a close relationship with the Inter-American System and the Universal System for the Protection of Human Rights, has ratified the human rights treaties arising from these systems and actively participates in their bodies. The recommendations formulated in this section are based on considering the range of obligations (respect, protect and guarantee) that States derive from the international protection of human rights.

Along these lines, the recent Resolution on AI of the United Nations General Assembly highlights “that human rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle of artificial intelligence systems” and “urges all Member States and, where appropriate, “Calls upon all interested parties to refrain from or cease using artificial intelligence systems that are impossible to operate in accordance with international law or that pose undue risks to the enjoyment of human rights, in particular of those in vulnerable situations, and reaffirms that the rights of individuals must also be protected on the Internet, including during the life cycle of artificial intelligence systems.”[102].

The legal protection of human rights in our country is based on the Constitution of the Republic, the norms of international human rights law that have been ratified, and a wide and diverse set of laws that specify the protection and regulate the exercise of certain rights. However, the legal protection of human rights in this field would be strengthened with the development of norms that specify protection in this area, in some cases.

Special measures aimed at the protection of human rights

Based on what has been set out in the previous section, and based on what has already been advanced through Law No. 20,212, the first recommendation aims to expand the specification of principles oriented to the AI Strategy made by article 74 of the aforementioned law, indicating them as guiding principles of AI policies and their different regulatory instruments.

However, these principles can be complemented with measures that provide them with substantive content and allow them to be put into practice, taking as a basis articles 6 to 12 of Law No. 18,331, which not only list the scope of the principles, but also determine certain actions that must be carried out in practice by those responsible for and in charge of processing personal data.

Additionally, and based on the guidance provided by Article 74 of Law No. 20,212, the current and potential risks and adverse impacts on human rights involved in the life cycle 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, through regulation and other measures.

Based on the need to address the above risks and impacts, it is suggested to consider adopting a risk-based approach in order to:

1. Analyze and define the applications of AI systems that are unacceptable to society due to their impact on people's rights, evaluating the prohibitions or moratoriums that are appropriate and consistent with the obligation to protect human rights; and,

2. Identify and define those AI applications that pose a high risk to people's rights based on the context and intended use, the severity and likelihood of potential impacts, in order to define the specific measures that may be applicable.

In order to address risks, different models and approaches have been developed at a comparative level. For example:

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

- The Executive Order adopted in 2023 by the United States Government orders government entities in accordance with their respective competencies to adopt different measures aimed at having guidelines and standards for the responsible development and implementation of AI according to their area of activity and provides a set of obligations aimed at providing information to different national agencies by companies that develop certain AI models.

- Article 16 of the Framework Convention adopted in March by the Council of Europe also states that each Party shall assess the need for a moratorium or ban or other appropriate measures with respect to certain uses of AI systems when it considers that such uses are incompatible with respect for human rights, the functioning of democracy or the rule of law.

Thus, it is suggested to assess, for certain types of risks that require special measures:

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

2. Establish the obligation to register the system in a publicly accessible state registry by the entity leading the AI policy in the country;

3. The submission of the systems to a prior authorization or certification process depending on the purpose or type of system involved;

4. Provide mechanisms for periodic auditing of the systems and eventual submission of results to the entity in charge of their review;

5. Complement the rules that guarantee the transparency and explainability of AI systems used to make decisions or to support decision-making, and human oversight related to the operation and results of such systems.

Furthermore, as highlighted in the preliminary 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 the provision of public services, facilitate access to knowledge, education, healthcare, productive development, agriculture, etc.

Consequently, along with addressing the risks, it is recommended to consider promoting the development of AI systems that aim for the common good.

through the determination of purposes that are understood to fulfill said purpose, also defining support and promotion measures, among others.

Implementation of rights

From the perspective of people, it is suggested to consider the implementation through legal provisions of certain rights such as:

1. The right to know that you are interacting with an AI system;
2. The right to obtain basic information on the operation of the system and the expected results, through a natural person if necessary and;

3. Eventually, the right to appeal when a decision is made based on that system, complementing the right to challenge personal assessments and the right to information provided for in Law No. 18,331 on the protection of personal data.

Equality and non-discrimination

The current National Digital Citizenship Strategy[103]points out that the "impacts that may arise in the context of the development of disruptive technologies such as artificial intelligence (AI) go beyond the individual, encompassing collective and social effects. In other words, we can speak of 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."

In the research work "Building citizenship in digital environments. Transversal perspectives of approach[104]", following the ECLAC document "Digital citizenship in Latin America. Conceptual review of initiatives",

---

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

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

It suggests that the concept of the digital divide today is associated with gaps in the uses and benefits of digital technologies (derived from differences in socioeconomic level, age, gender, cultural capital and digital skills).

The paper highlights the need to incorporate a perspective of inclusion or digital equality, and to develop the skills necessary to overcome limitations of access and capabilities, as well as to understand the rules of the game and reflect on our own behaviors.

Actions based on the recommendations in this document should include an approach that takes into account, in particular, the increased vulnerability faced by various groups in society, by adopting frameworks and policies to address biases that may deepen inequalities, and to protect people from all forms of discrimination and ensure that discriminatory outcomes are not passed on to AI systems, and where appropriate are detected and corrected.

Facing the challenges for democracies

There is growing global concern about the impact of disinformation and the protection of the integrity of democratic processes and the ability of people to form their opinions freely.

In this regard, for example, when analyzing the impacts and risks involved in Artificial Intelligence, the interim report of the UN High-Level Advisory Body on AI [105]analyzes that some AI risks originate in the technical limitations of these systems, such as harmful biases or so-called hallucinations in generative AI, while others are the product of human use, such as deep fakes, which "can pose a serious risk to social trust and democratic debate."

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

The Organization of American States (OAS) has decided to task the General Secretariat with developing an inter-American agenda on emerging technologies, particularly with regard to the ethical use of AI policies, algorithms and data governance, within the framework of a set of measures aimed specifically at strengthening democracy.

International concern about the above-mentioned challenges was reflected in the latest update of the OECD Principles on AI in 2024, in which one of the objectives was precisely to reflect the growing importance of addressing these phenomena in the context of generative AI. In this sense, the principles propose “addressing disinformation amplified by AI, 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, it is necessary to consider measures that are not only restrictive – undoubtedly necessary – but also digital and information literacy, generating instrumental and fundamental skills for the critical interaction of people in the digital environment.

As part of these measures, mechanisms can be promoted to identify the manipulation of information and content generated by AI, and 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 resources

In our legal system there are various public entities with powers in matters of human rights outside the scope of the justice system, such as the National Institution for Human Rights and the Ombudsman's Office, the Personal Data Regulatory and Control Unit, and the Public Information Access Unit, among others.

---

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

In order to ensure that potential human rights violations resulting from the use of AI are addressed through accessible, appropriate and effective mechanisms and resources, it is suggested that an analysis of current mechanisms be carried out in order to identify whether there is a need to strengthen the specific competencies of existing bodies or to create new mechanisms that may be necessary, as well as the articulation of their competencies.

Regulation of the development, use and acquisition of AI in the public sector

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

In identifying the key dimensions for the adoption of AI in Public Administration, the Charter proposes as a component of national strategies that: “national legislation should address issues that ensure that algorithmic systems are safe, transparent, traceable, non-discriminatory and environmentally sustainable. Regulations on the protection of personal data, as well as the use and reuse of public data in general, should also be adapted. Additionally, it must be guaranteed that Artificial Intelligence systems are supervised by humans, rather than being completely autonomous, minimizing potential damage and eliminating situations of extreme risk. In addition, 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 infrastructures. Finally, it would be necessary to ensure that public algorithms are transparent and not proprietary or subject to patents, promoting technological infrastructures based on open architectures."

These are principles shared by the AI Strategy currently under review, which also stresses that "any technological solution using AI must respect human rights, individual freedoms and diversity."

Based on the path that Uruguay has already been following within the framework of its national digital policy focused on people by definition, it is recommended to continue strengthening the regulatory instruments related to the public sphere, integrating those components of the new AI Strategy to be adopted in 2024 related to the use and development of these technologies specifically in this area.

In this regard, a specific measure to consider is the performance of human rights impact assessments as a requirement for the acquisition, development and/or use of AI systems by public entities in areas where it is determined that there may be a high risk to people's rights; Based on what has already been expressed, and in particular, it is recommended to analyze as part of the package of measures to be evaluated, the regulation of the development, acquisition and application of surveillance systems for public security purposes.

Additionally, and given that the development of Data and Cybersecurity strategies is underway, it will also be relevant to consider the guidelines defined therein to identify the elements that require legal regulation to complement the pre-existing general frameworks.

Training and education for AI

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

Other aspects related to the impact of AI on the world of work will require more comprehensive developments and open discussion with the participation of the State, employers, workers and unions, in order to obtain agreements that enhance the benefits of the application of this technology and mitigate adverse effects.

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

1. the promotion of training programs through technical, tertiary and university education entities on AI and data management issues, in collaboration with business chambers, unions, and other groups;

2. Establish specific support or particular benefits for companies that offer AI-oriented courses for their employees and management bodies, in predefined sectors;
3. Evaluate the obligation for employers to train workers who must implement or who may be affected by AI systems, prior to their implementation, in predefined sectors.

Summary of recommendations on ethics, human rights and democracy	
Recommendations for possible regulatory changes or updates	- Make explicit the principles listed in Article 74 of Law 20.2012 as guiding principles of the policy national AI and its implementation. - Define risks that are unacceptable as a society; and identify uses that represent a high risk and require measures

	special, also defining such measures. - Evaluate the adoption of measures aimed at combating disinformation and protecting the integrity of democratic processes and the ability of people to form their opinions freely. - Analyze the strengthening of existing mechanisms or the creation of new mechanisms to resolve rights violations humans resulting from AI systems. - Regulate instrumental rights in favor of transparency, explainability and challengeability.
Other recommended initiatives	- Establish specific rules regarding the development, use and acquisition of AI in the public sector. - Evaluate regional and international cooperation instruments on this matter. - Analyze the adoption of measures to continue addressing digital gaps and strengthen the development of digital citizenship.

	- Promote initiatives to use AI for the good of society. - Promote training especially for workers in collaboration with chambers business, unions, and other groups, and establish specific support or particular benefits for companies that carry out courses oriented to AI, in sectors predefined. - Evaluate the obligation for employers to train workers who must implement or who may be affected by AI systems, prior to their implementation, in predefined sectors.

Responsible innovation

Legal certainty in the aspects of civil liability and intellectual property

The analyses carried out show the need to review the national civil liability regime, as it does not seem reasonable to resort to interpretations or integrations of regulations that are not consistent with current reality, in order to provide greater certainty to developers, users and other actors in the system.

It is suggested to consider the following alternatives: i. to determine with competent entities suggestions for minimum content in contracts to be signed between those who make systems available and those who use them. In this regard, the regulations on proactive responsibility for the protection of personal data may be considered as background; ii. to establish a commission of analysis that specifically focuses on a possible reform of the civil liability regime in this area.

Legal certainty is also associated with an adequate system of attribution of rights in the case of creations in which an AI system is involved in some way.

This Agency suggests:

1. In the case of works generated by AI 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 considered for domestic use, or for other purposes;
2. Initiate a consultation process on how works generated exclusively by AI will be considered. There is currently no consensus on the view that such works can be attributed to these systems, so the consultation should be carried out with all the actors involved, taking into account not only aspects associated with the attribution of ownership but also the corresponding financial compensation;
3. Consider a definition of the system to be applied to AI-assisted works, such as attributing it to the person who directs the creative process of the finished work.[109];
4. Reaffirm that the scope for the treatment of data used by these systems for the generation of new works will depend on the current regulations - Article 35 of Law No. 9,376, and Article 9° bis of the Law No. 18,331-.

In other aspects related to intellectual property, it is suggested to consider that:

---

[109] Various alternatives in this regard can be seen in MANTEGNA. Op. Cit. Page 309.

1. Regarding registration, continue with the process already initiated by Law No. 20,212, and evaluate the possibility of communication between this registry, other registries, and the publication of public software indicated in article 7 of decree No. 44/015 in the case of public entities;

2. Extend the scope of Article 2 of Law No. 19,179 to computer programs (source programs or object programs), compilations of data or other materials, in any form, which for reasons of the selection or arrangement of their contents constitute creations of an intellectual nature, and the expression of ideas, information and algorithms, formulated in original sequences ordered in an appropriate manner to be used by an information processing or automatic control device.

