LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 24, NO. 1(2026)

TOWARDS AN INTERNATIONAL REGULATION OF ETHICAL AND RESPONSIBLE ARTIFICIAL INTELLIGENCE

Ait-Ali Zaina[1], HALILALI Amina[2]

[1]Faculty of Law and Political Science, University of Blida2 (Algeria).
[2]Faculty of Law and Political Science, University of Blida2 (Algeria).

z.ait-ali@univ-blida2.dz[1]
a.abdelmouizhalilali@gmail.com[2]

Corresponding author email: z.ait-ali@univ-blida2.dz

Received: 16/06/2025 Accepted: 28/11/2025 Published: 02/01/2026

Abstract:
Safeguarding the fundamental rights of individuals is essential to ensure the protection of privacy and personal data when using artificial intelligence (AI). AI algorithms collect, store and analyse large amounts of personal data, which can lead to risks of discrimination due to biases built into the algorithms, as well as breaches of privacy and data protection. To ensure respect for fundamental rights, the use of AI must be guided by ethical principles and be subject to rigorous human control. Regulation that protects individual freedoms is essential if AI is to be deployed responsibly.

Keywords: Artificial intelligence, fundamental rights, ethics, privacy, protection.

Introduction :

The dazzling development of artificial intelligence (AI) is emerging as one of the major technological upheavals of the 21st[e] century, affecting societies on a global scale. Present in sectors as varied as health, transport, education, security and finance, this technology is transforming modes of social organisation, decision-making processes and relationships between citizens and institutions, well beyond national borders.

While its benefits are considerable - improving medical diagnosis, optimising urban mobility, modernising public services - AI also raises universal legal and ethical challenges. Its operation is based on the use of massive volumes of personal data, often collected without explicit consent or sufficient transparency. The algorithms used, which are sometimes opaque, can produce automated decisions with discriminatory effects, reproducing or even amplifying pre-existing social biases.

These mechanisms threaten fundamental rights recognised in many legal traditions : the right to privacy, data protection and equal treatment. Yet these rights are not just a matter for national or regional frameworks: they form the bedrock of democratic societies and are enshrined in international instruments such as the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights.

Although some jurisdictions, such as the European Union, have begun to think about regulating AI systems, the cross-border nature of these technologies means that any strictly local approach is insufficient. Global governance, based on shared ethical principles and common legal standards, is becoming essential to provide a responsible framework for AI .

Research problem: As AI establishes itself as an autonomous actor in the public sphere, the risks of discrimination, invasion of privacy and algorithmic marginalisation become more tangible. These abuses are not simply technical errors, but rather the result of a structural imbalance between technological innovation and legal safeguards. It is in this context that a central question arises: How

can we ensure the ethical and responsible use of artificial intelligence on a global scale, while protecting fundamental rights and preventing algorithmic discrimination in a constantly evolving and legally fragmented technological environment?

Importance of the study: The issue is not just technical or economic: it is profoundly legal and ethical. Algorithmic biases, invasions of privacy and risks of systemic discrimination threaten the founding principles of democratic societies. However, in the absence of a coherent global legal framework, responses remain fragmented and often inadequate to provide a framework for technologies with transnational effects. This study is part of a critical reflection on the need for international governance of AI, based on respect for fundamental rights and the principle of non-discrimination.

Research methodology : This study adopts a legal and comparative approach, focusing on two main areas : Risk analysis: by examining algorithmic biases, invasions of privacy and automated decision-making mechanisms, the first part identifies the threats that AI poses to fundamental rights. Exploring normative solutions : the second part looks at existing legal instruments designed to provide a responsible framework for AI. Particular attention is paid to the need for human control and the construction of an international regulatory framework.

1-Tilte I: Artificial intelligence, a vector of risks for fundamental rights and attacks on the principle of non-discrimination

In recent decades, technological innovation has profoundly reshaped the structures through which individuals interact, communicate, and organize their personal, professional, and civic lives. Among these innovations, artificial intelligence (AI) stands out as a transformative force, driven by the exponential growth of data-centric technologies and the increasing automation of tasks once exclusively performed by humans. Far from being a neutral tool, AI systems are embedded within socio-technical frameworks that reflect—and sometimes exacerbate—existing inequalities and normative tensions.

The global health crisis triggered by the COVID-19 pandemic has accelerated the deployment of AI across multiple sectors, including healthcare, education, public administration, and security. This rapid expansion has been accompanied by a surge in data collection and sharing practices, often justified by the urgency of crisis management. While these developments have opened new avenues for innovation and efficiency, they have simultaneously exposed individuals and communities to heightened risks—particularly in relation to the protection of fundamental rights.

Two areas of concern have emerged with particular intensity: first, the proliferation of algorithmic biases that may reproduce or amplify discriminatory practices (1.1) under the guise of technical objectivity; and second, the erosion of privacy and data protection safeguards(1.2). in environments increasingly governed by opaque and automated decision-making processes. These risks are not merely theoretical—they manifest in concrete social, legal, and ethical dilemmas that challenge the foundational principles of equality, dignity.

1.1- Algorithmic biases, sources of discrimination

Machine learning algorithms are fundamentally built upon data generated, structured, and digitized through human activity. This data stems from a wide range of sources reflecting everyday behaviors and interactions: social media exchanges, consumer purchasing habits analyzed for commercial targeting, musical preferences tracked by streaming platforms, visual content shared online[1], written communications such as emails and text messages, search engine histories, and decisions related to employment, creditworthiness, or access to public services. Each data point

[1]-Bertail Patrice, Bounie David, Clémençon Stephan, and Waelbroeck Patrick, Algorithmes : biais, discrimination et équité, Télécom Paris Tech, Février 2019, p6.

contributes to a vast informational ecosystem from which algorithms extract patterns, correlations, and predictive models.

