Chapter 3 / Capítulo 3

Superintelligence Series
ISSN 3046-4463
Volume 2 – Thinking in Machine Code: Dialogues between technology, knowledge, and culture
ISBN of the complete work: 978-9915-9851-0-7
ISBN of this volume: 978-9915-9851-2-1
DOI of the chapter: https://doi.org/10.62486/978-9915-9851-0-7_202517

©2025 The authors. This is an open access article distributed under the terms of the Creative Commons Attribution (CC BY) 4.0 License.

REVIEW

Ethics, Identity and Algorithmic Decoloniality in Artificial Intelligence

Ética, Identidad y Decolonialidad Algorítmica en la Inteligencia Artificial

René Ernesto Esquivel Gaón[1]

[1]Universidad de Cuenca, Cuenca, Ecuador

ABSTRACT

The ethical dimensions in the application of Artificial Intelligence (AI) are significantly influenced by cultural identity and coloniality, particularly within algorithmic decision-making processes. Cultural identity shapes how individuals interact with AI: while individualistic cultures may perceive AI as an external entity that infringes upon personal autonomy, collectivist cultures may interpret it as an extension of the self, affecting notions of privacy and conformity. This chapter analyzes the interrelation between ethics, identity, and algorithmic decoloniality in the context of artificial intelligence (AI). It examines how algorithmic technologies reproduce historical structures of power and knowledge rooted in colonial modernity, thereby influencing the recognition of cultural and epistemic identities in Latin America, with a particular focus on the Ecuadorian case. From a philosophical, critical, and applied perspective, it proposes a decolonial evaluation methodology for the ethical development of algorithmic systems, aiming to foster a more just, transparent, and plural AI. The analysis concludes that algorithmic ethics must incorporate distributive justice, epistemic pluralism, and data sovereignty as fundamental principles for the responsible governance of artificial intelligence in the Global South.

Keywords: Algorithmic Ethics; Identity; Decoloniality; Artificial Intelligence; Epistemic Justice.

RESUMEN

Los elementos éticos en la aplicación de la inteligencia artificial (IA) está significativamente influenciada por la identidad cultural y la colonialidad, particularmente en los procesos algorítmicos de toma de decisiones. La identidad cultural determina las interacciones de las personas con la IA, donde las culturas individualistas pueden percibir la IA como una entidad externa que infringe la autonomía, mientras que las culturas colectivistas pueden verla como una extensión de uno mismo, lo que repercute en la privacidad y la conformidad. El presente capítulo analiza la interrelación entre la ética, la identidad y la decolonialidad algorítmica en el contexto de la inteligencia artificial (IA). Se examina cómo las tecnologías algorítmicas reproducen estructuras históricas de poder y conocimiento propias de la modernidad colonial, afectando el reconocimiento de identidades culturales y epistémicas en América Latina, con énfasis en el caso ecuatoriano. Desde un enfoque filosófico, crítico y aplicado, se propone una metodología de evaluación decolonial para el desarrollo ético de sistemas algorítmicos, promoviendo una IA más justa, transparente y plural. El análisis concluye que la ética algorítmica debe considerar la justicia distributiva, el pluralismo epistémico y la soberanía de datos como principios fundamentales para la gobernanza responsable de la inteligencia artificial en el Sur Global.

Palabras clave: Ética Algorítmica; Identidad; Decolonialidad; Inteligencia Artificial; Justicia Epistémica.

INTRODUCTION

Artificial intelligence (AI) has established itself as a structural technology of contemporary society, transforming systems of decision-making, communication, surveillance, economics, and culture. We live in a hybrid digital world where AI technologies shape our social and everyday relationships.[1] As Floridi points out, the transition from analog reality to an "onlife situation" means that digital tools are more than mere mediators, as they define the form and scope of our interactions. This irreversible global change requires philosophy, ethics, and public policy to seek to understand, shape, and implement what is morally good in the technological sphere.[1] However, most existing global frameworks (UNESCO or OECD) are based on Eurocentric epistemologies and cosmologies that have emerged from the European experience.[2] These are presented as universal norms that, in practice, can be imposed without real dialogue with the cultural logics of other latitudes.

Artificial Intelligence technology is not neutral, as it carries the DNA of those who control the data and its algorithms.[3] This implies that its expansion has taken place in an ethical and epistemic vacuum: algorithms are socio-technical artifacts that reflect the power hierarchies, cultural assumptions, and historical inequalities of the modern world. This chapter proposes an interpretation of the interaction between ethical elements, identity, and decoloniality, understanding that the use and design of AI in our countries requires the integration of philosophical frameworks of epistemic justice, data sovereignty, and epistemic pluralism.

