Unifya

ISSN : XXXX-XXXX | Vol 1, Issue 1, Oct – Dec, 2025

PUBLISHED BY
ERUDEXA PUBLISHING

Original Article

Received: 18 Oct 2025 | Accepted: 16 Nov 2025 |
Published: 19 Nov 2025

The Impact of Artificial Intelligence on Digital Identity, Privacy, and Personal Representation

Hanae Belhassani*

*National school of Applied Sciences. University Mohammed Premier. Oujda

Abstract

The advent of artificial intelligence in the digital age has presented demographic changes in the ways individuals construct, showcase, and sustain their online identities. This article investigates problematics related to identity, privacy, and personal representation in the context of AI, with a particular focus on how technology has fundamentally altered our engagement with these online platforms. To this end, we review the relevant literature that discusses AI's impact on the construction of online identities, ethical implications of AI surveillance systems and data privacy, and how AI systems (e.g., social media algorithms, facial recognition technologies) influence an individual's agency and self-conception within the digital space. By bringing together different shades of theoretical perspectives, this article will provide a comprehensive understanding of the evolving space between technology and the self and its implications for ethics as well as conceptualizing digital identity.

Keywords: Artificial Intelligence, Digital Identity, Privacy, Personal Representation, Ethics

1. Introduction and Background

1.1 The Impact of AI on Digital Identity

The rise of Artificial Intelligence (AI) has profoundly impacted a number of sectors, including alterations in human relationships, changes in economic structures, and shifts in social norms. The emergence of AI technologies within the scope of digital identity has become a focal point of research in recent years. Digital identity consists of many parts, including personal information/data, online actions, social media, and biometric indicators; and as an increasing number of people use AI systems to create, manage, or employ their digital identity, it is time to examine the implications of these changes imposed by AI, particularly in terms of privacy, security, and evolving social representation in online platforms.

The introduction of Artificial Intelligence (AI) has significantly influenced many industries and altered how people relate to one another, how economies operate, and how people interact socially. (...) These disruptions require rigorous conceptual clarity. In this paper, artificial intelligence (AI) means systems and technologies that replicate human cognition, programmed to learn from data, recognize patterns, and decide with little or no human involvement. Digital identity means the bundle of personal data, behavioral patterns, and digital artifacts that shape a person's presence and impression online. Personal representation is how individuals choose to display and construct aspects of their identity within digital environments, influenced by their actions and mediated by algorithms that set boundaries for visibility and interaction.

Despite the many ways that AI allows both personalization and self-representation, the impact of the rise of AI has brought many opportunities and challenges. AI-based services and websites enable users to curate digital identities that represent their aims and self-representation. AI facilitates a way for a user to engage and traverse online platforms, through the use of large processed data, to experience a more customized digital allure and information retrieval ecosystem. While these AI services provide compelling functionality, the proliferation of AI use brings the dangers of privacy and data protection into question. As AI systems have begun processing personal information on a scale never seen before, we have seen the commodification, indeed marketization, of personal data for profit, without regard to the privacy and ownership rights of personal data.

Beyond biases, digital identity management involving Artificial Intelligence raises significant security threats. Emerging biometric identification with advanced identity verification has greater potential for authentication, but it also encourages identity theft. Techniques involving AI (for example deep learning and neural networks) can easily facilitate identity theft—such as building synthetic identities, hacking security systems, or appropriating the verified identifiers—resulting in new opportunities for unauthorized access and unintended use. In addition to malicious actors, it is important to recognize the attitudes associated with inherent systems bias within artificial intelligence. AI is trained with prior data that reflects the attitudes associated with the data that produced it, and systematic approaches often replicated systemic biases that have been trained within their identity constructs. These attitudes often translate into discriminatory characteristics that unequal treatment is based on—and perpetuating discrimination based off of digitalized, construct identity. This situation indicates a clear need to create viable security policies that protect personal data and sensitive information.