Once collected, this data is processed by machine learning systems to construct statistical models that guide automated decision-making. These models enable algorithms to perform increasingly complex tasks—such as classification, recommendation, and autonomous decision-making—with minimal human oversight. However, despite their technical sophistication, these systems remain entirely dependent on the quality, diversity, and representativeness of the input data. When data is incomplete, biased, or skewed toward particular demographic or behavioral profiles, the algorithmic outputs may reproduce and reinforce those distortions.

In essence, the power of machine learning lies not only in its computational capacity but also in the human choices that shape its informational foundations. The selection, labeling, and interpretation of data are never neutral—they carry embedded assumptions, cultural norms, and systemic biases that can profoundly affect the fairness and reliability of algorithmic decisions.

Although AI algorithms are widely praised for their efficiency and scalability, they are also susceptible to bias. Algorithmic bias refers to flaws in the functioning of an algorithm that result in inconsistent, unequal, or unfair treatment of individuals or situations. Often described as "technological discrimination[2]," this phenomenon occurs when machine learning systems reproduce social inequalities by discriminating against specific groups. Such biases may arise from the ingestion of subjective data, the overrepresentation of certain populations in training datasets, or statistical distortions embedded in the modeling process. Despite the presumed neutrality of data, algorithms can generate outputs that reflect racist, sexist, or culturally prejudiced assumptions. Because they rely on statistical analysis of large datasets, algorithms tend to replicate existing social patterns—including problematic stereotypes.

Several mechanisms may explain the emergence of discriminatory biases in algorithms:

Cognitive Biases: Developers may unconsciously embed their own assumptions into algorithmic design. Confirmation bias, for instance, can influence how data is selected and interpreted. A 2018 study by the AI Now Institute[3] highlighted that the overrepresentation of white men among data scientists, coupled with the underrepresentation of minorities, can lead to blind spots in recognizing and mitigating bias.

Statistical Biases: These may originate from the training data or the algorithm itself. In 2015, Amazon discontinued an AI recruitment tool that discriminated against female candidates due to biased training data. Statistical bias can also result from modeling choices, such as omitted variable bias—where key variables are excluded—or selection bias, which arises when the sample used is not representative of the broader population. Endogeneity bias [4]may also occur when explanatory variables are correlated with the model's error term, distorting coefficient estimates and undermining reliability.

Economic Biases: Algorithms optimized for cost-efficiency may inadvertently favor certain groups over others. For example, researchers found that an algorithm used to deliver ads for STEM jobs showed fewer ads to women because the cost of targeting young women[5] was higher than that of young men. The algorithm, aiming to minimize expenses, thus reinforced gender disparities.

Contextual Biases: The deployment of algorithms in specific contexts—such as facial recognition used by law enforcement in certain neighborhoods—can produce discriminatory effects depending on the objectives and social dynamics involved.

---

[2] - Aurélie Jean, Les algorithmes font-ils la loi ; Editions de l'observatoire, Paris, 2021, pp. 209-210.

[3]-AI Now Report 2018, December 2018, available online at: https://ec.europa.eu/futurium/en/system/files/ged/ai_now_2018_report.pdf (20/02/2025).

[4] - Bertail Patrice, et al, op.cit, p10.

[5] - Bertail Patrice, et al, op.cit, p12.

Other types of biases are related to modeling, including **representation bias**, which results from unbalanced or non-diverse samples; **measurement bias**, caused by incorrect measurement of features or using inaccurate proxies; **evaluation bias**, which arises when benchmark datasets do not represent the target population; and **popularity bias** in recommendation systems, where items with higher ratings are prioritized regardless of users' actual interests.[6]

The consequences of algorithmic bias are far-reaching. They can distort outcomes and perpetuate discrimination. One notable example is Microsoft's chatbot "Tay," launched in 2016 and trained on Twitter data. Within 24 hours, it began producing misogynistic and racist messages, including statements such as "feminism is cancer." Other examples include biased credit scoring systems that disproportionately reject applications from minority groups, or translation tools that consistently render "nurse" as "infirmière," even when the context implies a male subject.

Ultimately, algorithmic bias undermines the principle of equality and non-discrimination. To ensure the ethical integrity and accountability of AI systems, it is essential to detect and correct these biases through rigorous algorithmic audits, inclusive data practices, and transparent governance frameworks.

Ultimately, algorithmic bias undermines the principles of equality and non-discrimination. To ensure ethical integrity and accountability in AI systems, it is essential to detect and correct these biases through rigorous algorithmic auditing, inclusive data practices, and transparent governance frameworks that ensure fairness and equality in technological decision-making.

1.2- Violations of privacy and data protection

While artificial intelligence offers undeniable advantages—particularly in its capacity to process vast datasets and automate complex decisions—it also introduces profound risks to the protection of privacy and personal data. AI systems are inherently data-driven. They rely on continuous—and often indiscriminate—collection, analysis, and interpretation of personal information. related to individuals[7]. This reliance gives rise to structural vulnerabilities, especially when data is gathered without explicit consent or used in ways that individuals neither anticipate nor control.

These risks to privacy and data protection manifest in several distinct yet interconnected forms. To grasp the full scope of these challenges, it is essential to examine three structural dimensions:

a) Massive and Opaque Data Collection

AI systems require vast quantities of personal data to function effectively. This data includes consumer preferences, browsing history, geolocation, online behavior, and biometric identifiers such as facial geometry, fingerprints, and voice patterns. Through aggregation across platforms and devices, AI constructs highly detailed and intrusive profiles—often without the individual's knowledge or consent.