This chapter is structured around three fundamental axes that articulate critical reflection on ethics and artificial intelligence in the Latin American context. First, it addresses algorithmic ethics, demonstrating the principles of justice, transparency, and responsibility in the design and use of intelligent systems. Next, it analyzes digital identity, understood as the construction and representation of subjects in data-mediated environments, where tensions emerge between autonomy, privacy, and cultural recognition. Finally, it examines algorithmic coloniality, revealing how technological structures reproduce epistemic and power hierarchies, demanding a decolonial perspective that promotes cognitive justice and technological sovereignty.

DEVELOPMENT

Ethics in Artificial Intelligence

Algorithmic ethics[1] faces the challenge of transcending approaches focused solely on bias mitigation or technical transparency. From a decolonial perspective, it seeks to dismantle the coloniality of knowledge, power, and being in intelligent systems, promoting a plural epistemology that recognizes local knowledge, non-Western forms of rationality, and the technological self-determination of peoples.

Floridi[1] proposes a set of core principles, additionally describing how they are violated or strained in these contexts and at least one of the moral implications that can be perceived. Furthermore, these principles encompass the concerns of multiple AI ethics lists presented in Europe and North America.

Now, putting these principles into practice reveals wide gaps when adapting to Latin American realities. Several researchers[1,4] warn that ethical policies are often reduced to mere voluntary statements, which opens the door to misleading uses, i.e., organizations can proclaim codes of ethics to clean up their image without changing bad practices, or select only the principles

[1]Algorithmic Ethics is a branch of applied ethics that studies, analyzes, and addresses the social, legal, and moral impacts of algorithms, especially those used in Artificial Intelligence (AI) and machine learning (ML) systems. (39)

that suit them. This highlights a gap between "strong ethics," based on principles that inspire regulation, and "soft ethics," with moral values that have no real legal application. In practice, the absence of robust regulatory frameworks makes it easier for organizations to export bad practices to countries with little regulation, increasing algorithmic injustice.

Table 1. Ethical dimensions involved

Ethical principle	How it is violated or strained in these contexts	Moral implications
Justice/equity	Racial, gender, socioeconomic biases; unequal access to the benefits of AI	Vulnerable populations are systematically excluded or disadvantaged; reinforcement of historical inequalities
Autonomy/informed consent	Use of data without individuals or communities fully understanding or consenting; algorithms operating without transparency	Violation of the right to self-determination, especially of indigenous or marginalized communities
Privacy	Collection, storage, and use of sensitive data without sufficient safeguards; insufficient legislation or legal loopholes	Risk of surveillance, discrimination, loss of control over personal or community information
Transparency and explainability	In many cases, the models are "black boxes"—it is not known how they make decisions—and the affected public is not informed	Difficulty in filing complaints or conducting audits; risk of arbitrariness or unfair decisions
Responsibility/accountability	Lack of mechanisms for accountability for damages or errors; public and private entities without scrutiny	Those harmed find no means of redress; incentives to ignore social impacts
Epistemological pluralism	Dominance of modern Western technical knowledge; invisibility of indigenous, Afro-descendant, and local knowledge	Impoverishment of cognitive diversity, imposition of foreign norms that may be harmful or inappropriate

In addition to the above, there are cross-cutting ethical challenges that hinder the robust implementation of artificial intelligence systems. A first obstacle lies in the disparity of technical resources and training, which manifests itself in a widespread lack of personnel specialized in algorithmic ethics and insufficient institutional capacity to assess socio-technological impacts. This situation is exacerbated by an incipient legal framework; despite the existence of instruments under development—such as Risk Analysis Matrices (RAM) or public policies in the design phase—specific regulations on ethical algorithmic governance are fragmented and lack effective oversight and enforcement mechanisms. There is also profound territorial, cultural, and linguistic inequality, with rural, indigenous, and Afro-descendant communities facing systemic barriers—including the digital divide, lack of language support, and limited recognition of their rights to data self-determination and cultural heritage—which perpetuate and exacerbate historical dynamics of exclusion. Finally, commercial and business pressure emerges as a fundamental obstacle, insofar as corporate imperatives of efficiency, profitability, and technological disruption often take precedence over ethical considerations, a tendency that is intensified in permissive regulatory environments and in the absence of substantial incentives for the adoption of responsible practices.

Identity in the data ecosystem

Artificial Intelligence redefines the notion of identity; the "digital self" is constructed and

advances through data, algorithms, and platforms that determine people's socioeconomic opportunities. This includes biometric features, ethnic/linguistic/cultural affiliations, socioeconomic histories, and political or gender self-identifications. Artificial Intelligence algorithms use these elements in classification, recognition, recommendation, or decision-making processes. They operate on representations of identity and, therefore, can transform, reinforce, or damage them.

This data economy introduces tensions with collective identities. In the dominant Western view, privacy is conceived as an individual right, and personal data is isolated to protect the autonomy of the subject. In fact, there are various laws in Latin American countries, which creates a complex regulatory landscape for companies operating in the region, making it essential to understand and comply with local laws (table 2).