Infrastructure and cybersecurity

This report has already raised the need for an adequate infrastructure for the development of AI, and the relevant role of the State in achieving this objective.

Following the OECD report released when analyzing this line, it seems necessary to adopt a set of measures associated with the review of computing capacities in the public and private sectors, consider the number, capacity and availability of existing data centers, define standards in data management, analyze processing capacities and hardware needs in the country, determine the potential demand for AI processing, distinguish processing needs for AI, provide training and coaching, map and analyze supply chains.

It is considered necessary to generate or update regulatory instruments that facilitate the acquisition, operation and maintenance of these infrastructures in order to promote capacity management that quickly adapts to the exponential progress shown by this particular technology.

For the purposes of this report, the purpose of which is to provide recommendations to the Legislative Branch, the analyses carried out must also be aimed at determining whether the current regulatory provisions are aligned with the needs in this area.

From this perspective, this Agency wishes to highlight that there is extensive legislation and regulation in areas such as data exchange, cybersecurity, the processing of information – personal and non-personal –, telecommunications networks, public procurement, among others. The difficulty posed by the existing regulatory dispersion can be acknowledged, which is why it could be relevant to organize the aforementioned regulations through an ordered text or similar instruments.

Cybersecurity in particular has been the subject of regulation since the creation of Agesic, and its relevance has recently been highlighted with the systematization of different provisions and the updating of the Agency's powers and the obligations of public entities in general and some private entities in particular, in several articles of Law No. 20,212.

The results of the process of building the National Cybersecurity Strategy, and the strategic objectives resulting from this process – as already mentioned on repeated occasions in this report – will be a central input for determining new measures that contribute to a secure ecosystem for the development of AI and other technologies.

In terms of infrastructure, and considering the contributions received throughout the process of preparing this report, Agesic proposes promoting a dialogue with other actors in this regard, for which the following alternatives are suggested:

1. Add as a specific task of the Public Information Technology Advisory Council the task of collaborating in the definition of recommendations;

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

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

In particular, in aspects of regulatory support for the secure exchange of data, it is advisable to enable the use of the Interoperability Platform created by decree No. 178/013 for the consumption of services by private entities and to evaluate the modification of decree No. 92/014, to normatively clarify the assumptions associated with the use of cloud provider services.

A comprehensive perspective of infrastructure and processes for digital transformation

It is necessary to work from a comprehensive perspective, rethinking the way in which the use of state infrastructure and processes is planned, facilitating the deployment of technology such as AI.

In this sense, the goal should be to promote the use of AI as an opportunity to improve public services, state efficiency and data-driven decision-making.

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

From this perspective, the improvement in the State's infrastructure, which supports technology such as AI, should result in a benefit for innovation and

---

[110] The provisional report of the initiative 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 economic and social development of the country.

In this logic, the aim should be to ensure that infrastructure components, when appropriate, can be used by actors in the innovative, scientific and entrepreneurial ecosystem, especially considering the different characteristics of these actors.

Environmental impacts of infrastructure

Although the environmental aspect was not part of the central thematic lines of this report, it is unavoidable to make some reference to the impacts that the accelerated development of technology in general and of AI in particular has on the environment.

The use of AI can generate great benefits to mitigate the impacts of climate change, and in fact, different initiatives, even at a national level, promote developments that attack this problem.[111].

However, there are aspects of negative impact linked to the extraction of materials for the creation of hardware components, the use of water, energy consumption, among others, which makes it necessary to bring the relevant authorities and actors into this discussion.

UNESCO's recommendation on AI ethics clearly points out the need for all those involved in the life cycle of AI systems to respect national and international standards and practices linked to precaution, designed for the protection and restoration of the environment and ecosystems, and for sustainable development.

CLAD includes among the principles of its charter the principles of sustainability and environmental protection, defending the use of environmentally sustainable and energy-friendly technologies, based on the application of materials and

---

[111] See as an example:https://www.anii.org.uy/apoyos/innovacion/309/fondo-de-investigacion-e-innovacion-en-cambio-climatic/ . Last accessed: 20/06/2024.

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

In light of the above, the environmental perspective must be present in any initiative associated with the development of infrastructure for AI.

Promotional measures

Promotion measures are multiple and should focus not on promoting technology, but on objectives to be achieved through it. The analysis mentioned some measures that arise from current regulations, and the entities in charge of carrying them out.

In January this year, the European Commission launched a package of measures to support European startups and small and medium-sized enterprises for the development of safe AI. Included in the aforementioned package is the installation of AI factories with supercomputers accessible to SMEs, support in the use of AI models for general purposes, the creation of an AI office within the Commission, financial support through different programs and the development of data spaces, among others.

From the process of building the strategies led by this Agency, the need for infrastructure development to include instruments such as tariff benefits, tax exemptions and incentives for the import of components and export of services from our country, among others, repeatedly arises.

Some promotional measures, such as incentives, exemptions, and other benefits that already exist in current regulations can be directed or reoriented to promoting activities that, thanks to AI, can result in a benefit for the economy, society, and, ultimately, people.

In terms of support for AI in the Public Sector, the World Bank already in 2021[112] suggested the establishment of a central innovation hub for AI in the 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 that our country currently has. In this document, the World Bank points out that investments should be directed towards human capital and digital infrastructure, prioritizing research, entrepreneurship, foundational digital technologies and digital skills.

The objectives set in this regard are linked, among others and at the discretion of this Agency, to the objectives already defined in the Uruguay 2025 Digital Agenda and to those resulting from the process of building the national Data and Cybersecurity strategies, and from the update of the National Artificial Intelligence Strategy.

Beyond the alternatives of financial support based on current regulations, there are other types of measures that promote the responsible use of AI, among which we find regulatory sandboxes and data spaces, instruments that enable safe experimentation, a limited framework of responsibility, and the collaboration of multiple parties (public, private, academic and civil society sectors).

For its part, the path of international cooperation in this area must be continued, as well as the signing of agreements that enable a better positioning of the country in terms of innovation and safe research in AI, as is the case with the signing of the recent Patent Cooperation Treaty.

Summary of recommendations on promoting innovation in AI	
Recommendations for possible regulatory changes or updates	- Promote the extension of the purpose 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 commission of analysis for a possible reform of the civil liability regime in this area. - Analyze, together with the competent bodies, proposals for minimum scope of liability in contracts signed between developers, users and other actors in AI systems. - In terms of Intellectual Property, promote a discussion on alternatives for the generation of works by AI without direct human intervention and for works assisted by AI. - Continue with the registration process initiated by Law No. 20,212, of November 6, 2023, and evaluate the communication between this registry, other registries, and the publication of public software. - Evaluate including as a specific task of the Public Information Technology Advisory Council the collaboration with Agesic in defining the necessary recommendations for the adequate development of the infrastructure for AI at the country level.

	- Consider preparing an analysis of the current and comprehensive infrastructure in this area, which will especially take into account measures for public investment and the promotion of private investment. - Evaluate the definition of a new cloud usage policy based on the one established in Decree No. 92/014, dated April 7, 2014. - Establish collaboration between entities in charge of promoting initiatives in the field of AI infrastructure, especially including the environmental perspective. - Consolidate the tools necessary to carry out the actions defined in the National Cybersecurity Strategy. - Finalize and implement the proposed regulation of controlled testing environments and other measures to promote innovation. - Evaluate together with the MEF, the MIEM, the ANII and other competent public entities the determination of the necessary support measures.

Annex 1: National background

Mapping of national regulations

In preparing this report, the existence of a set of legal and regulatory provisions was taken into account, which sought to focus strictly on aspects linked to the defined thematic lines and their link with AI.

Below is a table with the identified provisions, distinguished according to the associated thematic line and a brief description of each of them.

Institutionality of AI

Applicable standards	**Content summary**
Article 74 Law No. 20,212, of 6 November 2023	It places Agesic in charge of designing and developing a national data and AI strategy. In addition, the final paragraph expressly establishes that Agesic will make specific recommendations to public and private sector entities for the development and implementation of the aforementioned artificial intelligence systems, and for the supervision of their compliance, without prejudice to the powers of the URCDP and other public entities in their respective areas of action.
Article 34 Law No. 18,331, of August 11, 2008, as amended by article 63 of Law No. 20,075, of	It establishes within the duties of the URCDP the establishment of the criteria and procedures that must be observed by those responsible and in charge, in the automated processing of personal data indicated in article 16 of law No. 18,331.

October 20, 2022.	

Data governance

Applicable standards	Issue	Content summary
Law No. 18,331, of August 11, 2008, amendments and concordant, and No. 19,670, of October 15, 2018. Regulated by Decrees No. 414/009, of August 31, 2009, and 64/020, of February 17, 2020.	Data Personal	The forms of treatment of personal data in the public and private sectors are established, associated with a set of principles.
Law No. 18,381, of October 17, 2008. Standard regulated by Decree No. 232/010, of August 2, 2010.	Information Public	The public nature of information held by the State is established, as well as its exceptions.
Articles 157 to 160 of Law No. 18,719,	Interoperability ity and exchange	The conditions for interoperability and the exchange of public and private information are established in accordance with the regulations. Regulated standard

December 27, 2010		by decree No. 178/013, of June 11, 2013.
Decree No. 259/012, August 13, 2012	Data open and Government Open	Uruguay adheres to the "Open Government Declaration" of the "Open Government Partnership" and establishes the first action plan, which was followed by other subsequent plans.
Article 82 of Law No. 19,355, of December 19, 2015	Data Open and Government Open	The obligation of public bodies to publish the information contained in Article 5 of Law No. 18,381, in open data format is established. regulated by decree No. 54/017, of February 20, 2017.
Article 76 of Law No. 19,355, of December 19, 2015 in the editorial office given by article 2 of Law No. 19,670, of October 15, 2018	Interoperability ity and exchange	The obligation of public bodies not to request certificates is established, certificates, testimonies or other documentation of a similar nature issued by another public entity, when the information contained in said documents can be accessed through computer systems provided by the competent entities. Regulation regulated by decree No. 353/023, of November 9, 2023.
Decree No. 357/016, November 7, 2016	Data Open and Government Open	The Open Government Working Group is created, made up of a representative from each of the following organizations: Agesic, OPP, UAIP, MEF, MRREE, MIEM and INE. Their duties are also established.

Application of principles in AI

Rules	Content summary
Article 74 Law No. 20,212, of 6 November 2023	It puts Agesic in charge of designing and developing a national data and AI strategy. The second paragraph of the article establishes that "(t)he strategy must be based on principles of equity, non-discrimination, responsibility, accountability, transparency, auditing and safe innovation, respecting human dignity, the democratic system and the republican form of government. The principles of personal data protection included in Law No. 18,331, of August 11, 2008, will be part of the aforementioned strategy."
Article 5, Law No. 18,331, of August 11, 2008.	The article establishes the following principles for the protection of personal data, which Article 74 includes in the AI Strategy: legality, veracity, purpose, prior informed consent, data security, confidentiality and responsibility (proactive).

Intellectual Property

Applicable standards	Content summary
Constitution National, art. 33	It establishes that intellectual work, the rights of the author, the inventor or the artist, will be recognized and protected by law.

Law No. 9,739, of December 17, 1937, modified by Laws No. 17.616, of January 10, 2003, 19,857, of December 23, 2019 and 20,212, of December 6, November 2023. Regulated by Decrees No. 154/004, of May 3, 2004, 295/017, of October 16, 2017, 404/023, of December 12, 2023	It recognizes the right of authors to control the productions of their thought, science and art. Included in the protection of the law are computer programs or software and data compilations that, due to their content, constitute an intellectual creation. Rights are provided, a determined protection period, lawful and unlawful conduct and, eventually, sanctions. The works are registered in the National Library, with the exception of computer programs, data compilations or other materials that constitute intellectual creations, expressions of ideas, information and algorithms formulated in original sequences ordered to be used by an information processing or automatic control device and the transfer of property rights over these works, which will be registered in the Software Registry of the DNPI.
Law No. 14,910, of July 19, 1979	The aforementioned Law 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 December 13, 1994	The signed agreements resulting from the Uruguay Round of Multilateral Trade Negotiations, contained in the Final Act signed in Marrakech on April 15, 1994, and in particular the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), are hereby approved.