For instance, logging into a Google account enables the consolidation of data across services; emails, location history, search queries, and third-party interactions[8].

Such practices, common among digital giants like Google, Meta, and other GAFAM entities, reflect a structural tension between commercial data exploitation and the fundamental right to

[6] -Markus Kattnig, Alessa Angerschmid, Thomas Reichel, Roman Kern , Assessing trustworthy AI: Technical and legal perspectives of fairness in AI , Computer Law & Security Review 55 (2024) 106053 , journal homepage: www.elsevier.com/locate/clsr ; p 8,9.

[7] -Abdelli Naima, Protection des données personnelles dans la loi Algérienne, Revue des études sur l'effectivité de la norme juridique, Volume 4, n° 1, 2020, p278.

[8] -Rapport de Recherche, Intelligence artificielle et protection de la vie privée La perspective des consommateurs, Option consommateurs, Canada, 2021. p14.

privacy. The scale and opacity of these ecosystems make it exceedingly difficult for individuals to understand, let alone control, how their personal information is used, stored, or shared.

b) Algorithmic Profiling and Discrimination

Beyond data collection, AI technologies are increasingly used to automate decisions that directly affect individuals' rights and opportunities. Facial recognition systems can identify and track individuals in public spaces, potentially infringing on their right to anonymity and freedom of movement[9]. Algorithmic scoring systems assess eligibility for loans, employment, insurance, or public services.

These systems, often trained on biased or incomplete datasets and governed by opaque criteria, can produce discriminatory outcomes or unjust exclusions—particularly for marginalized populations. The lack of transparency and accountability mechanisms leaves affected individuals with limited avenues for contestation or redress.

By relying on historical data, these systems risk replicating entrenched societal biases—thereby reinforcing inequality while presenting themselves as neutral or objective.

c) Intrusion into Private Spaces Through Connected Technologies

The widespread adoption of connected devices—such as smartwatches, voice-activated assistants, surveillance cameras, and household appliances—has significantly expanded the scope of data collection within domestic environments. These technologies are designed to monitor user behavior continuously, record conversations[10], and transmit data to external servers, often without the user's full awareness or informed consent.

This continuous and often imperceptible surveillance transforms private spaces into data-generating environments, where everyday actions and interactions are captured, analyzed, and potentially exploited. As a result, highly sensitive personal information—including names, addresses, phone numbers, email accounts, financial details, and real-time location data—may be exposed to unauthorized access, commercial profiling, or even malicious use.

Such intrusions raise serious concerns about the erosion of the right to privacy within the home, a space traditionally considered inviolable. The lack of transparency surrounding how these devices operate, what data they collect, and how that data is processed or shared further complicates users' ability to protect themselves. In this context, the deployment of AI-powered connected technologies demands rigorous scrutiny to ensure that convenience and innovation do not undermine fundamental rights.

2-Tilte II: Guaranteeing respect for fundamental rights in the development of artificial intelligence

As artificial intelligence systems become increasingly embedded in decision-making processes across public and private domains, the imperative to safeguard fundamental rights grows more urgent. Ensuring that AI technologies operate in a manner that respects human dignity, equality, and autonomy requires more than technical efficiency—it demands a normative framework grounded in transparency, accountability, and ethical responsibility.

To this end, AI systems must be designed to be both transparent and explainable. Citizens must be able to understand not only the outcomes produced by algorithms, but also the underlying logic, data sources, and decision-making pathways that inform those outcomes. Without such intelligibility, individuals are left vulnerable to opaque systems that may affect their rights without recourse or comprehension.

---

[9] - Thierry Ménissier, Les Dispositifs de Reconnaissance Faciale un Défi pour l'Ethique de l'Intelligence Artificielle, Klēsis. Revue Philosophique, n°49, 2021, p 6-7.

[10] - Anne-Lise Thouroude, Les objets : de la communication à l'intelligence, Développer et conduire le numérique Enjeux numériques, Annales des Mines, n°20, December 2022.

It is essential to reaffirm that artificial intelligence must remain a tool in the service of humanity and the public interest—not merely a vehicle for technological advancement or commercial gain. Humanist values must guide its development, ensuring that ethical considerations are prioritized over market incentives. This includes the responsible collection and processing of training data, which must be conducted with full respect for users' informed consent, privacy, and confidentiality. The integrity of data must be protected through robust cybersecurity measures to prevent unauthorized access, manipulation, or exploitation.

Moreover, the deployment of AI must be accompanied by safeguards that preserve meaningful human oversight. Automated systems should never operate in isolation from human judgment (2.1), particularly in contexts where rights and freedoms are at stake. It is equally vital to establish clear and enforceable regulatory frameworks (2.2) that define the boundaries of acceptable AI use, promote fairness and inclusivity, and ensure that technological innovation does not come at the expense of legal and ethical standards.

2.1- The need for human control of AI systems

Artificial intelligence systems, regardless of their sophistication, lack the capacity for moral judgment and contextual reasoning. They execute tasks based on predefined objectives, without the ability to assess the broader social, legal, or ethical consequences of their outputs. This limitation makes human oversight indispensable at every stage of the AI system's [11] lifecycle, especially in sensitive domains such as healthcare, law enforcement, border control, and financial services, where automated decisions can directly affect fundamental rights and freedoms.

A consensus in the legal world has emerged on the need for "human control" of AI systems, particularly when they have a significant impact on human rights. It is not merely a technical safeguard, but a normative imperative aimed at preserving human autonomy, accountability, and the legitimacy of decisions made with or through AI systems.