Table 2. Legislation in South America on data protection

Country	Main Law	Year of Enactment	Supervisory Authority
Chile	Personal Data Protection Law (Law No. 19,628) (amended)[2]	2023[3]	Data Protection Agency (new)
Argentina[4]	Personal Data Protection Law (Law No. 25,326)	2000	National Directorate for Personal Data Protection (PDP)
Uruguay[5]	Personal Data Protection Law (Law No. 18,331)	2008	Regulatory and Control Unit for Personal Data (URCDP)
Mexico[6]	Federal Law on the Protection of Personal Data Held by Private Entities (LFPDPPP)	2010	National Institute for Transparency, Access to Information, and Protection of Personal Data
Peru[7]	Personal Data Protection Law (Law No. 29,733)	2011	Directorate General for Transparency, Access to Public Information, and Protection of Personal Data of the Ministry of Justice.
Colombia[8]	Statutory Law 1581	2012	Superintendency of Industry and Commerce
Brazil[9]	General Data Protection Law (LGPD)	2020	National Data Protection Authority (ANPD)
Ecuador[10]	Organic Law on Personal Data Protection (LOPDP)	2021	Superintendency of Data Protection

There is a clear trend in South America toward the adoption of modern and robust data protection laws, largely inspired by the European Union's General Data Protection Regulation (GDPR). Countries such as Argentina, Uruguay, and Brazil are leading the way, while Chile, Colombia, Ecuador, and Peru have established or recently updated legal frameworks.

However, in Latin American indigenous traditions, the notion of privacy is conceived differently.

[2]UNESCO. (2024, May 4). Chile launches a national AI policy and presents a draft law on AI following UNESCO recommendations. UNESCO.

[3]Original law of 1999. Substantial reform published in 2023

[4]Organization of American States https://www.oas.org/juridico/pdfs/arg_ley25326.pdf

[5]Official Information Center. https://www.impo.com.uy/bases/leyes/18331-2008

[6]Chamber of Deputies https://www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares

[7]Congress of Peru https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf

[8]Congress of the Republic (October 18, 2012) http://www.secretariasenado.gov,co/senado/basedoc/ley_1581_2012.html

[9]Ministry of Sport https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd

[10]UNESCO. (2025, June 11). Ecuador adopts first Code of Ethics for Artificial Intelligence (AI) in a public institution. UNESCO. Retrieved from https://www.unesco.org/es/articles/ecuador-adopta-primer-codigo-de-etica-de-inteligencia-artificial-ia-en-institucion-publica

For most indigenous peoples, individuality does not exist on its own; it is constructed and defined through relationships with the community, the territory, ancestors, and the spiritual world. As Piedra Alegria explains,[5] the indigenous culture of Sumak Kawsay understands human beings as an integral part of the community and nature. Individual identity is deeply intertwined with the identity of the community (the family, the clan, the tribe); the individual is not "I" but "we." The well-being of the collective take's priority over personal well-being. From this perspective, human "time and space" are communitized; privacy is not merely a personal reserve, but the way in which a community shares its living environment.[5] An Andean formulation states that "life can only be understood from the collective—sumak kamaña—", implying that privacy must be understood as a shared social way of being.[5]

This cultural difference is relevant in the application of artificial intelligence. An artificial intelligence system weighs resources based on *individual* data (energy use, health records, internet activity, etc.), preserving the privacy of each individual. But for rural or indigenous communities, identity is based on their relationship with the land, the extended family, and ancestral knowledge. For example, a health model based on mobile phone data may not capture the communication patterns of rural communities that rarely use smartphones. In other cases, the mass collection of images to train facial recognition algorithms can violate collective principles: these are neural networks that "learn" from faces and behaviors conceived by urban designers, rendering invisible the phenotypic traits of local populations.

The gap between conceptions of identity is also evident in open data and digital governance initiatives. The United States and Europe promote open data as a mechanism for transparency and citizen empowerment, but in Latin America there is concern that this approach favors academic or business elites without including social minorities. In response, various collectives[6] advocate for the data sovereignty of peoples, a decolonial approach that defends the right of indigenous communities to control how their cultural data is collected, stored, and used. The goal is to ensure that the digital identity of vulnerable groups is not co-opted or distorted by algorithms. In line with this, the European Union (2024) and regional bodies explicitly promote AI that is "human-centered, inclusive, and fair."

The combination of these elements creates a series of challenges that we will analyze separately, since the feeding of different forms of artificial intelligence can be generated through data sets, information, or instructions that reflect historical inequalities (underrepresentation of ethnic groups, dialects, facial morphologies, skin tones, communication styles), the models will produce predictions or classifications for those groups that are.[7] People's identities are "measured" poorly or in a distorted way; this would render them invisible (false negatives) or generate unfair exposure (false positives).