Similarly, artificial intelligence is altering representations of individuals in digital spaces which presents a challenge to the conceptualization of individualized authenticity. The evolution of unique digital identities highlights the compelling debates surrounding algorithmic influences and the diminishing agency of the individual. Algorithms continue to dictate elements of interactions, leading perspectives regarding who "actually" represents the individual user becoming complicated. AI's potential to develop hyper-realistic synthetic identities risks to raise ethical controversies that surround deception, depersonalization, and the individual’s integrity over their digital image. To discern the foregoing relationships involves an interdisciplinary view incorporating information technology, ethics, law, and sociology.

1.2 Research Objectives and Scope

As the implications of artificial intelligence (AI) technologies become more intertwined with digital infrastructures, it is imperative to examine the relationship they have to privacy, security, and personal representation. In this section, I will clarify the boundaries of this research project and outline its intended focus: to evaluate the monumental role of AI in the construction of digital identities and to consider the accompanying implications for data privacy and agency and the ethics of algorithmic governance around online self-representation.

Digital identity references the multifaceted assortment of data, actions, and digital artifacts that make up how a person is conceived and represented on the internet. This includes usernames, profile pictures, activity logs, items shared, biometric information, and behavioral markers such as browsing patterns or items used on the device. With the increased use of digital platforms for social, political, and economic places, digital identities are becoming less static and voluntary constructs (or there are fewer opportunities to exist after a digital identity) as they are modified in real time and subject to the influence of algorithmic actions that mediate how they are classified, perceived, and treated digitally.

AI is a vital part of this issue. While various techniques such as machine learning and data mining enable AI to sort through copious amounts of user-generated content and provide digital experiences tailored to individual desires, for better or worse, these refined user experiences accelerate the ethical concerns with surveillance, data commodification, and algorithmic bias. In light of recent advancements in AI's algorithms used in social media and e-commerce (Manheim & Kaplan, 2019), targeting has become operationally better while the institutionalization of private data surveillance is deeper (and often without informed consent).

The most troubling ramification of AI upon the construction of digital identity is the loss of privacy. AI-driven tracking programs have ushered in the possibility of extracting, pulling from, and aggregating personal information across various platforms into data portraits that may not just replicate previous activity but also predict future behavior. While remarkable, these predictive features extend the limitations of informational self-determination while simultaneously introducing new lawsuits to autonomy and privacy.

The dangers posed by AI advancements do not stop at threats to privacy. AI technologies are rapidly moving into the forefront of authentication and identity verification mechanisms, and the implications of a compromised data breach in an AI system are dramatically more serious. There is a risk that bad actors will leverage AI to create artificial synthetic identities or engage in deep-learning piracy to breach secured systems. Additionally, given that algorithmic decision-making systems often rely on training data that is biased, using AI technologies in the governance over digital identities creates the likelihood of users being unfairly profiled or remaining excluded from services, reinforcing social inequity within digital contexts.

Ultimately, the impact of AI on identity does not end with potential security risks, as AI helps to define the manner in which identity is represented and performed. On-platform actors are then profiled for visibility based on user actions online, such as clicking, sharing, or liking, by means of its recommendation algorithms, prioritization systems, and moderation systems that identify what portions of your identity are made visible—and which go unnoticed, perhaps even silenced. In the mixing of these diverse identities as represented digitally, AI may uniform or convolute the multiplicity of human experience, prioritizing alignment over authenticity and metrics tied to engagement instead of expression.

In this context, this study will be a multidisciplinary critique into ways that the introduction of artificial intelligence has disrupted the construction, perception, and governance of digital identity. In particular, this critique seeks to explore the possibility of agency in an algorithmically mediated space and to explore how regulatory, organizational, and ethical frameworks might evolve to help support the protection of fundamental rights within the digital environment.

2. Privacy and Security Challenges

2.1 AI, Privacy Erosion, and Ethical Concerns in Surveillance

The concept of privacy in the digital age is increasingly complex, especially in the light of the rapid advances of artificial intelligence (AI). AI systems analyze and process vast amounts of personal data, often exploiting the information that individuals may not even consciously recognize as part of their digital footprint. As a result, the mechanisms that support AI technologies such as machine learning and natural language processing algorithms introduced significant challenges for the notion of privacy, often undermining the individual rights that were traditionally protected in various legal structures (Murdoch, 2021).