The principle of human oversight in AI is multifaceted. To fully grasp its normative, technical, and legal dimensions, it is helpful to distinguish between two interrelated aspects :

a) - Models and Definitions of Human Oversight

A wide range of terms is used in legal and technical literature to describe the concept of human control over AI systems. These include: human intervention[12] , human monitoring and verification[13] , meaningful decision control[14] , meaningful human controls[15] , human-on-the-loop (HOTL)[16] , human in command (HIC)[17] , human-in-the-loop (HITL)[18] ,meaningful human review[19] ,

[11]- UNESCO, Recommendation on the Ethics of Artificial Intelligence, Paris from 9 to 24 November 2021, p 11. Available online at: https:// unesdoc.unesco.org/ark:/48223/pf0000380455_fre (25/02/2025)

[12]- Regulation No 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR), art. 22; European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework for the ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL), point 89; CNIL, "How to allow humans to stay in control? The ethical challenges of algorithms and artificial intelligence", CNIL Report, December 2017.

[13]- Regulation 2021/784 of 29 April 2021 on combating the dissemination of terrorist content online, art. 5(3).

[14]- Art 29 Working Party, Guidelines on automated individual decision making and profiling for the purposes of Regulation (EU) 2016/679, 3 Oct 2017 revised 6 Feb 2018 WP 251rev.01 p. 23

[15]- European Parliament resolution of 20 October 2020, point 68 and recital 10.

[16]- European Commission, Directorate-General for Communication Networks, Content and Technology, Ethical Guidelines for Trustworthy AI, Publications Office, 2019, https://data.europa.eu/doi/10.2759/54071 (HLEG Guidelines), point 65

[17] - Ibid.

[18] - Wu, Xingjiao & Xiao, Luwei & Yixuan, Sun & Zhang, Junhang & Ma, Tianlong & He, Liang (2021). A Survey of Human-in-the-loop for Machine Learning. 2 August 2021, arXiv 2108.00941.

[19]- Revised Code of Washington (RCW) §43.386.010, par. 7.

individual review by non-automated means[20] , human assurance[21] , or "meaningful human review, judgment, intervention and control"[22] .

These models differ in both the timing and scope of human intervention:

-HITL refers to human intervention at every decision cycle. It ensures maximum control but may be impractical for high-frequency or real-time systems.

-HOTL allows human agents to monitor the system during operation and intervene when necessary, striking a balance between autonomy and supervision.

-HIC designates a broader form of oversight, where humans retain strategic authority over the system's deployment and its legal, ethical, and societal implications[23].

Institutional definitions help clarify these distinctions. According to the High-Level Panel of Independent Experts on Artificial Intelligence, which defines it as follows: "Human oversight helps ensure that an AI system does not undermine human autonomy or cause other adverse effects: "Human oversight helps ensuring that an AI system does not undermine human autonomy or cause other adverse effects. Oversight may be achieved through governance mechanisms such as a human-in-the loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC) approach. HITL refers to the capability for human intervention in every decision cycle of the system, which in many cases is neither possible nor desirable. HOTL refers to the capability for human intervention during the design cycle of the system and monitoring the system's operation. HIC refers to the capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the system in any particular situation...".[24]

Similarly, the Revised Code of Washington (RCW) defines human oversight as : "means review or oversight by one or more individuals who are trained in accordance with RCW ...and who have the authority to alter the decision under review."[25]

from these and other definitions[26], we can extract three cumulative conditions that characterise effective human control :

(1) The individual must have sufficient knowledge of how the algorithm functions and its limitations ;

(2) They must engage in a cognitive process of reflection, potentially incorporating contextual information beyond the algorithm's scope ;

(3) They must possess both the authority and the material capacity to intervene and modify the system's output.

b) - Legal Frameworks and Ethical Implications

The requirement for human oversight is increasingly enshrined in legal instruments across jurisdictions.in France, the legislator specified in Law No. 2018-493 of 20 June 2018 on the protection of personal data in Article 21 that "No judicial decision involving an assessment of the

[20]- Directive (EU) 2016/681 of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, investigation, detection and prosecution of terrorist offences and serious crime, art. 6(6) (PNR Directive).

[21]- National Consultative Ethics Committee (CCNE) Opinion 129: "Contribution to the review of the 2018-2019 bioethics law", 18 September 2018.

[22] - European Parliament resolution of 20 October 2020, recital 10.

[23]-Lena Enqvist, Human oversight' in the EU artificial intelligence act: what, when and by whom?, Law, Innovation and Technology, Published by Informa UK Limited, trading as Taylor & Francis Group, 2023, p06.

[24]- The European Commission, Independent High -Level Expert Group on Artificial Intelligence Ethics Guidelines for Trust Worthy AI, 2019, p15. available online : https:// www.justice-ia.com/files/sites/181/2019/10/EthicsguidelinesfortrustworthyAI-FRpdf.pdf (24/02/2024).

[25]- Revised Code of Washington (RCW), op.cit.

[26]- Ben Green, The Flaws of Policies Requiring Human Oversight of Government Algorithms, , Computer Law & Security Review, Volume 45, July 2022 , p. 17, Frank Sauer, ICRAC Int'l Comm for Robot Arms Control, "ICRC Statement on Technical Issues to the 2014 UN CCW Expert Meeting," (May 14, 2014).

behaviour of a person may be based on automated processing of personal data intended to evaluate certain aspects of the personality of that person. No decision having legal effects on a person or significantly affecting him or her may be taken solely on the basis of automated processing of personal data, including profiling... ».[27]

Similar provisions appear in the Revised Code of Washington (RCW)[28] , and in the proposed U.S. Algorithmic Accountability Act of 2022[29] , both of which emphasize the necessity of human review in automated decision-making processes.