Therefore, all these elements, added to the conceptualization of identity in AI itself, pose challenges, as traditional human-centered notions of identity may not be sufficient in the contexts of Artificial Intelligence, raising questions about the implications of AI identity in social and practical settings.

Overall, addressing these challenges requires a multidisciplinary approach to optimize AI applications in identity management while ensuring alignment with stakeholder values and privacy concerns.

Technical and governance challenges

Another major challenge is the need for advanced hardware and standardized software to support AI-based IAM systems, which are essential for real-time threat detection and automated user provisioning.[8] In industrial environments, the implementation of AI-based IAM systems faces obstacles related to security, privacy, and continuous improvement, requiring robust solutions such as biometric and multi-factor authentication to enhance security measures.[9] Furthermore, the socio-technical design processes of AI systems often struggle to integrate the diverse values

of stakeholders, which is crucial for aligning AI systems with user needs and expectations. This challenge is compounded by difficulties in identifying and engaging stakeholders, as well as the practical complexities involved in embedding values into AI technologies.[7] Furthermore, AI-based authentication systems, while improving security through biometric recognition and anomaly detection, must address issues related to privacy-preserving authentication, such as federated learning and decentralized identity frameworks.[10]

Privacy concerns further compound these challenges, as the collection and use of personal data for identity verification may infringe on individual rights and raise surveillance issues.[4,11] Furthermore, the evolving nature of personal identity in the metaverse raises philosophical and legal questions about self-perception and the implications of multiple digital identities.[11]

Coloniality[11] and algorithmic power

The production of knowledge about AI is concentrated in global hegemonic centers. This reflects the "coloniality of knowledge" described by Aníbal Quijano[12] which refers to the coloniality of power as a global system of racial, economic, and cultural hierarchies that persist beyond formal colonialism.[6,13] In the context of AI, this coloniality manifests itself as a structural problem—the "problem of algorithmic coloniality"—which raises crucial questions: Who defines the problems that AI should solve? What knowledge is valued in its design? Who benefits from its innovations and who is excluded or harmed? In the algorithmic context, this logic manifests itself in the concentration of technological development in certain global positions, the extraction of data without consent, and the epistemic standardization of languages and cultural categories.[14]

Table 3. Fundamental Principles of Algorithmic Decoloniality

Principle	Definition	Implications for AI Development
Epistemic Justice	Recognition and equitable valuation of different knowledge systems, including ancestral and local knowledge.	Inclusion of diverse perspectives in development teams; validation of non-Western knowledge in algorithmic design.
Technological Sovereignty	The right of communities to decide on the technologies that affect their lives and to develop their own solutions.	Development of local technical capacities; promotion of technologies appropriate to specific contexts.
Pluriversality	Recognition of the coexistence of multiple worlds and realities, as opposed to Western universalism.	Design of flexible systems that can be adapted to different worldviews and cultural contexts.
Critical detachment	Ability to critically distance oneself from hegemonic frameworks in order to imagine alternatives.	Systematic questioning of cultural assumptions embedded in algorithms; exploration of non-Western design alternatives.

This analysis is based on the premise that worldviews are accumulated in culture and its history,[15] that these processes of rationalization are always influenced by the emotions, desires, dreams, and worldviews of scientists,[16] manifesting themselves in three colonialities: power, knowledge, and being. To understand colonialities, they intertwine and produce what is known as "algorithmic coloniality," which could be defined as the perpetuation of colonial hierarchies through the design, implementation, and governance of intelligent systems,[17] conceived as a structure integrated into the contemporary technological ecosystem and not merely as an "unwanted" side effect.[14]

Algorithmic Decoloniality is not a new set of technical principles, but rather a critical stance and a political-epistemic commitment.[18] It involves questioning how the entire life cycle of AI, from its conception and data collection to its training, deployment, and evaluation, reinforces

[11]It refers to the patterns of power established during colonialism that survive in the current order, shaping culture, work, intersubjective relationships, and knowledge production.

global power asymmetries, marginalizes local knowledge systems, and perpetuates extractive logics.

Instead, proposes a re-rooting of technologies in specific contexts, recognizing that there are no universal categories until the possible points of intersection and consensus between the various cultures that make up contemporary globalized culture are debated.[19] Algorithmic Decoloniality advocates for epistemic justice, which recognizes and values different forms of knowledge,[20] and for technological sovereignty, which ensures that communities have control over the technologies that affect their lives.

The analysis of artificial intelligence from a decolonial perspective has made it possible to identify fundamental problems in the structures of power, knowledge, and representation that underlie contemporary technological development. At the same time, critical universalism emerges as a complementary perspective that seeks to reconcile the necessary aspiration to shared ethical principles with the recognition of cultural and epistemic diversity.[21]

Critical universalism represents an evolution of traditional universalist thinking, as it does not impose Western values as absolute norms, but rather proposes a genuine intercultural dialogue to reconstruct the universal from the plurality of human experiences. As Santos points out,[15] this perspective "does not deny the idea of universality, but reconstructs it from the epistemologies of the South," recognizing that universal principles cannot arise from decontextualized abstractions, but from the reciprocal recognition of differences and the practice of cognitive justice.