The widespread use of AI systems raises critical questions about the informed consent and the transparency of data collection processes. Users often get involved with platforms without fully understanding to what extent their personal information is harvested and used. For example, social media platforms, e -commerce sites and research mechanisms use algorithms that accompany the behavior, preferences and user interactions to create profiles that are used for personalized marketing and information dissemination. This phenomenon is even more worrying because the information derived from these profiles can usually be reused beyond the original intention of data collection. This leads to potential misalignment between user's privacy expectations and the realities of AI driven data use.

In addition, personal data aggregation promotes an environment in which individual identities can be commodified. AI systems are able to link disparate data points to build comprehensive users' profiles that can be sold to third parties or used for targeted advertising. This transactional nature of personal data not only undermines individual's autonomy over their own information, but also increases vulnerabilities to identity theft, fraud and other malicious actions (Murdoch, 2021). As the digital scenario becomes increasingly intertwined with these AI infused practices, the effectiveness of existing privacy protections, often rooted in pre-digital contexts, is increasingly questioned.

The implications of these technological transformations extend beyond individual concerns, as they also raise broader social issues regarding surveillance and normalization of data monitoring. Governments and corporations can employ AI systems to monitor public behaviors and meetings, resulting in the intersection of personal privacy rights and state security interests. Confidence in AI in surveillance operations not only amplifies invasive supervision potential, but can also perpetuate systemic biases that affect disproportionate marginalized communities. As data is collected, analyzed and agided, the risk of reinforcing existing social inequalities becomes a pressing concern, bringing to light the ethical implications that accompany AI technologies.

By addressing the dynamics of privacy change in the digital age, it is evident that the traditional notions of control over personal information are being eroded. This erosion is aggravated by the rapid pace of technological advancement, which surpasses the ability of regulatory structures to adapt to new developments. The impact of AI on digital identity in relation to privacy requires a reassessment of controls and regulations around personal information. Consequently, as AI continues to evolve and shape the contours of digital interactions, stakeholders should deal with the need for more robust privacy protections that recognize the power of AI technologies and the rights of individuals to maintain control over their own digital identities.

2.2 Security Vulnerabilities in AI Systems

The incorporation of artificial intelligence (AI) into digital identity structures creates improvements but also risks—especially in the field of cybersecurity. On the one hand, AI can improve the functioning of authentication and allow organizations and individuals to detect threats to their digital identities in real-time. On the other hand, the integration of AI opens up personal data to novel vulnerabilities. Organizations are using AI with greater frequency to manage identity verification, access control, and biometric identification, and in doing so, organizations are expanding the attack surface for those with malicious intent as a result of the complexity and scale of these systems.

By design, AI requires a massive amount of personal data to be collected and processed. This presents a quandary: the more data that an AI uses to fulfill its intended purpose, the more severe the ramifications from a data breach. Braun et al. (2018) clearly articulated the potential effects that breaches of AI-enabled systems have, which could include thousands or millions of individuals. Breaches of AI-enabled systems are particularly concerning when the compromised data is sensitive (e.g. facial scans, fingerprints) or unique (i.e., behavioral data). Risks related to biometric data are particularly concerning because, unlike passwords, compromised biometric data cannot simply be changed.

While AI systems can help individuals defend against cybersecurity threats, they are also bringing new challenges to digital security via their use in cyberattack strategies. Cybercriminals are increasingly leveraging AI technologies to automate phishing attacks, replicate legitimate identities, and exploit vulnerabilities in authentication systems. An emerging avenue for adversarial AI techniques is to subtly manipulate AI algorithms (i.e., input test data) to fool machine learning-based models to bypass security verification systems. Evolving attack techniques such as these are at times moving more rapidly than attack detection systems can mitigate, so it is essential to rethink digital identity programs as ecosystem-focused security solutions powered by adaptive and AI-aware security measures.