At the European level, Directive 2016/681 on the use of Passenger Name Record (PNR) data imposes human control in Article 6(6), which stipulates that[30]: "The Passenger Information Unit of a Member State shall transmit, for further examination, the PNR data of persons identified in accordance with paragraph 2(a) or the result of the processing of such data to the competent authorities referred to in Article 7 of that same Member State. Such transfers shall be made only on a case-by-case basis and, in the case of automated processing of PNR data, after individual review by non-automated means".

The central role of human control in the protection of rights was affirmed by the of the Court of Justice of the European Union (CJEU) in its judgment of 6 October 2020 in the La Quadrature du Net case[31] , and reaffirmed on 21 June 2022[32] in a case concerning the analysis of PNR data of 2 air passengers. The Court held that a detection system generating over 80% false alerts may still be compatible with the Charter of Fundamental Rights of the European Union, provided it includes effective human control.

Human agents must monitor the objectives pursued by AI systems and ensure that the results are aligned with those objectives and socially acceptable. Algorithms pursue only the goals for which they are designed. Human oversight, therefore, is not a procedural formality—it is an ethical necessity. It ensures that AI systems serve human interests, respect legal boundaries, and remain subject to human judgment and correction.

c)-Legal Justice as a Guarantee for the Protection of Fundamental Rights in Artificial Intelligence Systems

Legal justice — understood here as justice under the law and procedural fairness —forms a cornerstone for safeguarding fundamental rights in the face of artificial intelligence challenges. It goes beyond merely addressing technical biases to encompass procedural fairness and legal accountability. Laws aim to ensure that automated decisions are governed by clear, understandable criteria, subject to human review, and accompanied by mechanisms for appeal and correction when necessary.

At the European level, the Charter of Fundamental Rights of the European Union (Article 21) protects citizens from any discrimination based on gender, race, religion, social origin, or any other personal characteristic, providing a benchmark for legal justice when evaluating AI algorithms.

---

[27]- Article 10 of Law No. 78-17 of 6 January 1978, as amended by Article 21 of Law No. 2018-493 of 20 June 2018.
[28]-See Revised Code of Washington (RCW) §43.386.010, par. 7.
[29]- Bill S. 3572 Algorithmic Accountability Act of 2022 by Senators Wyden, Booker and Clarke, February 3, 2022.
[30]- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, investigation, detection and prosecution of terrorist offences and serious crime.
[31]-CJEU, 6 October 2020, La Quadrature du Net, Joined Cases C-511/18, C-512/18 and C-520/18, which repeats the conditions already imposed by the Court in its Opinion 1/15 of 26 July 2017, EU-Canada PNR Agreement. IP/IT Directory and Communication Personal data - Automated decision and justice - Liane HUTTNER November 2020 ;
[32]-CJEU, 21 June 2022, Ligue des droits humains c. Conseil des ministres, aff. C-817/19; Vie privée - Conditions de transfert, de conservation et de traitement des données PNR - Veille par Dominique Berlin La Semaine Juridique Edition Générale n° 27, 11 Juillet 2022, 857; Répertoire de droit européen / La protection des données personnelles dans les relations internes à l'Union européenne Eur. - Céline CASTETS-RENARD - Updated June 2022

Furthermore[33], Article 22 of the General Data Protection Regulation (GDPR) states that "automated decisions that produce legal effects concerning an individual or significantly affect them may not be based solely on automated processing without effective human intervention," linking legal justice directly to the necessity of human oversight.[34]

National laws reinforce this principle. For instance, French Law No. 2018-493 on the protection of personal data stipulates that "any judicial decision relying on automated processing of personal data intended to assess certain aspects of a person's personality must be accompanied by human oversight." Similarly, Directive 2016/681 on the use of PNR data requires individual review by non-automated means before any action is taken, ensuring fairness in data handling.

Looking ahead, the European Union's Artificial Intelligence Act (AI Act, 2024) mandates that high-risk systems—such as facial recognition and automated decision-making tools—undergo comprehensive assessments of fairness and discrimination risks[35], and guarantees transparent mechanisms for human review and appeal. These legal measures underscore that justice is not merely an ethical ideal, but a legal obligation requiring AI developers and operators to uphold transparency, accountability, human oversight, and the right of individuals to challenge decisions affecting their lives.

In this way, legal justice becomes a practical tool that bridges technological innovation and the protection of fundamental rights. Laws, human oversight, and transparency work together to prevent violations and ensure tangible protection for citizens, striking a balance between technological progress and human dignity.[36]

2.2- Towards regulation that protects fundamental rights

Technological progress often outpaces legal frameworks, creating a temporal and conceptual gap between innovation and regulation. This was evident in the 1990s with the emergence of cyberspace, which proved difficult to regulate due to its rapid evolution and the transnational dispersion of websites and IP configurations. Similar arguments are now resurfacing in debates around artificial intelligence (AI), with some advocating against regulation on technical grounds. However, the urgency to protect fundamental rights calls for proactive legal responses that anticipate—not merely react to—technological disruption.

The regulation of artificial intelligence is a multidimensional challenge. To better understand how legal and ethical frameworks are evolving to safeguard fundamental rights, this section is divided into two key parts :

a) -the development of regional and national regulatory instruments

Europe has positioned itself as a pioneer in regulating algorithmic systems and personal data[37], The General Data Protection Regulation (GDPR), rooted in the French Data Protection Act of 1978, imposes heavy penalties on companies including impact assessments and safeguards against discriminatory data processing. Building on this foundation, the European Parliament adopted the Artificial Intelligence Act in February 2024, establishing a framework for responsible AI development. This regulation sets standards for high-risk systems—such as facial recognition and automated decision-making—and mandates human oversight to mitigate risks.[38].