Dimensions of Algorithmic Coloniality and Integrative Responses

Far from being a neutral technology, artificial intelligence reveals itself to be a cultural artifact deeply intertwined with historical power relations and persistent geopolitical asymmetries.[22] This complexity requires analytical approaches that transcend purely technical approaches in order to address the ethical, epistemic, and ontological dimensions of its development.

In the epistemic dimension, it is evident how certain hegemonic knowledge frameworks render local perspectives invisible,[23] generating what could be called "algorithmic epistemicide"[12] that excludes alternative conceptualizations, such as collective notions of privacy in indigenous communities. In response to this, both the decolonial approach and critical universalism agree on the need to broaden epistemological horizons, although they propose different, but potentially complementary, paths.

The data dimension manifests dynamics of contemporary extractivism where personal information is captured and monetized, creating representation gaps in training sets.[18] This results in systems with differentially poor performance for underrepresented populations, perpetuating structural exclusions. Both approaches converge in identifying this problem, although they emphasize different aspects of the solution.

In the workplace, there has been a profound transformation in employment patterns, with a significant reduction in traditional medium-skilled occupations in sectors such as manufacturing and logistics.[24,25] The international division of cognitive labor reproduces colonial hierarchies when lower value-added tasks are outsourced to regions with weaker labor protections.[26] This problem requires responses that combine universal protections with adaptations to specific contexts.

The infrastructure dimension reflects multiple technological dependencies and persistent challenges such as insufficient connectivity, limited access to advanced technology, and regional disparities in digital resources.[27,28] In higher education, for example, the effective integration of AI faces obstacles such as a lack of digital skills among educators and inadequate ICT

[12]It consists of killing, silencing, annihilating, or devaluing a system of knowledge. We argue that epistemicide occurs when epistemic injustices are persistent and systematic, and collectively act as a structured and systemic oppression of particular forms of knowledge.

infrastructure.[29] Addressing these gaps requires comprehensive public policies that combine robust technical standards with sensitivity to local conditions.

Finally, the identity dimension shows how algorithmic classification systems can reproduce stereotypes and generate systemic discrimination[30] against racialized groups[31,32] as evidenced by false positives in facial recognition that disproportionately affect indigenous, female, and Afro-descendant populations in Latin America.[33] The response to these challenges requires combining universal principles of non-discrimination with a deep understanding of the historical and cultural particularities of each context.

Addressing these gaps requires comprehensive public policies, investments in digital education, and collaborative efforts to ensure equitable access to the benefits of AI throughout the region, consolidating historical asymmetries.

Analysis of interrelationships

The interrelationship between algorithmic ethics, digital identity, and coloniality constitutes a complex web that defines the social impacts of artificial intelligence. Ethics, understood as a set of normative principles, cannot be separated from identity constructions or the historical structures that condition technological development.[22] In Latin America, this relationship manifests itself in a critical way, that is, AI systems, being designed predominantly from Eurocentric epistemologies, impose universal categories that collide with collective identities and local knowledge.[15,19] For example, the principles of privacy and autonomy, central to ethical frameworks such as Floridi's,[1] are insufficient to address the community notions of privacy present in indigenous peoples, where identity is constructed relationally with the territory and the community.[5] This tension shows that coloniality is not a mere addition, but a structural component that shapes ethics and identity in the algorithmic ecosystem.[14]

A comparative analysis of these three axes reveals significant points of convergence as well as fundamental divergences. Among the common points, the critique of technocratic universalism stands out. Both critical ethics and algorithmic decoloniality question the supposed neutrality of AI systems and denounce their capacity to reproduce inequalities.[12,34] Both approaches emphasize the need for justice, albeit from complementary angles, as algorithmic ethics advocates for distributive justice (mitigation of biases, equity in access), while decoloniality demands epistemic justice that recognizes and revalues subalternized knowledge.[20]

The main difference lies in their focus and scope. Predominant algorithmic ethics tends to operate within the system, proposing technical improvements and governance frameworks within existing paradigms.[35] In contrast, algorithmic decoloniality is a project of structural dismantling that questions the very foundations of knowledge and power in technoscience, advocating for technological sovereignty and pluriversality.[13]

Conceptual Synergies and Tensions

The articulation between ethics, identity, and decoloniality generates both promising synergies and irreconcilable tensions. A fundamental synergy is the potential of decoloniality to radicalize AI ethics. By incorporating decolonial critique, algorithmic ethics transcends its procedural focus and can address fundamental questions about who defines what is "good" or "fair" in a technological context.[18] For example, the principle of "do no harm" takes on a new dimension when interpreted as an obligation to avoid "algorithmic epistemicide".[15] However, profound tensions arise, particularly in the realm of implementation.