Law No. 17,011, of September 25, 1998. Regulated by Decree No. 34/999, of February 3, 1999.	The protection granted to trademarks is regulated, defined as a sign capable of distinguishing the products or services of one natural or legal person from those of another. Types of trademarks, rights, protection periods, registration, absolute and relative nullities with respect to certain signs are established. It also regulates trade names, geographical indications, designations of origin and indications of provenance.
Law No. 17,164, of September 2, 1999. Regulated by Decree No. 11/000, of January 13, 2000.	The rights and obligations regarding patents, utility models and industrial designs are regulated. As in the previous case, rights, nullities, protection periods, registration and possible sanctions are established.
Law No. 18,036, of October 20, 2006.	The World Intellectual Property Organization (WIPO) Copyright Treaty and Agreed Statements on the WIPO Copyright Treaty are adopted.
Law 18.253, of February 20, 2008	Approval of the World Intellectual Property Organization Treaty on Performances and Phonograms, and agreed statements relating thereto.
Law No. 19,179, of December 27, 2013. Regulated by Decree No. 44/015,	Regulates the format for the processing and storage of digital information in certain public and private entities.

of January 30, 2015.	

Infrastructure and Cybersecurity

Applicable standards	**Content summary**
Law No. 17,296, of February 21, 2001, articles 70 to 94 bis, in the wording given by Articles 143 and 418 of Law No. 18,719, of December 27, 2010, and 256 to 273 of Law No. 19,889, of July 9, 2020, among others. Regulated by Decree No. 212/001, May 4th 2001.	The powers of the Communications Services Regulatory Unit (URSEC) – currently a decentralized service -, of the Ministry of Industry, Energy and Mining (MIEM) and in particular of the National Directorate of Telecommunications and Audiovisual Communication Services (DINATEL) in telecommunications matters are established. As regards URSEC, the main tasks were established as regulation and control of the activities and sectors related to telecommunications and postal services. The definition of policies is the responsibility of MIEM.
Law No. 18,331, of August 11, 2008. Regulated by Decrees No. 414/009, of August 31, 2009 and	The general framework for the communication of personal data between public and private entities is established, as well as the basic requirements that must be met to ensure the security of the processing of personal data. Decree No. 64/020, of February 17, 2020, in particular recommends the adoption of certain security measures in its articles 3° and

64/020, of February 17, 2020.	4°, expressly suggesting the adoption of the Agesic Cybersecurity Framework.
Law No. 18,719, of December 27, 2010, article 149, in the editorial office given by article 84 of Law No. 19,924, of December 18, 2020.	Agesic is responsible for directing policies, methodologies and best practices, and regulating information security and cybersecurity at the national level, as well as supervising, auditing compliance and providing support in the implementation stages of these in all public entities, and also in private entities linked to critical services or sectors of the country.
Law No. 18,719, of December 27, 2010, articles 157 at 160. Regulated by Decree No. 178/013, June 11, 2013.	Rules are established for interoperability between public bodies. Agesic's role in the matter and its competences are established. The regulations determine the creation of an interoperability platform managed by this agency for the exchange of information between public entities.
Decree 92/014, of April 7, 2014	For the Central Administration, the obligation is established that secure data centres must be located in national territory, except for those that do not constitute a risk for the organisation. Likewise, the physical security conditions that must be put into practice by public entities are established in the Annex. The possibility of considering exceptions is also foreseen, with the granting of these being the responsibility of Agesic.
Law No. 19,924, of December 18, 2020, articles 372	The National Secretariat for Science and Technology is abolished and the name and powers of the Directorate are modified within the framework of the Ministry of Education and Culture.

a 375 that suppress the entity created by Law No. 19,355, of December 19, 2015, article 34, whose powers were found regulated by Decree No. 324/017, of November 10, 2017.	for the Development of Science and Knowledge, which is now called the National Directorate of Innovation, Science and Technology. The regulations of the aforementioned Secretariat had established within its competences, those of proposing science, technology and innovation policy projects, promoting the greater development of connectivity and telecommunications capacities and proposing infrastructures in the field of science, technology and innovation, in strategic areas for the development of the country.
Law No. 20,075, of October 20, 2022, article 461, regulated by Decree No. 216/023, July 17, 2023	The article provides for a budget allocation for the research, innovation and experimental development program to promote projects in science, technology and innovation, regulating by the aforementioned decree the creation of the Uruguay Innovation Hub Program, within the National Agency for Research and Innovation (ANII). Among its instruments are, for example, the installation of open laboratories, through financial and operational support.
Law No. 20,212, of November 6, 2023, articles 78 to 84.	Notwithstanding the fact that there are multiple regulations governing aspects of cybersecurity, both at a legal and regulatory level, the impetus that these articles provide to the matter is highlighted, imposing certain legal obligations on public entities and private entities linked to critical sectors or services in the country, as well as instruments for the control and supervision of their compliance by Agesic. On the other hand, the integration of two entities is established.

	Agesic advisers on cybersecurity and the definition of the bases for a National Strategy.

Work and training for AI

Applicable standards	Content summary
Law No. 18,046, of October 24, 2008. Regulated by Decree No. 52/021, February 8, 2021.	Law establishing the National Institute for Employment and Vocational Training (INEFOP). Its responsibilities include advising on the definition of training and education policies to generate and improve employment.
Law No. 18,437, of December 12, 2008. Regulated by Decrees No. 334/009, of July 20, 2009 and 294/013, of September 11, 2013.	The promotion of the enjoyment and effective exercise of the right to education as a fundamental human right is declared to be of general interest.
Law No. 19,121, of August 20, 2013.	The Statute of Public Officials of the Central Administration is regulated, promoting the training of public officials, which is considered essential for access to and promotion in office.

Decree No. 340/018, October 22, 2018.S	The National Commission for Occupational Certification is created within the scope of INEFOP.
Law No. 19,973, of August 13, 2021. Regulated by Decree No. 308/021, September 10, 2021.	Employment policies are established to promote paid employment for young people, adults and people with disabilities, including their training and education.

Civil liability and consumer rights

Applicable standards	**Content summary**
Civil code	The rules on liability are found in articles 1246 and following of the Civil Code, providing for contractual liability and non-contractual liability in the manner mentioned, providing, with some exceptions, a subjective liability regime for all types. In particular, article 1330 should be considered in this regard.
Law No. 17,250, of August 11, 2000. Regulated by Decree No. 244/000, of August 23, 2000.	In the specific case of consumer relations, a regime of subjective liability is also provided for. It establishes certain specificities related to liability in articles 34 to 36.

Promotional measures

Applicable standards	Content summary
Law No. 16,906, of January 7, 1998. Regulated by Decree No. 92/998, of April 21, 1998.	Law on investment and industrial promotion.
Article 461 of Law No. 20,075, of October 20, 2022	An annual budget of $400,000,000 (four hundred million Uruguayan pesos) is allocated from General Revenue, with the aim of promoting projects in science, technology and innovation, which are approved by the Ministry of Economy and Finance, with the advice of the Planning and Budget Office, at the proposal of the National Research and Innovation Agency.
Decree No. 216/023, July 17, 2023	The Uruguay Innovation Hub Program is created to promote the entrepreneurial and innovative ecosystem.
Law No. 20,121, of August 23, 2023. Regulated by Decree No. 360/023, November 14, 2023.	Law related to the promotion of the establishment in Uruguay of technicians and professionals in the information technology sector

Article 75 Law No. 20,212, of 6 November 2023	The creation of controlled test environments is promoted for projects that aim, among others, to build systems that apply AI.

Annex 2: International background

International principles and recommendations

Attention on artificial intelligence systems has become omnipresent on the agenda of international organizations and forums, covering the most diverse topics and areas: from how Artificial Intelligence can help achieve the Sustainable Development Goals, to debates around its application in the military field.

Amidst this diversity, however, it is possible to identify a common starting point in several of the international efforts made or underway aimed at the governance of artificial intelligence: and it is the emphasis on the need to build governance aimed at enhancing the opportunities and benefits implied in artificial intelligence for humanity by ensuring equitable access to these benefits, and at the same time addressing the challenges and risks derived from these technologies.

To this end, as the background outlined below shows, much of the ongoing effort emphasizes the need to adopt an approach that: puts people at the centre; protects human rights, democracy and the rule of law; is grounded in international law and international human rights law; promotes safe and reliable artificial intelligence systems that are developed and used in an ethical manner; and promotes innovation to harness the potential of AI for the benefit of humanity and sustainable development.

The objective of this annex to the Report is to present a summary of the guiding principles and recommendations that seek to guide the actions of States in the formulation of their legislation, policies or other instruments related to AI emerging from the international sphere, based on the review of international precedents carried out in the framework of the preparation of this report. These principles and recommendations should be understood as a complement to the international human rights obligations derived for States from current international law.

The selection of the reviewed backgrounds was made based on their international relevance and their impact in Uruguay, and they are presented in each subsection in chronological order.

United Nations

Within the United Nations, there is an ongoing process aimed at the international governance of Artificial Intelligence promoted by the Secretary General, while the Global Digital Compact is being negotiated, which would include a specific chapter on Artificial Intelligence. The Compact is expected to be adopted within the framework of the Future Summit that will take place next September. The ongoing processes have, as a background, among others, the milestones in the field of the United Nations that are 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]. It aims to guide States in formulating their laws and policies relating to artificial intelligence. To this end, the Recommendation promotes a set of values[114], principles and policy actions.

The text analyses “the profound and dynamic positive and negative repercussions of artificial intelligence” on societies, the environment and human life and states that “taking into account risks and ethical concerns should not hinder innovation and development”, but on the contrary, stimulate

---

[113] UNESCO. Recommendation on the Ethics of Artificial Intelligence, Adopted on 23 November 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381137_eng . Last accessed: 29/4/2024.

[114] The values indicated are: Respect, protection and promotion of human rights, fundamental freedoms and human dignity. Prosperity of the environment and ecosystems. Guaranteeing diversity and inclusion. Living in peaceful, fair and interconnected societies.

Research and innovation carried out in an ethical and human rights-based manner[115].

In 2023, Uruguay adhered to the UNESCO Recommendation, thus reinforcing the country's commitment to implementing the framework of the new Artificial Intelligence Strategy and the first National Data Strategy.[116].For the above reasons and given its importance as a frame of reference for the preparation of this Report, a summary of the 10 guiding principles promoted by the Recommendation is presented below.

UNESCO Principles[117]

Principle	**Scope**
Proportionality and safety.	The Recommendation states that risk assessment procedures and measures to prevent damage to humans, the environment and ecosystems should be ensured. It should also be ensured that processes related to the life cycle of AI systems are aligned with legitimate purposes or objectives. The Recommendation maintains that AI systems should not be used for social scoring or mass surveillance purposes.
Safety and protection.	The Recommendation states that security and protection risks should be identified,

---

[115] Ibid. Preamble.

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

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

	prevented and eliminated throughout the AI lifecycle.
Equity and not discrimination	The Recommendation highlights that an inclusive approach should be taken to ensure that the benefits of AI technologies are available and accessible to all, taking into account the specific needs of different groups. It also argues that digital divides within and between countries and biases throughout the life cycle of AI systems should be addressed.
Sustainability	The Recommendation underlines the need to assess the sustainability impacts of AI technologies, i.e. the continuous evaluation of the human, social, cultural, economic and environmental effects involved in this technology.
Right to privacy and data protection.	The Recommendation states that privacy should be respected, protected and promoted throughout the lifecycle of AI systems. It argues that algorithmic systems require appropriate privacy impact assessments, and notes that appropriate data protection frameworks and data governance mechanisms should be established, and in line with a multi-stakeholder approach.
Supervision and decision human	The Recommendation maintains that Member States should ensure that, at any stage of the life cycle of AI systems, they always

	it is possible to attribute ethical and legal responsibility to existing natural persons or legal entities.
Transparency and explainability	The Recommendation states that people should be fully informed when a decision is based on AI algorithms or is made based on their results, and in particular when it impacts on their rights, and suggests that there should be appropriate mechanisms to review and amend the decision. It argues that AI actors should inform users in an appropriate and timely manner when a product or service is provided directly or with the help of an AI system. The Recommendation defines explainability as making the results of AI systems intelligible and providing information about them. It also refers to the intelligibility of the input, output and operation of each algorithmic component and the way it contributes to the results of the systems (traceability).
Responsibility and accountability	The Recommendation states that AI actors and Member States should respect, protect and promote human rights, encourage the protection of the environment and ecosystems, assuming their respective ethical and legal responsibilities. To this end, appropriate monitoring, impact assessment, auditing and due diligence mechanisms should be developed, including with regard to the protection of whistleblowers.

	irregularities, to ensure accountability for AI systems and their impact throughout their lifecycle.
Awareness and education.	The Recommendation emphasizes that public awareness and understanding of AI technologies, their functioning and impact should be promoted through open and accessible education, civic participation, digital skills and training on AI ethics, media and information literacy.
Governance and adaptive and multi-stakeholder collaboration.	The Recommendation states that in order to ensure an inclusive approach to AI governance, it is necessary to guarantee the participation of different stakeholders (governments, intergovernmental organizations, academia, civil society, the private sector, human rights institutions, among others).