Another stakeholder concern is about AI-based access control systems. Biometric-based authentication systems (i.e., facial features, voice characteristics) can potentially improve user experience and security but can expose ethical and practical risks. A compromise of a biometric identifier is much more impactful, mainly because biometric identifiers cannot be replaced if exposed (i.e., we have DNA, fingerprints, and facial photographs for life). Further, facial recognition technologies have been shown to perform differentially across subgroups, including misidentifying people from marginalized communities. The technical and ethical risks associated with viewing users' identities on behavior profiles establish a critical need for transparency, accuracy measurements, and regulation when using AI-based identification systems.

AI may also present further risk when one observes surveillance and behavioral profiling. Identity management platforms that observe user behavior across numerous websites and applications can be used to develop an even more effective behavioral profile about the individual, which means the individual may not only lose autonomy over their actions, but provide uses for that data that could be cause harm. When AI-based systems that use location services, browsing habits, or social connections are created, they created derivative understandings not only to violate individuals' privacy but also to use the knowledge for discrimination. In practice, the end result of that analytics is often focused on predicting future criminality (predictive policing) or excluding users from bankers' or financiers' choices.

Addressing these risks is a complicated process requiring both organizational governance and citizenship. Organizations must incorporate more than just technical solutions; they must incorporate ethical data governance practices as principles of consent, data minimization, and regular security assessments as evidence of cultural and ethical behaviors accountable as organizations. At the same time, citizenship awareness and digital literacy must be developed further to empower users to both recognize the nature of risk dealing with AI-based identity systems and account for risks of their actions when dealing with their data and to render decisions for themselves as informed consumers and individuals.

In sum, while AI technologies offer considerable opportunity to enhance digital security, they also enhance the existing vulnerabilities of existing frameworks to provide protection. Addressing the identifiable risks associated with both behavior profiling and AI requires rivals of both future technological innovation and cultures of institutional accountability to derive standards of identity systems that account for users' safety, agency and trust.

3. Ethical and Societal Implications

3.1 Algorithmic Bias and Digital Representation

Perhaps the most fundamental ethical quandary facing artificial intelligence (AI) systems is that of algorithmic bias. Algorithmic bias generally occurs as a result of the data used to train AI models. If the training data represents historical injustice, cultural bias, or demographic underrepresentation, then the AI will reinforce and perhaps exacerbate those forms of discrimination. This creates market segmentation in the interfaces, affordances, and identities represented within digital systems.

Facial recognition technologies illustrate this issue plainly. Cumulative research in computer vision has found that facial recognition systems exhibit bias towards individuals from marginalized communities, particularly women and individuals of color. For instance, Buolamwini and Gebru (2018) find that commercial facial analysis systems systematically misidentify women of color in their datasets at far higher rates than white men. Some mistakes are not merely technical errors—they violate our right to fair and equal treatment in digital spaces and threaten the stability of individual identity.

Additionally, AI systems do not simply misidentify identity—they also potentially shape our identities as they are made and remade online. Algorithmic functions of social media, search engines, and recommendation systems shape what a person sees and interacts with, which voices get the most amplification, and which voices get silenced. Gillespie (2018) writes that algorithmic curation significantly shapes both our perceptions of ourselves as individuals and the amount of social recognition we receive. In a multitude of scenarios, users may conform their online identity to the dominant norms of social media or the more “algorithm-friendly” version of themselves in order to be seen or receive validation. This does a disservice to authentic self-expression.

The ethical issues expand exponentially when those adverse implications stemming from algorithmic bias result in problems of access in the real world (e.g. jobs, education, health care, legal). For instance, hiring algorithms rooted in bias could systematically further discriminate against women or individuals from lower socio-economic strata (O'Neil, 2016). In these situations, digital identities shaped through AI systems as tools of exclusion would eliminate any potential forms of empowerment.

In the Moroccan context, where there are already significant social disparities, unchecked AI systems could only serve to exacerbate systemic discrimination. These technologies, aided by a lack of transparency and governance, could merely reproduce colonial legacies of non-transparent and inequitable treatment across historically gendered as well as class-based forms of social ordering evident within digital infrastructures.

Ultimately, algorithmic bias is not a technical issue; it is a socio-political issue. Solutions will include inclusive design practice, transparent data practices, and ongoing and regular audits of decisions made by AI. More importantly, it will require existing disadvantaged communities to be granted agency in how the technologies that affect and represent their identities are constituted. In order to maintain the relationship at the core of practice within algorithmic systems of fairness and accountability to preserve the integrity of digital identity and equitable digital futures.