Data protection regulatory frameworks, inspired by the GDPR and listed in Table 2, are based on an individualistic notion of privacy and identity. This conflicts directly with the community-based views of indigenous peoples and with the decolonial principle of data

[13]It is a perspective that affirms that there are multiple possible worlds and different realities rather than a single imposed "universality."

sovereignty, which claims collective rights over information.[36] Overcoming this tension requires genuine dialogue that does not subordinate one perspective to the other, but rather generates creative syntheses, such as data governance frameworks that articulate individual consent with community authorization, ensuring that the ethical development of AI does not reinforce, but rather dismantles, colonial hierarchies of power, knowledge, and being.

In consideration of the relationships and details established in this chapter, some concrete strategies are outlined that aim to materialize the principles of algorithmic decoloniality in the Latin American context. These proposals represent a comprehensive framework for action that seeks to transform the current dynamics of technological coloniality.

An effort to articulate Multi-actor for the Transformation of the Artificial Intelligence Ecosystem, which denotes the complexity of the broad challenge that requires a systemic approach and involves all relevant actors from countries and institutions. As Santos points out,[15] the transformation of epistemic power structures requires an "ecology of knowledge" that mobilizes different forms of knowledge and action. In this sense, we propose a model of quadripartite governance that specifically articulates the role of universities, companies, governments, and continuous professional learning processes.

The development of a regulatory framework with its own approach. This should be a proposal for the creation of a "Framework Law on Artificial Intelligence for Latin America" that transcends purely technical approaches and explicitly incorporates the principles of epistemic justice, technological sovereignty, and pluriversality.[15] This legislation should be established from public services, following emerging models such as that proposed by,[19] built on the right to collective data sovereignty, particularly for indigenous peoples and local communities, establishing protocols for free, prior, and informed consent at the community level.[37]

Implementation of Public Innovation Laboratories with an Intercultural Perspective. The creation of a network of "Public and Community AI Laboratories" is recommended. These spaces would function as co-design centers where technicians, public officials, and community representatives develop contextualized algorithmic solutions. As Crawford[22] points out, the localization of technological development is essential to break epistemic dependencies. These laboratories would prioritize specific regional problems, such as early warning systems for natural disasters adapted to territories or medical diagnostic tools valid for genetically diverse populations.

Strengthening local technical capacities with a critical approach. It is imperative to develop specialized training programs in "Ethical Algorithm Auditing" at public universities in the region. These programs would train professionals capable of identifying structural biases and proposing alternatives from diverse epistemological frameworks. Following Ruha[34] training must combine solid technical skills with a deep understanding of the political dimensions of technological development.

CONCLUSIONS

Artificial intelligence in its current configuration functions as a device of contemporary coloniality that reproduces and amplifies historical hierarchies of power, knowledge, and being.[12,35] From a decolonial perspective, processes of "algorithmic epistemicide" are evident, silencing local knowledge and perpetuating structural inequalities.[14,18] In response to this, critical universalism offers an essential complement: rebuilding the notion of universality through genuine intercultural dialogue, where shared ethical principles emerge from reciprocity between opposing epistemologies.[15,21]

The analysis has highlighted two fundamental tensions: on the one hand, the need for distributive justice and procedural transparency in algorithmic design,[1] and on the other, the demand for epistemic justice and technological sovereignty for subalternized communities.[5,20] Only by articulating both approaches can the "vicious circle of algorithmic coloniality"

be broken: underrepresentation in data leads to discriminatory results, which reinforce socioeconomic exclusion and perpetuate the invisibility of non-hegemonic groups.[18,22]

The analysis developed throughout this chapter leads to the conclusion that artificial intelligence, in its current configuration, often operates as a device of contemporary coloniality, reproducing and amplifying historical hierarchies of power, knowledge, and being. Conventional algorithmic ethics, which is predominantly abstract and universalist in nature, has proven insufficient to address these structural challenges, as it tends to mask its own cultural biases under an appearance of technical neutrality. Given this situation, there is a pressing need for a transformative political-technological project that, far from falling into fragmentary relativism, is based on Critical Universalism. This universalism does not impose Western values as absolute norms, but is continually reconstructed through genuine intercultural dialogue and the recognition of the pluriversality of worlds and knowledge. In closing, the following main recommendations are presented, conceived as a comprehensive framework for action for ethical, fair, decolonial, and critically universal AI governance.

Adoption of a Critical Universalist Governance Framework

It is imperative to move towards a governance model that dialectically articulates decolonial criticism with Critical Universalism. This implies that public policies and regulatory instruments must emerge from a creative synthesis between indispensable epistemic justice—which revalues subaltern knowledge—and the aspiration to shared ethical principles, reconstructed from the plurality of human experiences. The goal is to avoid both the imposition of abstract universalism and fragmentation into incommensurable relativisms, moving toward regulatory frameworks that are both globally relevant and locally meaningful.