In order to implement these principles, the UNESCO Recommendation promotes a set of specific actions to be implemented by States and other actors. Based on the purpose of this report, the following are highlighted:

- Ensure AI governance mechanisms are inclusive, transparent, multidisciplinary and multi-stakeholder.

- Ensure that legislation on AI systems complies with Member States' human rights obligations and promote human rights and fundamental freedoms throughout the life cycle of these systems.

- 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 should always ultimately rest with natural or legal persons and that AI systems themselves should not be granted legal personality and incorporate the principle of human oversight.

- Have frameworks in place to protect personal data and ensure effective and independent oversight within a data governance mechanism.
- Establish clear requirements for transparency and explainability of AI systems to help ensure the trustworthiness of such systems throughout their lifecycle. These requirements should cover the design and implementation of impact assessment mechanisms that take into account the nature of the scope, intended use, audiences and feasibility of each particular AI system.

- Ensure compliance with environmental laws, policies and practices by all AI stakeholders.
- Allocate specific funds from the public budget to finance gender-responsive plans, ensure that national digital policies include a gender action plan and develop relevant policies.

- Promote general awareness-raising programmes on AI developments, including on data and the opportunities and challenges posed by AI technologies, the impact of AI systems on human rights, including children's rights, and their implications. These programmes should be accessible to both technical and non-technical groups.

- Promote research and encourage private sector companies to facilitate access to their data for research purposes by the scientific community.
- Ensure that AI actors respect and promote freedom of expression and access to information in relation to the automatic generation, moderation and curation of content, through appropriate frameworks, including regulatory frameworks, that enable transparency, ensure that users have access to diverse viewpoints, and provide for processes for prompt notification to users of the reasons for removal or other processing of content, as well as recourse mechanisms that allow users to seek redress.

- Evaluate and address the impact of AI systems on labor markets and their consequences on the educational needs of each country.
- Promote and support the efforts of other actors to adapt training programmes and strategies to the future implications of work and the needs of industry, including small and medium-sized enterprises, and to launch professional development and retraining programmes, and explore social protection programmes for those who cannot retrain.

- Take 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 during their life cycle.

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

This background emerges from the Interim Report: Governing AI for Humanity prepared by the United Nations Advisory Body on Artificial Intelligence, published in December from 2023[118]The body was created that same year at the request of the Secretary-General, in order to address the risks, opportunities and international governance of AI and is made up of independent experts.[119].

The advisory body's report outlines a set of opportunities and risks involved in AI systems and analyses that the global governance deficit means that benefits and risks are unequally distributed around the world. It highlights 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 international global governance of AI based on five guiding principles summarized below.

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

Principle	**Scope**
AI must be governed inclusively, by and for the benefit of all.	The report argues that AI should be governed in such a way that all people and all countries, regardless of their level of development, can benefit from it.
AI must be governed by the public interest.	The report argues that binding rules are needed that are consistently applied by the

---

[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 complete list of members is available at the following link:https://www.un.org/en/ai-advisorybody/members Last accessed: 29/4/2024.

	Member States to ensure that public interests prevail.
AI governance must be built from jointly with data governance and the promotion of common data.	The report raises the need to consider how data is collected, stored and shared, to ensure that data is shared and used in a way that benefits society as a whole.
AI governance must be universal, networked, and rooted in adaptive collaboration between multiple parties interested.	The report highlights that any AI governance effort must prioritise universal support from different Member States and stakeholders and inclusive participation from the Global South, taking into account different cultural contexts.
AI governance must be based on standards and commitments international.	The report argues that AI governance should be based on the United Nations Charter, international human rights law, and other agreed international commitments such as the Sustainable Development Goals.

It has been announced that the final report of the Advisory Body would be presented in mid-2024, and that it would be a fundamental input for the definition of the specific commitments and actions on Artificial Intelligence that the Member States will assume within the framework of the Global Digital Pact in September.

2024. Uruguay has participated in the consultation sessions promoted by the Advisory Body on AI and is participating in the ongoing negotiation of the Global Digital Pact.

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

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

The Resolution covers “non-military artificial intelligence systems whose life cycle includes the stages of pre-design, design, development, evaluation, testing, deployment, use, sale, acquisition, exploitation and decommissioning.”

The text defines the characteristics that distinguish safe and reliable AI systems in the following terms: “(...) they are human-centered, reliable, explainable, ethical and inclusive, fully respect the promotion and protection of human rights and international law, maintain privacy, are oriented towards sustainable development and are responsible.”[121].

The Resolution states that[122]“human rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle 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 accordance 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 21 March 2024. 78/265. Harnessing the opportunities of safe and trusted 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. Considerations.

[122] Ibid. Point 5.

The UN resolution encourages Member States to promote safe and reliable 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 innovation and investment in artificial intelligence, while promoting safe and trustworthy AI systems[123].

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

- Encouraging the development and deployment of effective, accessible, adaptable and internationally interoperable technical tools, standards or practices, including trusted content and origin authentication mechanisms, such as watermarks or tagging, where technically feasible or appropriate, that enable users to identify instances of information manipulation, distinguish or determine the origin of authentic digital content from artificial intelligence-generated or manipulated content, and increasing media and information literacy[125].

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

---

[123] Ibid. Point 6. Literal a)

[124] Ibid. Point 6. Literal e)

[125] Ibid. Point 6. Literal g).

biased throughout the life cycle of artificial intelligence systems[126].

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

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

- Strengthening investment in the development and implementation of effective safeguards, including risk and impact assessments, throughout the entire life cycle of artificial intelligence systems to protect the full and effective enjoyment of human rights and fundamental freedoms and mitigate the potential impact on it[129].

---

[126] Ibid. Point 6. Literal h).

[127] Ibid. Point 6. Literal i).

[128] Ibid. Point 6. Literal k).

[129] Ibid. Point 6. Literal l).

Other intergovernmental processes

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

OECD Recommendation on Artificial Intelligence (2019)

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

The principles seek to facilitate the interoperability of global policies and advocate for AI that is innovative and trustworthy, and that protects human rights and democratic values. In 2024, Uruguay formally requested to join 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 states that interested parties [131]They must proactively participate in responsible management of AI for the benefit of people and the planet, promoting growth

---

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

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

	inclusive, well-being, sustainable development and environmental sustainability.
Respect for the rule of law, human rights human and democratic values, including fairness and privacy.	The Recommendation maintains that AI actors[132] They must respect the rule of law, human rights and democratic values throughout the lifecycle of the AI system, including implementing mechanisms and safeguards to address risks arising from uses other than 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 under applicable international law.
Transparency and explainability	The Recommendation underlines that AI actors should commit to transparency and responsible disclosure of AI systems by providing meaningful, contextually appropriate and state-of-the-art information. Such information should enable a general understanding of AI systems, including their capabilities and limitations, knowledge when interacting with AI systems, and where feasible and useful, simple and easy-to-understand 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 allow the outcome to be understood and, if necessary, to question its outcome for those negatively affected by the outcome.
Robustness, safety and protection	The Recommendation states that AI systems should be robust, secure and protected throughout their life cycle, such that under any conditions of use they do not pose unreasonable security risks. Where technically feasible, to strengthen the integrity of information while ensuring respect for freedom of expression.
Responsibility	The Recommendation states that AI actors should be responsible for the proper functioning of AI systems and for respecting the above principles. To this end, they should ensure traceability, including in relation to data sets, processes and decisions taken during the AI system lifecycle and apply a systematic risk management approach to each phase of the AI system lifecycle on an ongoing basis and adopt responsible business conduct to address risks related to AI systems.

G20 Artificial Intelligence Principles (2019)

In 2019, through a resolution, the Group of Twenty (G20) expressed its support for the OECD Principles and took note of their recommendations.[133]The resolution reproduces the aforementioned principles already discussed in the previous 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 Organisations Developing Advanced AI Systems, adopted by the G7, called the Hiroshima Principles.[134]Its adoption took place in 2023 within the framework of the Hiroshima Process[135]and seek to address recent developments in the most advanced AI systems, including generative AI, by offering guidance for organizations developing and using 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 in:https://digitalstrategy.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 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 in support of the development of responsible AI tools and best practices (Cf. (https://digital-strategy.ec.europa.eu/en/library/g7-leadersstatement-hiroshima-ai-process),

Hiroshima Principles

Principle	**Scope**
Identifying, assessing and mitigating risks throughout the AI lifecycle.	Appropriate measures should be taken throughout the development of advanced AI systems, including before and during their deployment, to identify, assess and mitigate existing risks throughout the AI life cycle.
Identification and mitigation of vulnerabilities and, where appropriate, of incidents and misuse.	Vulnerabilities, incidents, emerging risks and misuse should be monitored post-implementation and appropriate action taken to address them. Mechanisms for reporting vulnerabilities, where appropriate, should be accessible to a diverse set of stakeholders.
Transparency.	The aim is to provide clear and precise information on the capabilities, limitations and areas of appropriate and inappropriate use of advanced AI systems to the public in order to help ensure sufficient transparency and increase accountability.
Exchange of information.	The aim is to work towards a responsible exchange of information and notification of incidents between organisations that develop advanced systems, including industry, governments, civil society and academia.

AI governance and risk management policies.	It is proposed to develop, implement and disclose AI governance and risk management policies, based 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	It is planned to invest in and implement robust security controls, including physical security, cybersecurity and protection against internal threats throughout the AI lifecycle.
Mechanisms of authentication of contents	We plan to develop and implement reliable authentication and content provenance mechanisms, where technically feasible, such as watermarks or other techniques to allow users to identify AI-generated content.
Research to mitigate social and security risks and investment in mitigation measures effective.	It aims to conduct, collaborate and invest in research that supports the advancement of AI safety and trust, and to address key risks, as well as invest in the development of appropriate mitigation tools.
Develop systems advanced AI focused on people and global challenges and supporting the achievement of the SDGs.	The development of advanced AI systems is planned to be prioritized to address the world's greatest challenges, including but not limited to the climate crisis, global health, and education. Support progress on the United Nations Sustainable Development Goals. Organizations should prioritize responsible management of trustworthy AI and

	human-centered and also support digital literacy initiatives.
Development and adoption of standards and norms international techniques relating to AI.	It is intended to contribute to the development and, where appropriate, use of international technical standards and best practices, including watermarks, and to work with standards development organisations.
Implementation of measures for the protection of personal data and intellectual property	Implement appropriate data entry 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 data sets and the use of data. 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]The Convention was formally adopted by the Committee of Ministers of the Council of Europe (COE) in May 2024 and will be opened for signature by Member States and non-Member States of the Council in September. The text of the Convention was negotiated within the framework of the Committee on Artificial Intelligence of the COE in a process that extended from 2021 to March 2024. In October 2023, Uruguay joined the Committee as an observer, a status that enables non-Member States to adhere to the treaty.

---

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

In the case of this precedent, it is a legally binding instrument for the States that sign and ratify it.

The Framework Convention aims to ensure that activities within the life cycle 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 AI lifecycle activities in both the public and private sectors, establishing nuances regarding the scope of States' obligations with respect to the private sector in the context of the Convention.

The Explanatory Report accompanying the Treaty argues that the Treaty ensures that each Party's existing applicable obligations on human rights, democracy and the rule of law also apply to activities within 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 is intended to create new human rights or human rights obligations or to undermine the scope and content of existing applicable protections, but rather, by establishing various legally binding obligations contained in its Chapters II to VI, to facilitate the effective implementation of each Party's applicable human rights obligations in the context of the new challenges posed by artificial intelligence.[137].

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

---

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

It does not merely recognize those risks, but requires the adoption or maintenance of appropriate legislative, administrative or other measures to give effect to this provision, as well as cooperation among Parties as provided for in the provisions on the monitoring mechanism and international cooperation. It clarifies, however, that the obligation does not necessarily require additional legislation, and Parties may make use of other appropriate measures, including administrative and voluntary measures. So, while the obligation is binding and all Parties must comply with it, the nature of the measures adopted by Parties could vary.[138].