---

[33] Charter of Fundamental Rights of the European Union, Article 21, Official Journal of the European Union, C 326, 26.10.2012, p. 391–407.

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Article 22, OJ L 119, 4.5.2016, p. 1–88.

[35] European Union, Artificial Intelligence Act, 2024, Official Journal of the European Union.

[36] Markus Kattnig, Alessa Angerschmid, Thomas Reichel, Roman Kern , op.cit; p 2-3.

[37]-cf. Francis Donnat, *Droit européen de l'internet*, Paris, lgdj, 2018, p. 65 et seq.

[38]-A European Commission White Paper on AI has been published, demonstrating that AI regulation is essential to protect the Union's fundamental rights and values. Based on the Council of Europe's standards on human rights,

In addition to the General Data Protection Regulation which applies to AI practices in Europe, a European AI Regulation was recently adopted by the European Parliament: Artificial Intelligence Legislation, also known as the Artificial Intelligence Act[39] . This regulation aims to ensure that AI is designed and used in a responsible manner that respects fundamental rights, in particular the rights of individuals relating to the protection of personal data[40] .

It also defines specific standards for high-risk AI systems, such as facial recognition, profiling and automated decision-making systems. The design and implementation of these systems must be carried out in such a way as to minimise the risks to the individuals concerned and include human supervision. This regulation is in line with the European approach to AI, which focuses "on excellence and trust, aiming to strengthen research and industrial capabilities while guaranteeing safety and fundamental rights" .[41]

In order to guarantee respect for fundamental rights, a number of initiatives have also been launched, notably by the Commission nationale de l'informatique et des libertés (CNIL), with the aim of responding to the challenges posed by artificial intelligence. The CNIL states that the main aims of its work are : "to understand how AI systems work and their impact on individuals, to enable and supervise the development of AI that respects personal data, to bring together and support the innovative players in the AI ecosystem in France and Europe, to audit and monitor AI systems and protect individuals" .[42]

In France, the National Consultative Commission on Human Rights (CNCDH) published an opinion in April 2022 on the impact of artificial intelligence on fundamental rights[43] , recommending in particular that the legal and ethical framework for AI be strengthened, that the transparency and accountability of AI players be guaranteed and that the risks of AI-related discrimination be prevented.

For its part, in June 2022 the Canadian federal government tabled the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27, the Digital Charter Implementation Act, 2022, which includes three laws on privacy protection, the data court and AI[44] . The government had previously passed the Artificial Intelligence Accountability Act (AIAA) in December 2021, which aims to provide a framework for the use of AI by federal institutions and to protect the rights of people affected by AI. Among other things, the AIAA sets out obligations for impact assessment, transparency, redress and oversight in relation to AI.[45]

---

democracy and the rule of law, the Council of Europe's Committee on Artificial Intelligence (CAI) has also been working on a legal framework on artificial intelligence.

[39]-European Commission, Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (ARTIFICIAL INTELLIGENCE ACT) and Amending Certain Union Legislative Acts, 2021/0106 (COD) ,21.4.2021. available online : https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF (29/02/2025).

[40]-At the end of September 2021, the Brazilian Congress passed a bill creating a legal framework for artificial intelligence. This bill still has to be passed by the Brazilian Senate.

[41]- European Commission, A European approach to artificial intelligence, available online: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (29/02/2025).

[42] -CNIL,Création d'un service de l'intelligence artificielle à la CNIL et lancement des travaux sur les bases de données d'apprentissage, 23 January 2023, available online : https:// www.cnil.fr/fr/creation-dun-service-de-lintelligence-artificielle-la-cnil-et-lancement-des-travaux-sur-les-bases-de (29/02/2025).

[43] -CNCDH, Opinion on the impact of artificial intelligence on fundamental rights (A-2022-6), JORF n°0091 of 17 April 2022, text n° 99.

[44] -Simon Hodgett, Kuljit Bhogal and Sam Ip Government of Canada Artificial Intelligence and Data Act: Overview, .osler. 27 June 2022, available online: https://
www.osler.com/fr/ressources/reglements/2022/loi-sur-l-intelligence-artificielle-et-les-donnees-du-gouvernement-du-canada-apercu (29/02/2025).

[45] Canada and France adopted a Joint Declaration in June 2018, in which they affirm their desire to work towards an artificial intelligence that is ethical, responsible, human-centred and respectful of human rights, in line with the report by

In the United States, although there is no specific federal legislation on AI several initiatives at the federal level have been launched to regulate AI, including facial recognition, predictive policing, employment equity and data privacy. For example, a task force on algorithmic accountability was created by New York City in 2018 to examine the use of automated systems by city agencies and propose measures to avoid bias and discrimination.[46]

China, for its part, has drawn up a series of technical and ethical standards to guide the development and responsible application of AI in various sectors, such as finance, health and public safety.[47]

b) – the emergence of global ethical principles and multilateral cooperati

At international level[48], ethical reflection has gained momentum. the OECD published its guidelines on the protection of privacy in 1980. But it was not until May 2019 that the first such principles on AI were adopted by its members, who envisage that artificial intelligence should serve the interests of the planet and individuals, and that they should be designed with respect for the rule of law, human rights, democratic values and diversity. They also mention the need for transparency, security and upstream control of these systems.[49]

For its part, in November 2021 UNESCO adopted the Recommendation on the Ethics of AI, which consolidates a number of fundamental principles such as transparency and fairness, human control of AI systems, and data governance...[50] .

Other initiatives are also underway at international level, such as the Global Partnership on Artificial Intelligence (GPAI) launched in 2020 by fifteen G7 member countries, which aims to promote a coordinated and responsible approach to the development of AI.