Implementation of an Impact Assessment

When deploying high-risk Artificial Intelligence systems, an Impact Assessment must integrate two dimensions: one, decolonial, using participatory methodologies to assess impacts on cognitive justice and collective identities; and the other, critically universal, ensuring compliance with fundamental thresholds of distributive justice and non-maleficence, defined through intercultural dialogue.[19] This approach follows the guidelines , but radicalizes them by explicitly incorporating the productive tension between the local and the universal.

Development of Data Sovereignty Mechanisms

It is crucial to develop data sovereignty frameworks that operationalize both individual rights, a central concept in human rights charters, and collective rights over data and knowledge, which are characteristic of many worldviews in the region. This involves creating dual governance systems that articulate individual informed consent with community authorization and control protocols. At the same time, the harmonization of regional standards must seek a common ethical floor (concrete universalism) that avoids "race to the bottom"[14] and protects the region from data extractivism, as analyzed by Couldry and Mejias.[18]

Promotion of Intercultural Co-Creation

Create spaces for public and community experimentation and innovation. These spaces should function as agoras for "knowledge dialogue" where, through intercultural co-creation, contextualized algorithmic solutions are negotiated and constructed. In these spaces, technical-scientific knowledge and ancestral knowledge will meet on an epistemic equal footing, thus practicing universalism not as an imposition, but as a collective and negotiated construction.

[14]It is an economic and political concept that describes a negative competitive dynamic in which different countries, regions, or companies seek to attract investment or economic activity by progressively relaxing their regulatory standards, social protections, wages, or, in this context, their ethical principles.

Strengthening Academic Training

Higher education must incorporate the teaching of algorithmic ethics, decoloniality, and critical universalism as frameworks in dialogue and tension. It is necessary to train professionals who, in addition to technical skills, possess the critical capacity to navigate this complexity: capable of deconstructing the colonial assumptions of technoscience, but also of participating in the construction of universal principles from a position of difference. This requires a new type of literacy that is technically, ethically, and politically sophisticated.

Establishment of Technological Diplomacy

Given the asymmetry of geopolitical power, we must act in concert. This implies establishing regional agreements on foreign policy and global governance that allow for collective negotiation with the major poles of technological power. The objective would be to co-define, from a position of collective strength, global standards that reflect a truly pluralistic and non-hegemonic universalism, creating a bloc capable of influencing the global governance of AI in line with the interests and values of the region.

Decolonizing artificial intelligence in Latin America, in light of Critical Universalism, reveals itself as a project that transcends mere resistance. It is an affirmative construction effort that will attempt to participate in the very redefinition of what we consider universally valuable in the digital age. It involves the construction of full technological citizenship, where the peoples of the region are not only protectors of their knowledge, but also co-architects of the ethical principles that will guide the global technological future. The path outlined by these recommendations is complex and will be fraught with productive tensions between the local and the global, the particular and the universal. However, continuing on the current path of uncritical and dependent adoption carries the undeniable risk of consolidating new and more sophisticated forms of colonialism. The task is arduous, but it is essential to ensure that artificial intelligence effectively serves to build a more just, diverse, sovereign, and genuinely universal future for our hemisphere.

BIBLIOGRAPHIC REFERENCES

1. Floridi L. The ethics of artificial intelligence: principles, challenges, and opportunities. Oxford: Oxford University Press; 2023.

2. UNESCO. Chile lanza una política nacional de IA y presenta un proyecto de ley sobre IA. 2025. Disponible en: https://www.unesco.org/es/articles/chile-lanza-una-politica-nacional-de-ia-y-presenta-un-proyecto-de-ley-sobre-ia-siguiendo-las

3. Ruiz SD. La revolución silenciosa: inteligencia artificial, justicia social y cambio comunitario. Naturaleza y Sociedad. Desafíos Medioambientales. 2025;213–23.

4. Mittelstadt B. Principles alone cannot guarantee ethical AI. Nat Mach Intell. 2019;1:501–7.

5. Piedra-Alegría J. Descolonizando la "Ética de la Inteligencia Artificial". Dilemata. 2022;247–58.

6. Wong PH. Cultural differences as excuses? Human rights and cultural values in global ethics and governance of AI. Philos Technol. 2020;33:705–15.

7. Sadek M, Mougenot C. Challenges in value-sensitive AI design: insights from AI practitioner interviews. Int J Hum Comput Interact. 2024;1–18.

8. Muppa KR. Enhanced identity and access management with artificial intelligence. Int J Inf Secur Cybercrime. 2024;9–17.

9. Vegas J, Llamas C. Opportunities and challenges of artificial intelligence applied to identity and access management in industrial environments. Future Internet. 2024;16.