3.1.1 Systemic Discrimination in Moroccan AI Applications

In Morocco, artificial intelligence has begun to permeate key industry sectors, including recruitment, justice, health, and finance; this raises serious issues of systemic discrimination. Algorithms tout a degree of efficiency and objectivity, but they invariably embed existing social stratification biases lurking in the data and assumptions that technology captures or replicates what was collected. For Morocco, a nation of extreme socioeconomic disparity and imbalance, the use of AI without some institutional mechanisms is likely to reinforce or repeat historical forms of exclusion.

For example, in recruitment, companies are increasingly using AI recruitment technology to narrow candidates down to a manageable level quickly. Commonly used as an input into a recruitment funnel, hiring technology will often rely upon large datasets; machine learning will typically rely on training data collected from other recruitment processes. If previous recruitment processes have already privileged certain identity constructs—typically urban males and, often, elitist academic institutions—the inertia of this algorithmic decision-making becomes multiplied over time and results in systemic exclusion of women, applicants from rural areas, and ethnic minorities. As Benhmama and Bennani (2024) point out, once we become reliant on automated decisions based on historical discrimination, systematic discrimination becomes institutionalized.

The potential for bias and discrimination is not limited to employers and recruitment. For example, in law enforcement, the use of predictive policing technologies skews surveillance towards specific communities based on historical crime data that also reflects a history of discrimination against targeted groups. In 2024, the Moroccan insurance sector also exhibited bias in pricing analysis based on demographic factors, thus marginalizing and charging higher premiums to individuals from poor or rural backgrounds based on demographic factors that had no relation to the individual's behavior. In health, some segments of the population remain and are not covered in training datasets, while other populations may be misdiagnosed or even denied based on typical data received by AI. Finally, in a sophisticated finance ecosystem, some risk-scoring algorithms will discriminate against individuals with limited or genuinely non-traditional banking experience and refuse loans despite more predictable behavior.

As illustrated, the following table summarizes the key sectors in Morocco with algorithmic bias, the forms of discrimination, the vulnerable populations being discriminated against, and the consequences.

Table 1. Manifestations of algorithmic bias across key sectors in Morocco

Sector	Type of Algorithmic Bias	Affected Groups	Consequences
Recruitment	Replication of biased historical hiring data	Women, rural applicants, ethnic minorities	Systemic exclusion, limited access to job opportunities
Law Enforcement	Predictive policing based on overrepresented data	Youth, low-income urban populations	Over-policing, mistrust in legal institutions
Car Insurance	Risk profiling based on location and demographic	Low-income residents, linguistic minorities	Unjustified rate increases, restricted access to basic services
Healthcare	Diagnostic tools trained on non-diverse datasets	Women in rural areas, Amazigh communities	Misdiagnoses, unequal treatment, medical exclusion
Finance Credit	Credit scoring based on traditional financial history	Youth, unbanked populations, working-class groups	Restricted access to loans, deepening of financial precarity

The forms of bias cited here above are not single occurrences but are part of a larger pattern that connects algorithmic systems to systemic inequalities. If algorithms are to function without forces of transparency, inclusivity, or oversight, they will continue to operate as furthering inequality instead of equity. Moreover, the lack of diverse representation in the development and testing of algorithmic systems will continue to make certain communities invisible while skewing the digital identity that we have created value for.

Within the Moroccan context in which regional equity, gender inequality, and linguistic marginalization already existed, the challenge of algorithmic bias adds additional risk. Resolving this challenge will require not only technical audits but also legal and ethical frameworks that promote equity, protect vulnerable people, and promote ethical AI that values the contributions of a more inclusive society instead of exacerbating divides in society.