Activities within the life cycle of artificial intelligence systems related to the protection of their national security interests are excepted from the scope of the Convention. The Explanatory Report specifies that this exception applies only if and to the extent that the activities relate to the protection of national security interests, such that all regular law enforcement activities for the prevention, detection, investigation and prosecution of crimes, including threats to public security, also remain within the scope of the Framework Convention as long as the national security interests of the Parties are not at stake.

The Framework Convention consists of 36 articles and 8 chapters.

Chapter II sets out the general obligations of States Parties to: adopt or maintain measures to ensure that activities within the life cycle of artificial intelligence systems are consistent with the obligations to protect human rights, as enshrined in applicable international law and in their domestic law (Article 4) and to adopt or maintain measures that seek to guarantee the integrity, independence and effectiveness of democratic institutions and processes (Article 5). While Chapter III stipulates the common principles that will guide the implementation of the Convention.

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

---

[138] Ibid. Para. 29.

artificial intelligence systems, adopting or maintaining, consistent with such frameworks, measures to ensure the availability of accessible and effective remedies for human rights violations resulting from activities within the life cycle of artificial intelligence systems (Article 14).

The Convention also states that States Parties must adopt or maintain ex ante measures and, as appropriate, iteratively throughout the life cycle of the artificial intelligence system, for the identification, assessment, prevention and mitigation of risks, considering the actual and potential impacts on human rights, democracy and the rule of law. It indicates that such measures must be gradual and differentiated, appropriate to the context and use.

In this regard, the Explanatory Report specifies that this provision grants flexibility to the Parties in the approaches and methodologies for carrying out the assessment. It notes that “in particular, the Parties may choose to implement this assessment at different levels, such as at the regulatory level, prescribing different risk classification categories and/or at the operational level by relevant actors assigned responsibilities for activities within the life cycle of the artificial intelligence system. Likewise, each Party shall assess the need for a moratorium, ban or other appropriate measures with respect to certain uses of artificial intelligence systems when it considers that such uses are 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

	related to activities within the life cycle of artificial intelligence systems.
Transparency and supervision	Adopt or maintain measures to ensure that appropriate transparency and oversight requirements are in place tailored to the specific contexts and risks with respect to activities within the lifecycle of AI systems, including with respect to the identification of content generated by AI systems.
Accountability and responsibility	Adopt or maintain measures to ensure 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 not discrimination	Adopt or maintain measures to ensure that activities related to the life cycle 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 protection of personal data	Adopt or maintain measures to ensure the protection of individuals' privacy and personal data within the lifecycle of AI systems, including through national and international laws, standards and frameworks, and establish effective safeguards and guarantees for individuals.

Reliability	Take measures to promote the trustworthiness of AI systems, which could include requirements related to adequate quality and safety throughout the lifecycle of AI systems.
Safe innovation	Establish, where appropriate, controlled environments to develop, experiment 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 within the framework of the Eighth Ministerial Conference on the Information Society in Latin America and the Caribbean, which took place from 16 to 18 November 2022 and was jointly organized by the Economic Commission for Latin America and the Caribbean (ECLAC) and the Government of Uruguay. It sets out a set of policy priorities and strategic actions at the regional level along four axes.

Axis 3 of the instrument addresses productive and sustainable digital transformation and establishes as one of the objectives of the regional agenda the "promotion of the effective use of emerging digital technologies to promote productivity, foster innovation and entrepreneurship, especially providing for solutions for the Internet of Things, artificial intelligence and environmentally friendly technologies."

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

Working groups have been established to implement the Agenda's objectives. Working groups are a space for cooperation within the framework of eLAC2024, with the aim of achieving a specific goal under the leadership of a coordinating country.

The Artificial Intelligence Working Group is one of the groups established for the period 2023-2024 under the coordination of the National Center for Artificial Intelligence of Chile and the Agency for Electronic Government and Information and Knowledge Society of Uruguay (AGESIC).

Santiago Declaration (2023)

The Santiago Declaration to "Promote Ethical Artificial Intelligence in Latin America and the Caribbean"[140]It was adopted in October 2023 by the participating governments – including the Government of Uruguay – within the framework of the Forum on the Ethics of Artificial Intelligence in Latin America and the Caribbean, and the Ministerial and High-Level Summit of Latin America and the Caribbean, organized by UNESCO, CAF and the Government of Chile.

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

Through this instrument, the signatory countries agreed to "initiate an analysis of the need to develop and adopt new legal frameworks and regulatory agendas for the design, development and responsible 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 5/15/2024.

[140] Available in: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, in particular the principles of proportionality and safety, security and protection, equity and non-discrimination, inclusion, gender diversity, cultural diversity, accessibility, sustainability – social, cultural, economic and environmental –, the right to privacy and protection of personal data, human oversight and decision-making, transparency and explainability, responsibility and accountability, awareness-raising and education, and smart governance and adaptive and multi-stakeholder collaboration."[141]

The Declaration argues that it is urgent to integrate the particularities of the cultures of Latin America and the Caribbean in the creation of AI technologies for the region and states that it is essential to encourage greater investments in the region to take full advantage of AI to solve its various problems, and to promote the innovative use of this technology, developing the necessary incentives for this purpose.

Recent regulations in the United States and the European Union

United States Executive Order 2023

In October 2023, the United States government issued an Executive Order for the Safe and Secure Development and Use of Artificial Intelligence[142], which explicitly states the purpose of promoting an "approach that addresses the risks of AI without unduly reducing its benefits"[143].

---

[141] Ministerial and High-Level Summit of Latin America and the Caribbean (2023). Santiago Declaration, "To promote ethical artificial intelligence in Latin America and the Caribbean", resolution point 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 content of the Executive Order can be consulted at:https://www.whitehouse.gov/briefing-room/presidentialactions/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, literal (a).

The regulation directs federal entities to take multiple steps to establish safeguards around artificial intelligence technologies and imposes new rules for certain AI system developers. The Executive Order sets forth eight guiding principles and priorities for artificial intelligence policy, which are 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 the risks of these systems before putting them into use.
2. Responsible innovation and competition: The Executive Order promotes a set of measures to attract talent to the country, investments in education, training, development, research and capacity related to AI, the need to address intellectual property (IP) issues to protect inventors and creators.

3. Support for workers: The Executive Order analyzes that it is necessary to adapt labor training and education to support a diverse workforce and help facilitate access to the opportunities created by AI, and address that AI is not deployed in a way that undermines workers' rights.
4. Equity and protection of civil rights: The Executive Order states that Artificial Intelligence policies must be consistent with policies promoting equity and civil rights.
5. Consumer Protection: The Executive Order calls for protecting the interests of consumers who interact with AI systems, particularly in critical areas, while promoting the responsible use of AI.

6. Privacy: The Executive Order raises the need to protect privacy as AI continues to advance.
7. Manage the risks of federal entities' use of AI: The Executive Order seeks to increase internal capacity to regulate, govern, and support the responsible use of AI to deliver better outcomes.
8. International Leadership and Cooperation: The Executive Order proposes that the United States should be a global leader in AI and a pioneer in the systems and safeguards necessary to deploy the technology responsibly, and proposes to lead

regulatory efforts aimed at establishing common frameworks for assurance and risk management, and promoting global technical standards for AI.

The specific measures provided for by the Executive Order to achieve the aforementioned objectives include:

1. Safety Standards.
   - Require developers of certain systems to share information with the U.S. government.
   - Develop standards, tools and tests to ensure that systems are secure and reliable before being put into production.
   - Protection against the risks of using AI on hazardous biological materials.
   - Protection from AI-enabled fraud and deception. Content authentication guidelines and watermarks will be developed to identify AI-generated content.
   - Establish an advanced cybersecurity program to develop AI tools and collaborate on the detection and resolution of vulnerabilities in critical software.
   - Order the development of a National Security Memorandum to guide future actions on AI and security.
2. Protection of privacy.
   - Prioritize federal support to accelerate the development of privacy-preserving technologies.
   - Strengthen research and technologies that preserve privacy.

- Evaluate how agencies collect and use available information and strengthen privacy guidance for federal agencies.

- Develop guidance for federal agencies to evaluate the effectiveness of privacy-preserving techniques.

3. Advance civil rights and equity

- Provide guidance for landlords, federal benefit programs, and federal contractors to avoid the use of discriminatory algorithms.
- Addressing algorithmic discrimination through technical assistance, coordination, and best practices.
- Ensuring equity in the criminal justice system

4. Protect consumers, patients and students.

- Advancing responsible use of AI in healthcare
- Design resources that support the transformation of education through AI tools.

5. Support for workers.

- Develop principles and best practices to mitigate the harms and maximize the benefits of AI for workers
- Prepare a report on the potential impact of AI 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.

- Utilize existing authorities to expand the skills of highly specialized immigrants and nonimmigrants with expertise in areas critical to studying, remaining, and working in the United States.

7. Advance U.S. Leadership Abroad

- Expand bilateral, multilateral, and multi-stakeholder engagements to collaborate on AI.

- Accelerating the development and implementation of vital AI standards

- Promote safe, responsible and rights-centered development and implementation abroad to solve global challenges.

8. Ensure responsible and effective government use of AI.

- Establish guidelines for the use of AI by government offices.

- Support government agencies in the acquisition of AI products and services.

- Accelerate rapid hiring of AI professionals in government.

European Union Artificial Intelligence Act

The European Regulation on Artificial Intelligence[144]It was approved by the countries of the European Union on March 13, 2024. In accordance with the provisions

---

[144] **Artificial Intelligence Regulation, March 13, 2024. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.html**

Article 1 aims to protect fundamental rights, democracy, the rule of law and environmental sustainability against high-risk AI while promoting innovation.

The European Union instrument adopts a risk-based approach, establishing prohibited applications and high-risk systems for which it regulates a set of requirements and obligations:

a) Unacceptable risk (Title II).

The following prohibited applications are included in this classification:

- Cognitive manipulation of people's behavior that affects their autonomy and ability to choose freely or exploit the vulnerabilities of people derived from their age, disability, among others. The ban does not affect legal practices related to medical treatments[145].
- Biometric categorization systems based on biometric data[146].
- AI systems that allow public or private agents to carry out a citizen score of natural persons based on several data points related to their social behavior in multiple contexts or personal or personality characteristics known, inferred or predicted during certain periods of time[147].

- Use of AI systems for remote "real-time" biometric identification of natural persons in public spaces for law enforcement purposes (exceptions established)[148].

b) High-risk AI systems (Title III).

Those whose output is relevant to an action or decision with a possible significant risk to the company are placed under this classification.

---

[145] Paragraph 29.

[146] Paragraph 30.

[147] Paragraph 31.

[148] Paragraphs 32 and 33.

health, safety or fundamental rights of persons. The regulation indicates that the classification must be made taking into account both the seriousness of the potential harm and the likelihood of it occurring. It provides that the commissioning or use of high-risk AI systems must be subject to compliance with certain mandatory requirements.

Among others, the following are included in this classification:

- Several use cases of biometric identification systems.
- AI systems intended to be used as security components in the management and operation of critical infrastructures.

- AI systems used in education or vocational training.

- AI systems used in the fields of employment, workforce management, particularly for recruitment and staff selection.

- AI systems are used to assess the credit rating or solvency of individuals, as they decide whether such 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 for the administration of justice.
- AI implementations of products or product safety components already covered by European legislation (such as medical devices, railways, aircraft or machinery).

The Regulation defines a number of supervisory authorities. It also sets out a number of requirements that high-risk system providers must comply with. Among these, Article 9 states that a risk management system shall be established, implemented, documented and maintained. It also states that:

It establishes that, where appropriate, providers must ensure that natural persons are informed that they are interacting with an AI system.

Annex 3: Contributions received in the consultation process

Institución Nacional
de Derechos Humanos
y Defensoría del Pueblo

Montevideo, June 11, 2024.

Ref. Report on the application of article 74 of Law No. 20,212

Yo. Background

In accordance with the provisions of article 74 of Law No. 20,212, of 6 November 2023, AGESIC is entrusted with the design and development of a strategy national data and artificial intelligence based on international standards, in the public and private spheres. Within this framework and as part of this strategy, the established a period of 180 days for the presentation to the Legislative Branch of a report and recommendations for its legal regulation, aimed at its ethical development, the protection of human rights and, at the same time, the promotion of technological innovation. To this end, the aforementioned regulation provides that AGESIC may Establish working groups, advisory committees and other participation mechanisms that include the perspectives of actors from the public sector, the private sector, the academia and organized civil society.

On April 30, 2024, AGESIC prepared the Bases document for the development of the report provided for in art. 74 of Law No. 20,212, participating in various public entities, including the National Human Rights Institution and the Ombudsman's Office.