Beyond legislative efforts, it is crucial that a global ethical reflection accompanies the development of this technology. The regulation of artificial intelligence is a major challenge if we are to preserve our democratic values and guarantee a future in which AI serves humanity. and societal well-being.

c)- Effective Safeguards in the Development and Regulation of Artificial Intelligence

---

MP and mathematician Cédric Villani. The two countries are working to set up an International Group of Experts on Artificial Intelligence (G2IA).

[46]-Stany Nzobonimpa, Algorithmes et intelligence artificielle : une note sur l'état de la réglementation des technologies utilisant la reconnaissance faciale automatique au Canada et aux États-Unis, Revue Gouvernance Governance Review, Volume 19, Number 2, 2022, p107.

[47]- CJO Collaborative Team, China issues code of ethics for next-generation AI, 01 November 2021, available online: https:// en.chinajusticeobserver.com/a/china-issues-code-of-ethics-for-new-generation-ai (03/03/2025).

[48]-Although there is as yet no specific legislation governing artificial intelligence in many countries, the international human rights conventions ratified by these states also apply to the development of AI. For example, the International Covenant on Civil and Political Rights, ratified by most countries, guarantees the right to privacy, the right to freedom of expression and the right to equality and non-discrimination. These fundamental rights enshrined at international level therefore provide an initial protective framework in the face of the potential risks of artificial intelligence, even without specific national legislation on AI.

[49]-OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, Adopted on 22/05/2019, available online: https:// legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (03/03/2025).

[50]-UNESCO, Recommendation on the Ethics of Artificial Intelligence, SHS/BIO/PI/2021/1, available online : https:// unesdoc.unesco.org/ark:/48223/pf0000381137_fre (03/03/2025)

There is broad consensus on the need for AI systems to uphold fundamental rights, including privacy protection, fairness and integrity, transparency, accountability, non-maleficence, beneficence, and the preservation of individual freedoms. Regulatory frameworks should explicitly aim to safeguard these rights. Given the specific risks posed by AI, regulatory efforts must be precise and context-sensitive, as overly general regulations often fail to address complex challenges, leaving critical gaps unaddressed.

Computer scientists have developed practical solutions to mitigate AI-related risks, and ignoring these technical tools in regulation would weaken its effectiveness. At the same time, regulatory policies should reflect the variability of ethical commitments among companies and create incentives that promote positive behavior. While regulation is essential, stricter rules are not always better; rigid regulations can stifle innovation, slow technological progress, and hinder economic growth, especially in fast-evolving domains.

Effective AI governance requires a multi-level approach that considers the unique characteristics of each sector and leverages expertise from government, industry, academia, and computer science. Tools such as AI system certification and regulatory sandboxes play a crucial role, clarifying legal responsibilities, allowing testing in controlled environments, and proactively reducing risks before deployment—thereby ensuring safe innovation while protecting fundamental rights.

Finally, regulators must ensure that policies uphold ethical principles, protect individual rights, balance innovation with safety, and remain flexible to accommodate future technological developments. Robust compliance mechanisms are also necessary to enforce standards, enhance trust and accountability, and guarantee the responsible deployment of AI technologies in ways that respect the fundamental rights of all users.[51]

Conclusion:

Artificial intelligence (AI) has become an increasingly pervasive force in contemporary society, offering transformative potential across a wide range of sectors. From facial recognition and autonomous vehicles to predictive analytics, resource optimization, and administrative transparency, AI systems promise significant gains in efficiency, precision, and scalability. These technological advancements are reshaping not only how institutions operate but also how individuals engage with public and private services.

Yet, this evolution is not without profound ethical and legal challenges. The deployment of AI raises critical concerns regarding algorithmic bias, data confidentiality, and the erosion of individual autonomy. These issues underscore the urgent need to ensure that AI development and implementation are firmly anchored in the respect for fundamental rights. It is not enough to pursue innovation for its own sake; rather, AI must be guided by normative principles that prioritize human dignity, fairness, and accountability.

To achieve this, several safeguards must be put in place. First, ethical frameworks must be integrated into the design and governance of AI systems, ensuring that their objectives align with societal values rather than purely commercial or technical imperatives. Second, human oversight must be maintained throughout the entire lifecycle of AI systems—from data collection and model training to deployment and evaluation—so that automated decisions remain subject to human judgment and democratic control. Third, robust regulatory mechanisms must be established to guide AI toward responsible and rights-respecting practices.

[51] Daniel Oliveira Cajueiro , Victor Rafael Rezende Celestino, A comprehensive review of Artificial Intelligence regulation: Weighing ethical principles and innovation, Journal of Economy and Technology 4 (2026) 77–91, journal homepage: www.keaipublishing.com/JET ,p89-90.

Although the task is complex and the stakes are high, it is imperative to uphold the principles of justice, equality, and transparency in the digital age. If approached with care and foresight, artificial intelligence can serve as a powerful instrument for social progress rather than a source of exclusion or surveillance. The challenge lies not in rejecting AI, but in shaping its trajectory to serve the public good.

To this end, we propose the following strategic recommendations:

1-Implement sector-specific regulations tailored to the unique risks and requirements of each domain of AI application, ensuring contextual relevance and legal precision.

2-Promote a harmonized international legislative framework to prevent regulatory fragmentation, which could undermine both the protection of citizens and the competitiveness of global innovation ecosystems.

3-Encourage multi-stakeholder collaboration between public authorities, private enterprises, civil society, and academic institutions to develop shared ethical and technical standards, and to disseminate best practices in the responsible design and use of AI.