3.1.2 Exclusion of marginalized voices and design bias in AI Systems

In addition to algorithmic bias in outputs, another troubling and frequently overlooked issue occurs in the design stage of AI systems. The exclusion of marginalized voices at the design stage represents an even more pervasive design bias than can be found in algorithmic outcomes themselves. To put it plainly, when technological tools are developed without the participation of marginalized communities, people from those communities will always be the "test" against which the product was not designed. Even if AI systems do not intentionally discriminate against individuals from marginalized communities, the perspectives and experiences of the designers will necessarily be shaped by the experiences of the designers' own community.

A well-documented case of this exclusion is facial recognition technology. Studies show that these systems are routinely misclassifying racial minorities and gender-diverse persons. Buolamwini and Gebru's (2018) study of facial recognition software indicated the software assumed the gender identity of darker-skinned women and misidentified them as much as 34.7% of the time when it used classification systems of lighter-skinned men at rates of 0% or less than 1%, respectively. The documented cases of misclassification are not merely a technical error but rather indicative of deep exclusion from the training data and design practices. For those excluded, the consequences can include wrongful arrests, lowered service, or a refusal to trust AI-based applications due to systemic marginalization.

Design bias, particularly as it relates to the potential for participatory practices, relates to community design that was never included in the design phase of digital applications in the first place. Costanza-Chock (2018) describes inclusive, or 'design justice,' as a practice that is not inherently focused on participatory processes. Community involvement in the design of digital applications could help create new dynamics to nullify the systematic inequalities built into the form of physical and digital tools. Within the scope of Morocco, the issue of marginalization in AI is particularly acute as rural populations and linguistic minorities remain absent in datasets, pilot studies, and similar programs, and in policy discussions about digital innovation. Gender-diverse voices are frequently absent as well.

The effects of such exclusion are not just symbolic but substantive harms. For example, there are challenges that transgender and non-binary folks experience using AI-powered voice assistants or identity verification that depend on binary genders, and as Streette, Keyes, and Cath (2021) explained, these voice recognition systems can fail or misinterpret their voices, leading to frustration, misgendering, and, in some cases, leaving them unable to access necessary digital services.

To reduce these barriers and negative consequences, participatory and inclusive practices must be put in place throughout the AI design cycle, from ideation and data set choices to testing, deployment, and governance. Participatory design with community co-design workshops, adapting from feedback, and user testing that includes marginalized groups will collectively reflect the diversity of users in the world. Buddemeyer et al. (2022) further emphasize that even when fair design practices improve design, involving usually excluded groups will help develop trust in the design process and engagement with the user.

Audits and accountability also matter. Inclusive is not a one-time project; it is a consistent practice of ethically and fearlessly critiquing and developing with institutional support. Developers and policymakers must shift their mindset from 'product' concerning AI design to a more inclusive one of people, where the legitimacy of AI systems should depend on equality for all the engaged members of society.

In short, excluding marginalized voices from the design process of artificial intelligence systems is a structural flaw. Inclusivity directly reduces both the functionality and legitimacy of AI systems. A continuous commitment to participatory, transparent, and justice-inclusive design will create real inclusive technologies empowering all users.

3.2 Ethical Frameworks for AI and Digital Identity

The rapid transformation of artificial intelligence (AI) technologies has redefined the way digital identities are created, mediated, and regulated. As AI systems progressively interfere in shaping what is seen, known, and remembered about individuals in digital contexts, the ethical issues of transparency, responsibility, and consent have moved from a secondary consideration to a primary one.

Transparency is the user's ability to know when and how AI systems operate, which is complicated when personal data is the input. Many AI algorithms are not explainable or visible to the individual being affected by them. Users usually consent to a set of terms of service without cognizance of data being collected, analyzed, or commercialized. As Müller (2020) points out, when algorithmic systems are opaque, it undermines trust as a strong force, rendering users powerless to understand or question a decision made for them. If transparency does not advance, the idea of digital identity may become something that is performed for users rather than co-constructed with them.

Responsibility is equally important. As the role of making individual decisions in AI systems grows increasingly autonomous, it becomes more difficult to ascertain who is responsible for errors or harm derived from decisions. If a digital identity is misclassified by a facial recognition system or barred from an experience due to an AI-generated risk score, who is to be held responsible—the developer, the platform, or the data provider? Müller (2020) states responsibility must be shared equally among all actors embedded in AI governance. This capacity must include some combination of technical control, including auditability, as well as legal authorities that enable users to challenge decisions and seek restitution for harm or losses. Without this capacity, algorithmic injustice can (and will) be couched in the distance of complexity.