Within this framework, the INDDHH will make the following contributions to the document: issue, within the framework of its institutional duties and powers of defence, promotion and protection of human rights and, with the aim of contributing to the question and answer the questions raised in the report as elements of contribution to participating entities.

This does not imply an analysis of all the points referred to in the extensive report that has been noted, but some issues that the Board of Directors of the INDDHH considers it more relevant to refer, without prejudice to the significance of all aspects referred to in the document and the possibility of, in future instances, address other issues not addressed herein.

ii. On institutionality and governance

According to the document submitted, one of the first aspects to be analyze is related to the institutionality and governance of AI and, in particular, the question to the organic institutional position of the governing entity in the matter.

In this regard, the case of AGESIC itself, created in 1999, is cited as an example. by virtue of Law No. 17,930 as a decentralized body of the Presidency of the Republic and, subsequently, Law No. 18,331, which created the Regulatory and Control Unit Control of Personal Data (URCDP) as a decentralized entity of AGESIC, always within the scope of the Presidency of the Republic.

Examples of comparative law are also established, both in Latin America as in Europe, verifying the existence of autonomous entities (which in our law would be translated into what the constituent considered as Autonomous Entities or Decentralized Services) and entities dependent on Ministries, functioning as a sort of technical secretariats, in a sort of mechanism similar to the one existing in our country (with the exception that in our country case the link is with the Presidency). Finally, it refers to the point to which European Regulation, the North American case and the current regulation in the United Kingdom.

Regarding the point and in consideration of the provisions of Law No. 20,212, by which AGESIC and the URCDP are responsible for establishing general criteria on the subject matter (which even includes the subject matter of oversight), it is considered that its The scope of action should ideally be located outside the orbit of the Presidency of the Republic (leaving aside doctrinal discussions in the subject on the role of the Presidency in the key of our Constitution and the enormous expansion in themes and tasks that this organic system has had) and, in general, of the Executive Branch itself, given that the latter, in fact, is the system that produces and uses the most information and data in our country.

Taking into account the importance that management has every day data, information and AI, the ideal should be the existence of a data entity completely autonomous control, as in our country the Constitution recognizes The three supervisory bodies, which are also endowed with autonomous regulatory powers, as is especially the case with the Court of Auditors and the Electoral Court.

This scenario is not feasible, considering that it implies a reform constitutional, two possible institutional paths are proposed for the eventual institutionalization.

Firstly, one option is the location of this agency within the field of action of the Legislative Branch, as an autonomous entity and independent, as is the case with the INDDHH, created by Law No. 18,446. The case of the Parliamentary Commissioner for the Prison System although also It belongs to the orbit of the legislature, it has a role of direct accountability to parliament, which does not happen with the INDDHH and which should not happen in the case of a agency as indicated in the field of AI. As a strength of this point without a doubt There is the representative role that the legislative framework has and, In particular, the clear separation of the action with respect to the Executive Branch, with the particularities mentioned above.

The second feasible option with strong precedents in our law, It would be the possibility of following the path of other control entities such as URSEC, URSEA and JUTEP, which have recently (in institutional terms) been transformed into what in comparative law is called self-sufficient entities and adopted -in all three cases- the form of decentralized services, although They could also eventually take the form of Autonomous Entities, given that are not limited by art. 186 of the Constitution, as is the case with the control role held by the BCU.

The Decentralized Service form, which, as indicated, seems to be the path adopted for the control entities, attentive to the specificity of their tasks and the correct application of the principles of specialty and specialization for public bodies and, in particular, this type of entities, removing them from the hierarchical orbit of action of the Executive Branch (or the Presidency of the Republic) and even adopting a form of hierarchical designation that exceeds the five-year terms of government.

Without prejudice, naturally the control of the system will continue to exist, attentive to the characteristics of the way decentralized services operate and the aspects relating to administrative protection, functional status and provision budgetary within the framework of art. 220 of the Constitution. This last point, however, doubt poses one of the most substantive challenges, since the budget allocation chord, as recognized in the report, is essential for the correct performance of this type of control agencies.

iii. Another aspect highlighted in the report is related to the example of data trusts. While clearly the figure of the trust - collected

In our country, Law No. 17,703- is oriented to the subject of property and finance (be it whether it is testamentary, administrative, guarantee and financial trusts), application to the field of data seems clearly innovative.

Taking into consideration examples of comparative law - especially the figure of the trust of Anglo-Saxon law - and the substantive bases of the figure of the trust, that is, especially, the existence of trustors, trustee and beneficiaries and, on the other hand, a series of assets or rights in trust and a mandate, it is essential that a regulation that makes this type of instruments viable must have a legal normative basis, in order to protect the rights of the data holders and regulate the roles of each of the parties, especially the trustee, which should preferably be a state entity (for example, the (control agency).

Hand in hand with this, there are an important set of regulatory aspects and control that must be clearly established by law, in particular the powers of action of that trustee with respect to the data they handle and the potential beneficiaries of this collected data.

In this context, the trust option, although not ruled out, doubt involves an extensive regulatory development that allows guaranteeing the security of information and the proper protection of people's rights.

iv. (.....)

Contributions from Data Uruguay for the development of 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 from your experience to promote the lines defined in this document?

At Data Uruguay, we analyze the document “Bases for the development of the report provided for in art. 74 of Law No. 20,212” and highlight the importance of adapting national regulations to regulate artificial intelligence (AI) in Uruguay according to the most recent international human rights standards.

We highlight the importance of Agesic's work in establishing ethical frameworks and soft law standards through the AI Strategy for the public sphere, although we understand that this task must be complemented by updating national regulations. The aspects that require more urgent regulation are related to automated decision-making through artificial intelligence systems, especially in public administration. These situations not only include fully automated decision-making but also include human-machine interaction and the concept of meaningful supervision (when operators act while being aware of the biases or limitations of the system).

In order to promote the lines defined in this document, we understand that, after this consultation, the Uruguayan Parliament should consider holding a public hearing in which our legislators can interact with companies, academia and specialized civil society, since legislation is currently being passed on these issues based on very superficial understandings of some of the challenges of regulating this issue and its consequences.

We suggest a list of possible aspects to discuss in the proposed public hearings on AI regulation, including:

- The determination of which uses pose a high risk of violating individual rights that would merit specific regulation.
- The establishment of basic guarantees 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.
- The mandatory application of risk assessment tools in certain critical scenarios that do not involve the use of personal data or where personal data protection obligations do not apply (such as in public safety or defence).
- Mandatory labelling of synthetic contents.
- Conceptualizing the principle of meaningful human supervision.

Finally, we understand that, although the National Institution for Human Rights and the Ombudsman's Office is the body mandated to make recommendations and public policy guidelines on human rights to Parliament, the members of this Institution do not have a critical mass of knowledge sufficient to be able to fulfill this recommendation function on AI. Therefore, it would be desirable to suggest some type of support to the INDDHH to establish agreements with academia and civil society specialized in digital rights.

2. Are there deficiencies or inconsistencies from a regulatory perspective that impact the aspects evaluated in the lines defined in this document and have not been considered?

In relation to the analysis developed around articles 13 and 16 of the Personal Data Protection Act in point “3.3 Preliminary diagnosis on AI and Human Rights of the document”, we highlight the importance of the right to challenge automated decisions and to obtain information on “the assessment criteria, the processes applied and the technological solution or program used”. In any case, this regulation is insufficient and it is necessary to update it to include modern standards such as, for example, the standards on algorithmic transparency[1]and significant human oversight[2]These same standards could also be included through obligations imposed on the public administration through amendments to the Law on Access to Public Information.

3. Have you identified potential improvements or modifications to current regulations that could contribute to the development of AI in Uruguay?

Reform of Law No. 19,179 on open formats and free software and its regulatory decree (Decree No. 44/015)

Following the same logic of updating the existing regulations proposed by Agesic in the draft document, it is suggested to implement a support system for decision-making regarding the acquisition of software or AI-based solutions by the public administration by introducing modifications to Law No. 19,179 on open formats and free software and its regulatory decree (Decree No. 44/015). This law is an instrument that already exists in our legal system since before the rise of AI and that could be revised to give priority to Open AI solutions, avoiding black boxes and promoting guarantees of transparency and explainability. We understand that, in addition to reviewing Law No. 19,179 and its decree to promote the preferential promotion of the use of Open AI models, an intervention mechanism should also be included by which Agesic determines the risk and advises public entities to carry out impact assessments prior to the acquisition of AI-based solutions, at least for some key sectors or uses (health, public safety or education, for example).

4. Are there other aspects that you do not find considered and that should be analyzed?

Urgent regulation of the acquisition and use of surveillance software by the Ministry of the Interior

A search of the press is enough to confirm that, in recent years, the Ministry of the Interior has been steadily acquiring new technologies to combat crime. Many of these acquisitions use powerful AI systems, whether to detect gunshots or to detect theft.

---

[1] IDB (2022), “Algorithmic auditing for decision-making or support systems”. See: https://publications.iadb.org/publications/spanish/document/Algorithmic-audit-for-decision-making-or-support-systems.pdf

[2] EU AI Act. See:https://www.euaiact.com/key-issue/4

placing microphones in public spaces to identify people based on biometric patterns. None of these technologies are properly regulated by law under the standards demanded by the different Rapporteurs of the international human rights system.

The UN Human Rights Committee's approach to surveillance measures is that governments may take such measures on their citizens provided that 1) they are authorized by a national law that is accessible and precise, 2) they have a legitimate objective, and 3) they meet the criteria of necessity and proportionality. The UN High Commissioner for Human Rights warned 10 years ago that these requirements were not being met.[3], and that States often use surveillance systems without adequate national laws, due process and sufficient oversight. The High Commissioner notes “the worrying lack of government 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 understand that the report that Agesic will present to Parliament should recommend that the Ministry of the Interior regulate the use of AI for surveillance purposes as a matter of urgency.

---

[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 the development of the report provided for in art. 74 of the Law No. 20,212

Document prepared by Patricia Díaz Co-
coordinator of the Data and Society Laboratory | Datysoc

Preliminary questions

We make some suggestions related to the structure of the document:

- Since this will be a document of considerable length, we suggest generating an index with hyperlinks to improve its navigability and usability.

- We suggest placing a bullet point at the end of each line with a summary that specifically and clearly states the regulatory recommendations.

Authorization: The Agesic team is authorized to copy, adapt and/or incorporate any part of this document into the final version to be presented to Parliament, without the need for citation.

1. What are the specific recommendations you could make? from your experience to promote the lines defined in this document?

We express that, in general terms, we agree with the analysis proposed and with the prioritized aspects and with the general guidelines of the proposal presented in the draft "Bases for the development of the report provided for in art. 74 of Law No. 20,212". Although there is a central aspect that the document fails to address explicitly and clearly, it is a question that several legislators surely have in mind: Do we need a general regulation of AI or should we regulate certain uses of AI or its use in certain sectors?

We understand that the conditions for a general regulation based on the determination of different levels of risk, the assignment of differentiated obligations for each of these levels of risk and the creation of new specialized institutions for AI are not yet in place. It is necessary to better understand the panorama in order to regulate, which is why**We propose to recommend to parliamentarians the creation of a forum to promote the lines defined in this document, identify other priorities at the national level and formulate recommendations by different social actors for an adequate and sustainable regulation.**.

In parallel to this discussion,**We suggest focusing current regulatory efforts on updating the current national regulatory body and on regulating current uses of AI by the government that involve high risk.**.

In this way, and without ruling out the possible existence of other emerging issues, we highlight the police use of AI as a high-risk emerging issue that urgently requires regulation and we propose the creation of a new line: “*Linea uses AI for police surveillance purposes and as evidence in criminal proceedings*” (see question 4).

2. Are there deficiencies or inconsistencies from the point of view regulatory that impact the aspects evaluated in the lines defined in this document and have not been considered?

Below we present some aspects that have not been considered in the document and that we understand should be added:

Section “3. Human Rights Line”

We propose to add the following considerations in the section “**3.3 Preliminary diagnosis on AI and Human Rights**”:

Regarding Personal Data Protection Law 18331 (LPDP) and Decree 64/020.