4-Establish independent oversight bodies, such as regulatory agencies or ethics commissions, tasked with monitoring AI systems' compliance with legal and ethical norms, conducting audits, and enforcing sanctions in cases of violation.

References:

Books:

- Aurélie Jean, Les algorithmes font-ils la loi; Editions de l'observatoire, Paris, 2021.
- Bertail Patrice, Bounie David, Clémençon Stephan, and Waelbroeck Patrick, Algorithmes : biais, discrimination et équité, Télécom Paris Tech, Février 2019.
- Francis Donnat, *Droit européen de l'internet*, Paris, LGDJ, 2018.
- Lena Enqvist, Human oversight' in the EU artificial intelligence act: what, when and by whom?, Law, Innovation and Technology, Published by Informa UK Limited, trading as Taylor & Francis Group, 2023.

Articles:

- Abdelli Naima, Protection des données personnelles dans la loi Algérienne, Revue des études sur l'effectivité de la norme juridique, Volume 4, n° 1, 2020.
- Anne-Lise Thouroude, Les objets : de la communication à l'intelligence, Développer et conduire le numérique Enjeux numériques, Annales des Mines, n°20, December 2022.
- Ben Green, The Flaws of Policies Requiring Human Oversight of Government Algorithms, Computer Law & Security Review,Volume 45, July 2022.
-Daniel Oliveira Cajueiro , Victor Rafael Rezende Celestino, A comprehensive review of Artificial Intelligence regulation: Weighing ethical principles and innovation, Journal of Economy and Technology 4 (2026) 77–91, journal homepage: www.keaipublishing.com/JET
-Frank Sauer, ICRAC Int'l Comm for Robot Arms Control, "ICRC Statement on Technical Issues to 2014 UN CCW Expert Meeting," May 14, 2014.
-Markus Kattnig, Alessa Angerschmid, Thomas Reichel, Roman Kern , Assessing trustworthy AI: Technical and legal perspectives of fairness in AI , Computer Law & Security Review 55 (2024) 106053 ,journal homepage: www.elsevier.com/locate/clsr
-Nzobonimpa, Stany, Algorithmes et intelligence artificielle : une note sur l'état de la réglementation des technologies utilisant la reconnaissance faciale automatique au Canada et aux États-Unis, Revue Gouvernance, vol. 19, n° 2, 2022.
- Thierry Ménissier, Les Dispositifs de Reconnaissance Faciale un Défi pour l'Ethique de l'Intelligence Artificielle, Klēsis. Revue Philosophique, n°49, 2021.
- Wu, Xingjiao & Xiao, Luwei & Yixuan, Sun & Zhang, Junhang & Ma, Tianlong & He, Liang (2021). A Survey of Human-in-the-loop for Machine Learning. 2 August 2021, arXiv 2108.00941.

Laws, regulations, case law

-Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Article 22, OJ L 119, 4.5.2016
-Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016 (RGPD), art. 22.
- Directive (EU) 2016/681 of the European Parliament and of the Council, 27 April 2016, art. 6(6), on PNR data.
- Regulation (EU) 2021/784, 29 April 2021, on terrorist content online, art. 5(3).
- Article 10 of Law no. 78-17 of 6 January 1978 as amended by Law no. 2018-493 of 20 June 2018.
-Revised Code of Washington (RCW) §43.386.010, par. 7.
- Bill S.3572 - Algorithmic Accountability Act of 2022 (United States), introduced on 3 February 2022.
- CJEU, La Quadrature du Net, C-511/18, C-512/18 and C-520/18, 6 October 2020.
- CJEU, Ligue des droits humains v. Conseil des ministres, C-817/19, 21 June 2022.

International statements and positions

- Canada-France joint statement, June 2018 (following the Villani report on AI).
- Council of Europe, White Paper on AI, CAI Committee, legal framework under development.
- International Covenant on Civil and Political Rights, UN (guaranteeing the right to privacy and non-discrimination in the development of AI).

Institutional reports and opinions

- AI Now Report 2018, December 2018. Available at: ec.europa.eu (accessed 20/02/2025).
- CNIL, Report on the ethical challenges of algorithms and artificial intelligence, December 2017.
- CNIL, Service IA et travaux sur les bases de données d'apprentissage, January 23, 2023. cnil.fr (consulted on 02/29/2025).
- CNCDH, Opinion on the impact of artificial intelligence on fundamental rights, A-2022-6, JORF n° 0091 of April 17, 2022.
- CCNE, Avis 129 - Contribution à la révision de la loi bioéthique, September 18, 2018.
- European Commission, Ethical Guidelines for Trustworthy AI, Publications Office, 2019: data.europa.eu (accessed 24/02/2024).
- European Commission, AI Act - Proposal for a Regulation on Artificial Intelligence, 2021/0106 (COD), eur-lex.europa.eu (accessed 02/29/2025).
- European Commission, European approach to AI, digital-strategy.ec.europa.eu (accessed 02/29/2024).
-European Union, Artificial Intelligence Act, 2024, Official Journal of the European Union.
-Charter of Fundamental Rights of the European Union, Article 21, Official Journal of the European Union, C 326, 26.10.2012
- UNESCO, Recommendation on the Ethics of Artificial Intelligence, November 2021: unesdoc.unesco.org (consulted on 02/25/2025).
- UNESCO, SHS/BIO/PI/2021/1, unesdoc.unesco.org (consulted on 03/03/2025).
- OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, May 22, 2019: legalinstruments.oecd.org (consulted 03/03/2025).
- Government of Canada, Artificial Intelligence and Data Act, June 27, 2022: osler.com (accessed 02/29/2024).
- CJO Collaborative Team, China Issues Code of Ethics for New Generation AI, November 1, 2021.