10. Mohammed D, MacLennan H. Secure authentication and identity management with AI. In: Advances in Computational Intelligence and Robotics. 2025. p. 271–306.

11. Mitrushchenkova AN. Personal identity in the metaverse: challenges and risks. Kutafin Law Rev. 2023;10:793–817.

12. Quijano A. Coloniality of power, Eurocentrism, and Latin America. Nepantla Views South. 2020;533–80.

13. Cave S. The problem with intelligence: its value-laden history and the future of AI. Proc Natl Conf Artif Intell. 2020;29–35.

14. Mohamed S, Png MT, Isaac W. Decolonial AI: decolonial theory as sociotechnical foresight. Philos Technol. 2020;33:659–84.

15. Santos B de S. The end of the cognitive empire. Durham: Duke University Press; 2018.

16. Harding S. Objectivity and diversity: another logic of scientific research. Chicago: University of Chicago Press; 2016.

17. Salmi J. A democratic way of controlling artificial general intelligence. AI Soc. 2023;38:1785–91.

18. Couldry N, Mejias UA. The costs of connection. Stanford: Stanford University Press; 2019.

19. Eke D, Chavarriaga R, Stahl B. Decoloniality impact assessment for AI. AI Soc. 2025.

20. Fricker M. Epistemic injustice: power and the ethics of knowing. Oxford: Oxford University Press; 2007.

21. Dussel E. Filosofías del Sur. México: Akal; 2022.

22. Crawford K. The atlas of AI: power, politics, and the planetary costs of artificial intelligence. New Haven: Yale University Press; 2021.

23. Vesna V. Towards a decolonial I in AI and society. AI Soc. 2024:6–5.

24. García Marengo SA. ¿Por qué la IA generará una crisis del empleo en América Latina y cómo enfrentarla? Polit Int. 2023.

25. Liang Y. The impact of artificial intelligence on employment and income distribution. J Educ Humanit Soc Sci. 2024.

26. Tubaro P, Casilli AA, Coville M. The trainer, the verifier, the imitator: human platform

labour and AI. Big Data Soc. 2020;7:1–15.

27. Siatan MS, Gustiyana S, Nurfitriani S. Infrastructure development and regional disparities. KnE Soc Sci. 2024;799–806.

28. Marian Sinaí OC. Análisis multidimensional de la brecha digital en Venezuela. Prohominum. 2024;49–59.

29. Serafim A, Fernandes SDV, Mesquita C, Veloso CM, Sousa BB. Artificial intelligence in higher education. In: Innovations and challenges in student engagement. 2025. p. 153–76.

30. Falangola RdF, Lima FPLD, Castro DFD, Gomes CLP, Vaz P, Santos RP. Direito antidiscriminatório e algoritmos. Aracê. 2025;e8368.

31. Terrones AL, Bernardi MR. El valor de la ética aplicada en ingeniería en un horizonte de IA confiable. Sophia. 2024.

32. Booker MD, Booker FC. The name game: algorithmic gatekeeping in digital hiring. Int J Res Innov Soc Sci. 2022;2210–23.

33. Kassam A, Marino P. Algorithmic racial discrimination: a social impact approach. Fem Philos Q. 2022; doi:10.5206/fpq/2022.3/4.14275.

34. Buolamwini R. Race after technology: abolitionist tools for the new Jim Code. Cambridge: MIT Press; 2019.

35. Jobin A, Lenca M, Vayena E. The global landscape of AI ethics guidelines. Nat Mach Intell. 2019;1:389–99.

36. Oliveira NH. Uma teoria crítica decolonial da inteligência artificial. Public Consultation. 2024;1–18.

37. Hummel P, Braun M, Tretter M, Dabrock P. Data sovereignty: a review. Big Data Soc. 2021;8:1–15.

FUNDING

None.

CONFLICT OF INTEREST STATEMENT

None.

AUTHORSHIP CONTRIBUTION

Conceptualization: René Ernesto Esquivel Gaón
Data curation: René Ernesto Esquivel Gaón
Formal analysis: René Ernesto Esquivel Gaón
Research: René Ernesto Esquivel Gaón
Methodology: René Ernesto Esquivel Gaón
Project management: René Ernesto Esquivel Gaón
Resources: René Ernesto Esquivel Gaón
Software: René Ernesto Esquivel Gaón

Supervision: René Ernesto Esquivel Gaón
Validation: René Ernesto Esquivel Gaón
Visualization: René Ernesto Esquivel Gaón
Writing - original draft: René Ernesto Esquivel Gaón
Writing - correction and editing: René Ernesto Esquivel Gaón.

USE OF ARTIFICIAL INTELLIGENCE

In preparing this chapter, generative artificial intelligence tools were used to assist with certain tasks. Specifically, large language models (LLMs) were used for refinement of wording and style, as well as concept synthesis.