We agree with the assessments in the draft document that Articles 13 and 16 of the LPDP should be reviewed. We believe that these provisions are not sufficient for the following reasons:

1) The right to challenge personal assessments based on automated data processing (Art. 16) only applies 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 from an AI system that analyses water and air pollution data in which the health of a group of citizens is deemed to be at risk.
2) Art. 16 only enables the challenge of decisions “**whose only foundation**is a treatment of personal data”. It is enough to “put a human in the middle” and say that the system “advises” but that the human makes the decision for the application of the article to fall. Faced with the well-known “automation biases”[1]Consideration should be given to including some provision defining the concept of “significant human supervision”

---

[1] Report “Towards meaningful oversight of automated decision-making systems” (2022).DigitalFutureSociety.Available at: https://digitalfuturesociety.com/en/report/towards-meaningful-oversight-of-automated-decision-making-systems/

including minimum required aspects such as the training of the 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 consider the protection of personal data as a collective right, so that, based on these provisions, no public or private institution can be required to account for basic parameters of explainability of its automated systems in the face of a potential risk to fundamental rights.

4) In Decree 64/020, the obliged subjects are not obliged to publish their impact assessments, they are only obliged to share them with the URCDP if the assessment reveals a potential and significant risk (Art. 7).

5) Arts. 13 and 16 of the LPDP do not specify the requirements for configuring explainability and do not require traceability or auditability, so this obligation is met when the administration itself presents explanations unilaterally.

6) Standards are needed to ensure a minimum level of**transparency, interpretability and algorithmic auditability**(Stoyanovich, Julia (2020)[2] understanding that:

- **Algorithmic transparency is not synonymous with releasing the source code** ,Releasing source code helps, but is sometimes unnecessary and often insufficient. In some cases, the requirement to release source code may be excessive or infringe rights.
- **Algorithmic transparency requires data transparency** , explainability can only be achieved in the context of data, the data used for training and testing, the data to be used for system implementation and validation (reference datasets), data on system performance and accuracy. Data transparency is necessary for all automated systems, not just for systems based on *Machine Learning*.

- **Data transparency is not synonymous with making all data public** , data should be released whenever possible; if this is not possible (for reasons of data protection, confidentiality, intellectual property, for example) it is also possible to: publish the selection or collection methodologies, use synthetic data sets, publish statistical summaries or samples, the data used for preprocessing, the origin of the data and information on its quality/representativeness and the known sources of bias identified.

---

[2] Stoyanovich, Julia (2020). TransFAT. Translating fairness, accountability, and transparency into datascience practice. Available at: https://pdfs.semanticscholar.org/061f/de41f92e6bd408b5722428bdcc8b2a7d0858.pdf

- **Actionable transparency requires interpretability or understandability** In short, it is about explaining the assumptions and effects of the system (not just the operating details) and involving the public - technical and non-technical.

On Law 18381 on Access to Public Information (LAIP).

The LAIP should include a provision introducing the**right to be informed about which decisions are made automatically or with the support of an automated system by the public administration**and how these systems work (taking into account what was expressed in the previous section in relation to algorithmic transparency, interpretability and auditability and the conceptualization of “significant human intervention”).

A provision should also be included guaranteeing the right to human and face-to-face interaction with public administration.

Section “4. Intellectual Property Line”

We propose to add the following considerations in the section “**4.1 Preliminary considerations**”:

> Currently, most AI development activities require the massive use of large volumes of data and often include the use of thousands of copyrighted images, audios, texts, etc. for the purposes of computational analysis or model training. These uses include the application of text and data mining techniques (such as crowding, scraping and parsing), the creation of technical or ephemeral copies for the purposes of model training, among others. Thus, in order to encourage innovation and generate a secure legal environment for local researchers and developers, it is necessary to include in copyright laws an exception that enables the use of works for the purposes of computational analysis. This exception should include as a restriction the condition that these uses do not compete with the normal exploitation of the works and that they do not unjustifiably harm the interests of the authors.
>
> Considering that software and databases are also protected by copyright and technological protection measures, it will be necessary to clearly regulate the relationships between copyright, trade secrets and the auditability of systems. The auditability of AI systems is of particular public interest both for reasons of cybersecurity and transparency and explainability, and often requires the violation of technological protection measures for access.

to systems, making test copies or reverse engineering activities.

We propose to add the following considerations in the section “**4.2 Selection of international backgrounds**”:

As regards exceptions to copyright for the purposes of computational analysis, the most recent precedent in the WIPO context is the report on “Challenges for research centres and the purposes of research in relation to copyright” (2023).[3]. This report was requested from Raquel Xalabarder by the Committee on Copyright and Related Rights (SCCR/WIPO) and in it the author states:

> *“The role of non-human (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 copyrighted works, from academic papers to music and press publications.*.” (our translation)

In that same report we find an Annex with examples of national regulations that contain this type of exceptions to copyright for research activities for computational analysis purposes that are already present in almost all legislation in the Global North.

Regarding exceptions to copyright and technological protection measures for the purposes of auditability of systems, we find the 2022 OECD Working Group report on Security in the Digital Economy[4]. This report states that “ *Copyright law may be infringed when the disclosed information contains parts of copyrighted software code. Such copyright protection could restrict the sharing of vulnerability information with the original vendor, making it difficult to implement Coordinated Vulnerability Dissemination (CVD) in many cases.*The document explains that the lack of updating of exceptions to copyright and technological protection measures entails legal risks for auditors and digital security researchers, and also states that these rules are used to threaten legal proceedings by the owners of the software that is intended to be investigated.

---

[3] Xalabarder, Raquel (2023). “The challenges of research centres and the purposes of research in relation to copyright”. Available in: https://www.wipo.int/meetings/es/doc_details.jsp?doc_id=621815

[4] OECD (2022). OECD Policy Framework on Digital Security. Available in: https://www.oecd.org/publications/oecd-policy-framework-on-digital-security-a69df866-en.htm

We propose to add the following considerations in the section "**4.3 Preliminary diagnosis in AI and Intellectual Property**":

> The Uruguayan Copyright Law (Law 9,739) does not provide exceptions to copyright (or to the regime of technological protection measures) that enable the correct development of computational analysis or audit activities, whether for security or explainability purposes. That is why it is necessary to include a new exception in Art. 45 of the Copyright Law (Law 9,739) that enables the use of works for computational analysis purposes. It is also suggested to add an exception to copyright (and to technological protection measures) to enable the access, copying and analysis of systems for the exclusive purpose of allowing auditability instances when a judge or other law so requires. These exceptions should explicitly state that competitive uses or uses that unjustifiably harm the author or owner of the rights to the works are strictly prohibited.

3. Have you identified potential improvements or modifications to the current regulations that can collaborate in the development of AI in Uruguay?

- - -

4. Are there other aspects that you do not find considered and that should be analyzed?

The inclusion of a new line is proposed below, which constitutes the largest **Emerging use of AI with high risk of violating fundamental rights in Uruguay**, so it should be analyzed independently and**urgently requires regulation** :

Linea uses AI for police surveillance purposes and as evidence in criminal proceedings.

Preliminary considerations:

The use of AI for crime prevention and public safety purposes puts citizens' rights at risk due to its potential for discrimination and because it is a highly intrusive technology, beyond the possible biases or failures that imply risks of discrimination. Some of the concerns

The main concerns regarding the use of these systems by the police and in criminal justice are:[5]:

The violation of the presumption of innocence. The right to the presumption of innocence in criminal proceedings is a fundamental human right. However, the increasing use of AI in the criminal justice field, and more particularly the use of remote biometric surveillance and certain types of predictive policing software, raises questions about the scope of this right and how AI systems should be built and used to protect it.

The preservation of procedural equality and due process. One of the main concerns raised in studies on certain AI systems is that they are inaccessible to proper scrutiny by defendants and their lawyers. This has serious implications for the principle of equal procedural rights and the right to an adversarial process, because without information on how a decision is made, it is difficult to foresee how defendants can challenge the correctness and legality of the decision. In this regard, one of the main problems preventing sufficient challengeability of AI systems in criminal proceedings is the lack of notification. If a person is not notified that they have been the subject of an automated decision by an AI system, they will not have the possibility to challenge that decision, or the information on which the decision was based. In turn, the phenomenon of black boxes is another risk factor in the application of AI since, in order to preserve due process and the right to procedural equality, the system and its results must necessarily be explainable and demonstrably free of bias.

The lack of mandatory training for actors in the judicial system: Training of those involved in the judicial system is essential to determine the admissibility and to make a correct assessment of digital evidence, as well as to give meaning to the concept of “significant human intervention” in the judicial context. Training is not only necessary for primary users of AI systems, such as judges and police officers who use them to base their own decisions. Training should also be available to criminal defence lawyers, so that they are better able to challenge AI systems, when necessary.

Selection of international backgrounds

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in his report “Surveillance and Human Rights” (2019)[6]proposes drastic measures. Urgently calls for

---

[5] Policy Paper: Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU (2022).FairTrials.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 monitoring and human rights”, A/HRC/41/35. (General Assembly)

establish "*an immediate moratorium on the global sale and transfer of tools used by the private surveillance sector until strict human rights safeguards are put in place to regulate such practices and it can be ensured that governments and non-state actors will use such tools in a legitimate manner*." and also requests "*Tighter regulation of exports of surveillance equipment and stricter restrictions on its use*".

In the "EU Artificial Intelligence Regulation" (Art. 5 of Chapter II "Prohibited Artificial Intelligence Practices")[7]**It is prohibited**the use of real-time biometric identification in places accessible to the public by law enforcement agencies for police or public order applications,**except**In these cases: searching for potential victims of crimes; preventing specific and substantial threats to critical infrastructure or to individuals; preventing terrorist attacks; and prosecuting crimes punishable by more than five years of imprisonment. It will first be mandatory to assess the probability and scale of the possible damage without these systems and the damage they could cause;**judicial authorization**or binding administrative; and temporal, geographical and personal limitations will be imposed.

Another important precedent is the "Resolution of the European Parliament of 6 October 2021 on artificial intelligence in criminal law and its use by police and judicial authorities in criminal matters"[8]. This The resolution addresses the use of artificial intelligence (AI) in the field of criminal law, focusing on its application by law enforcement and judicial authorities. The document underlines the need to establish a robust regulatory framework that guarantees respect for fundamental rights, privacy and data protection. Furthermore, it emphasises the importance of transparency, human oversight and accountability in the use of AI systems to prevent bias and discrimination. The resolution also calls for regular impact assessments and audits of these systems to ensure their compliance with EU ethical and legal standards.

In this Resolution, the European Parliament highlights the potential of AI to improve efficiency and effectiveness in the fight against crime, but also warns of the associated risks, such as the possibility of judicial errors and the

---

of the Nations United, 28 of May of 2019). Available in:. https://www.undocs.org/es/A/HRC/41/35

[7] European Union Artificial Intelligence Regulation approved by legislative resolution of the European Parliament, 13 March 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 law enforcement authorities and the judiciary in criminal matters (2020/2016(INI)). Available in: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

violation of human rights. The resolution proposes the creation of a specific legal framework for the use of AI in the criminal field, including clear guidelines on data collection and processing, as well as measures to ensure fairness and non-discrimination. It also recommends that authorities and legal professionals receive adequate training on the use and implications of AI, thus ensuring a fair and safe application of these technologies in the judicial system.

Preliminary diagnosis

The Ministry of the Interior has been building an automated surveillance ecosystem to support the fulfillment of its duties, based on both AI and other types of systems. This ecosystem has not been accompanied by proper regulation or proactive transparency criteria that provide confidence in its operation. There is no regulation related to the police use of the systems recently acquired by the Ministry of the Interior. For example, automated facial recognition, UCINET software (intelligence software on open sources such as social networks), the ShotSpotter system (a system that involves placing microphones on the streets so that an AI can detect gunshots) or even camera analytics software to "determine suspicious behavior that can warn the police before the crime occurs."

In Uruguay, the control of the use of personal databases used in the activities of "public security, defense, State security and its activities in criminal matters, investigation and repression of crime" are not covered by the obligations established by Law 18331 on the Protection of Personal Data (LPDP Art. 3 Lit. B and Art. 25)[9].

Regarding the Automated Facial Recognition (AFR) software that the Ministry of the Interior acquired in February 2020 via public tender, we highlight that this acquisition is related to the approval of the creation of a facial identification database for processing for public security purposes by the Secretariat of the Ministry of the Interior (arts. 191 and 192 of the 2020 Budget Law). In this way, the use of facial photographs (and information associated with them) from identity cards and passports in the database of the National Civil Identification Directorate (DNIC) is enabled to create a biometric database for a purpose other than identification. There are many issues that arise from this massive contracting and enabling for the use of facial identification.

---

[9] "However, it should be noted that, even in the cases indicated in the previous paragraph, the URCDP has interpreted that the principles of personal data protection are also generally applicable." See consultation to the URCDP Executive Council published in: Report "Out of Control. Police use of automated facial recognition in Uruguay". Datysoc (2022), p. 49.
Available in:
https://datysoc.org/wp-content/uploads/2022/03/Informe-recambio-facial-automatizado-Uruguay-2022-Datysoc.pdf

biometric data of the entire population For what exact purposes was the system contracted? Who authorizes the use of the RFA system? How will the use of the system be audited? How will access to the system be controlled? How should an officer proceed when faced with a biometric match in the different contexts of use? When can a biometric match be accepted as evidence? How will this evidence be assessed? How will the possibility of bias in the system be addressed? When and how will the accused be informed of the existence of this type of evidence? How will the differences between a biometric match in a controlled environment and one in an uncontrolled environment be addressed? How will this personal data be deleted when it is no longer needed? None of this has been defined yet and most of these decisions**They should be established through precise and publicly accessible legal regulations.**.

It is also worth noting that neither in the Code of Criminal Procedure nor in the Law of Police Procedure do we have any regulation on the admissibility or assessment of digital evidence, nor public protocols on the use of AI acquired by the Ministry of the Interior, nor training of judicial actors on the operation of this AI.

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 the acquisition of surveillance software until there is a legal basis that adequately regulates the police surveillance ecosystem.

In order to establish strict regulation on its use and provide guarantees against discriminatory acts and against its abusive or arbitrary use, the necessary modifications should be introduced in the Code of Criminal Procedure and in the Law of Police Procedure to regulate the issue appropriately, including:

- The obligation to carry out an impact analysis (if possible public) on fundamental rights before acquiring AI solutions for surveillance purposes, as well as knowing and declaring in advance the exact purposes for which the contract is being made.
- Establishing red lines as to which uses are strictly prohibited to the police and which uses require a court order,
- The possibility of requiring algorithmic auditability and explainability, traceability, access control protocols and the description of detailed responsibilities for those who use these surveillance systems.

- Adequate training of police officers, judges and prosecutors on the functioning and limitations of the system through mandatory certification.

Specific recommendations related to biometric surveillance and facial recognition:

- The prohibition of mass enrollment of the entire population in the facial recognition system acquired by the Ministry of the Interior. This implies the repeal of arts. 191 and 192 of the 2020 Budget Law, as these articles violate the principle of presumption of innocence.
- The prohibition of the use of 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 processing of biometric matches as investigation methods and as digital evidence.

CONTRIBUTION OF THE COMMISSION ON COMPUTER LAW AND TECHNOLOGICAL SECTOR OF THE URUGUAYAN NOTARIES ASSOCIATION.

Consultation: Basis for discussion of the contents of the report preliminary provided for in art. 74 of Law No. 20212 (AGESIC)

1. What specific recommendations could you make from your experience to promote the lines defined in this document?

As for governance, a primary definition should be whether it is It is necessary that the regulations be general or sectoral, given that there are sectors with a high institutional, social and economic sensitivity. In both cases and as it happens with the Artificial Intelligence Regulation of the European Union, it would be appropriate to approach it from the risks that could cause, as well as in the allocation and distribution of responsibilities for damages (given the multiplicity of actors that may participate) to ensure equitable reparations for people harmed.

It will be a challenge to resolve the issue of assigning responsibilities for the use of AI, in a system where it may not be based in Uruguay, but whose consequences will be borne in our country.

In judicial matters, we understand that it may be advisable to "use "White box" AI systems, which are based on techniques that serve to perform intelligent predictions, classifications and detections that present enormous benefits to the judicial task and the digital transformation of the organizations, without the risk of inexplicability of black boxes"[1]

The “PretorIA” system created by the Innovation and Artificial Intelligence Laboratory of the Faculty of Law of the University of Buenos Aires (UBA IALAB), a predictive system developed to be used by the Constitutional Court of Colombia, can be highly recommended

“PretorIA combines functionalities based on expert systems and techniques of *machine learning* (“white box machine learning”[2]

2. Are there deficiencies or inconsistencies from a regulatory point of view that impact the aspects evaluated in the lines defined in this document and have not been considered?

To be able to determine these criteria and through them put AI at the service of the citizen and achieving greater social well-being should be thought of as country, what are the limits that we are willing to set for the different AI developments and thus regulate them.

Establish the corresponding impact assessments of an AI development to minimize risks to human rights.

---

[1] Treatise on artificial intelligence and law : volume II / Juan Gustavo Corvalan... [et al.] ; directed by Juan Gustavo Corvalan. - 2nd ed. - Autonomous City of Buenos Aires : La Ley, 2023. Digital Book, Book "app" for Android Digital File: download and online ISBN 978-987-03-4642-5

[2] Cited work

These topics will be evaluated based on the recent EU AI Regulation

3. Have you identified potential improvements or modifications to current regulations that could contribute to the development of AI in Uruguay?

In section 3.3. “Preliminary diagnosis on AI and Human Rights”

“Humans”From the document put up for consultation, “7 aspects” stand out central, linked to the points mentioned by the High Commissioner for United Nations Human Rights Council, and detailed above...”

In this report we will focus on two of the questions raised there:

1.- What are the scopes of transparency and explainability to be guaranteed within the framework of the development of AI systems focused on the person?

Answering this question we say that although in our regulations in force, we could apply Law No. 18331 regarding data personal, using the principles of purpose and prior consent informed, given the impact that AI has on both its development and its application has on the person and society they should be reinforced in its definition and application. Prior informed consent should clearly establish the information that must be delivered to either the consumer of an AI service or who buys an AI product. (games for children, glasses, GPT chat) What is established by art. 9 of law No. 18331 is not sufficient.

This conclusion is reached due to the type of personal data that can be collected. to be used in AI training, which can be data biometric and sensitive data which can be breached at any time of its treatment. As for the principle of purpose, its most basic definition explicit and focused on AI development would help achieve greater transparency.

“We understand it is essential that a regulatory scheme” focuses on the human being and "considers the obligation of companies to explain where and how artificial intelligence technologies and techniques are used automated in its platforms, services and applications, likewise, the duty to prevent and ensure that AI equipment and systems reflect non-discriminatory attitudes and avoid bias”[3]

“In terms of scoring performed by AI, data cannot be considered personal data that are not part of the list of data for whose purpose they are does the study.

The result of the scoring must have all the principles of AI, to which effects of being properly explained by a human being to the person affected by it same

Synthetic data may not be used in notarial or contractual matters.

---

[3] Treatise on artificial intelligence and law : volume II / Juan Gustavo Corvalan... [et al.] ; directed by Juan Gustavo Corvalan. - 2nd ed. - Autonomous City of 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, dir. CDD 346.002

Privacy policies must specify whether synthetic data is used.

and how they are used"[4]

4. Are there other aspects that have not been considered and that should be analyzed?

A new technological gap will have to be foreseen, much deeper than the previous ones, where many people will be left on the side of the road with the danger of falling into vulnerable situations.

On the other hand, "adaptability and the acquisition of new skills always have been imperative in the changing world of law. However, in the digital age and artificial intelligence, these skills evolve and must adapt to the challenges and opportunities offered by new technologies

"An example of this is the*legal prompt engineering*, an emerging skill which refers to the ability to interact and communicate effectively with AI-based conversational agents, such as ChatGPT.

In that understanding, we will see that the*legal prompt engineering*It is a crucial skill that encompasses and enhances several aspects of legal practice In the digital age, not only in the search for information but also in the preparation of legal documents, the argumentation of cases effectively or the design of improved legal strategies through interaction accurate and effective with sophisticated conversational agents. This adaptation

---

[4] Ob.cited

Not only is it necessary, but it can offer great opportunities for

to emphasize the path of reconversion and optimize the course of legal practice and

“The development of intelligent justice in the machine age”[5]

Esc. Elisabeth Bouvier Villa
Esc. Javier Wortman

---

[5] Cited work

In this document we gather the contributions of the IA Advisory Group to present to the Legislative Branch provided for in art. 74 of Law No. 20,212 by Agesic.

The contributions are made by the Artificial Intelligence Advisory Group of the Uruguayan Chamber of Information Technology

Institutionality and Governance*(Ref. Chapter 2 of the document)*
The objective of this line is to determine the fundamental aspects to ensure adequate institutionalization of Artificial Intelligence in our country.
Comments
The document shows that the existing institutions are adequate to deal with the challenges posed. It is essential to have advisory groups with the participation of all the actors, which function on a regular basis.
The concept of working groups is clear, but they should have greater say in defining policies, which are articulated, managed and led by AGESIC. It would be good to give them greater significance and decision-making power than a working group. The role of the URDCDP is shared Agesic should promote the development of artificial intelligence systems, but it would not be appropriate for it to develop them. I also think it is appropriate to define criteria and mechanisms to monitor that the criteria are properly applied.
The path to incorporating AI as a central aspect for creating innovative solutions is a path that involves taking risks (like all innovation). When a solution is developed to provide a public service (and in many cases on sensitive topics), the impact of failure is greater, and this can lead to innovation being slowed down by not taking these risks. Mechanisms to resolve these types of “conflicts” must be incorporated into governance.
Seek to evaluate the solutions developed by the Uruguayan ecosystem, under international standards at the level of impact of the solution, data quality, etc. in such a way that the solutions that are evaluated locally under this standard can be "exported" to other countries where the same standard is used.

Human Rights*(Ref. Chapter 3 of the document)*
The objective of this line is to raise which risks cannot be ignored within the framework of the development of a public policy on Artificial Intelligence, and which should require - if deemed necessary - special measures, due to their impact on people's rights and which measures could be relevant in order to take advantage of AI systems for the benefit of people and their rights, identifying those of a normative order.
Comments

It is important to identify the cases to which it is being applied. Different sciences should be looked at to assess the impact on human rights. It would be advisable to set up a committee or working group specific to this topic and the implications it may have in the long term.

The risk classification approach, while appropriate, requires great caution so that it does not constitute a barrier to innovation and investment in AI. Definitions must be sufficiently precise to provide legal guarantees and sufficiently flexible to adapt to contexts.
For example: a facial recognition system for monitoring citizens is not the same as a facial recognition system for finding missing children.

As described in the Agesic paper, the current legal and institutional framework is already appropriate for handling most of the potential risks. Updates made to the personal data protection law already prevent some of the potential problems.

Intellectual property*(Ref. Chapter 4 of the document)*

The World Intellectual Property Organization (WIPO)27 points out that the concept of Intellectual Property refers to creations of the intellect, from works of art to inventions, computer programs, trademarks and other commercial signs.

NO COMMENTS.

Infrastructure and Cybersecurity

(Ref. Chapter 5 of the document)

The development of Artificial Intelligence depends on several factors. One of the most important is having an adequate infrastructure, with the State having a central role in this regard.

Comments

Infrastructure and technological architecture must accompany the country's strategy in AI policies. Processing algorithms and controlling them is key to generating capabilities at the country level and having the independence to promote this technology.

At the Infrastructure level, it is necessary to differentiate between the availability to provide services and others for research and Innovation.

It is important to delve into a country strategy on what things can be enabled to be taken to the cloud and use its algorithms and which cannot.
Finally, interoperability platforms are needed to improve data quality and thus system interoperability.

Line of work and training AI

(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 address emerging challenges.

Comments

In this field there are three large groups to train:

- Associated with reconversion, it is necessary to familiarize workers with these technologies so that they incorporate them into their work environments. This is required to have more competitive companies and industry.
- Personnel who will develop the models do not have to be from technical areas.
- Raise public awareness of the strengths that good use provides and the threats that can arise if misused.

Civil liability and consumer rights line

(Ref. Chapter 7 of the document)

The line raised at this point refers to two aspects that are well regulated by law, such as civil liability and consumer relations.

Comments

In a technology-producing country like Uruguay, where the impact of this industry on the economy is expected to grow, it is important to provide adequate protection to developers and manufacturers of AI applications. Liability must be associated with non-compliance with current legal regulations and with proven cases of negligence. Overregulation at this point can generate liabilities that impose a high barrier for entrepreneurs.

Line of measures to promote AI

(Ref. Chapter 8 of the document)

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

Comments

It is important to create spaces with public policies that promote the inclusion of this technology in industries that we want to promote at a national level. For example, agriculture.

Define policies and practices for the proper use of data and their training. Generate seals that validate companies that apply it. These seals can being recognized globally by improving the quality of the services provided by companies, on the other hand, citizens are given guarantees that good practices are applied.