Perhaps most importantly, we must redefine the idea of user consent for the age of AI. Traditional models of consent—even static checkboxes or unread policy statements—are entirely insufficient in contexts where AI systems change, learn, and repurpose data over time. Meaningful consent considers not only what data is collected and for what purpose, but also users' ability to withdraw, modify, or limit that consent as contexts change. Consent in this way should be conceived of as a dynamic, participatory process rather than a one-time contractual agreement. Users should own and control the authorship of their own digital life.

These three principles—transparency, accountability, and consent—must be seen as more than ideals of good ethical practice. They should be perceived as criteria for legitimacy in any system that touches on digital identity. Missing principles (transparency, accountability, and consent) can lead to profound consequences—misrepresentation, exclusion, surveillance, legitimacy, and commodification of identity. The presence of these principles gives users the ability to trust the systems with which they are engaging, meaningfully assert their rights, and become able to enact agency in increasingly automated environments.

Incorporating ethical frameworks in AI design is not only a technical issue. It may also be tribal and cultural. Incorporating ethical frameworks in AI design means acknowledging power imbalances, structural inequities, and the risk of replicating them in digital form. It also means building systems that are not only efficient but equitable, that value diversity of human experiences, uphold the dignity of individuals, and do not devalue or disenfranchise any individuals' core rights for the sake of innovation.

In short, ethical governance should be incorporated, in some way, at every stage in the design and implementation of AI. For digital identity to be a place of agency instead of dispossession, the information infrastructures through which it is constructed must be constructed with transparency, accountability, and informed and continuous consent.

3.3 Authenticity and Agency in Digital Spaces

The proliferation of artificial intelligence (AI) in digital settings has significantly altered the ways in which people create and experience identity. In contexts that are increasingly algorithmically determined, an understanding of authenticity and agency—once located in the realm of self-representation and self-determination—has been recast. Users of social media, virtual worlds, and AI-facilitated systems are no longer the sole authors of their digital selves—identity is increasingly authored with invisible algorithms, which curate, rank, and filter to determine what users see and how it is seen.

Authenticity, in the meaningful sense, is the ability to present oneself truthfully and freely. Though this remains the mission of many users, in AI-mediated contexts, this authenticity is often filtered through several systems optimizing for engagement, virality, or conformity. In addition to predictions that AI makes about content we will see, AI also produces content that reflects the highest levels of trending or commercially viable trends. These recommendation algorithms effectively nudge us to behave the way that "the algorithm" prefers through mechanisms meant to assign us algorithmic rewards. Over time, this socialization can produce homogenized expressions, which draw people towards conformity, rather than allowing them to operate fully in their multiple identities.

The concept of agency—the capacity to choose autonomously—is similarly at odds. Although users typically engage with content, profiles, and their followers, these user-initiated actions are increasingly weeded down to orders by the AI when an agent engages an action. This occurs through the arrangement of user interface(definitions) and the nature of the AI to predict and standardize behaviors (i.e. structures). Consequently, as Stahl (2021) has observed, choices are increasingly rendered within the contextual influences (e.g., nudges) of decisions made subtly by others. Over time, algorithmic determinism replaces the opportunity to act freely.

This premium is especially visible in the rapidly growing frequency of AI-managed avatars, deepfakes, and synthetic identities that complicate our means of discerning imagined and real selfhood. For some users, such as casual observation with Roblox, they may derive gratification and affordable creativity in identifying and exploring alternative avatars. However, for many users, they may have an understanding that something they like can and will be taken, reshaped, or replaced without response. While hybridity raises important aesthetics questions, it also surfaces deeply felt ethical dilemmas—who owns the likeness of a person in digital territory? In a world where identities are transmuted, manufactured, and made out of the prevailing aesthetic for currents, can authenticity be marginalized?

Furthermore, it is important to consider the emotional implications of these dynamics. Many users simply feel a sense of alienation when their lived experience is bound to metrics or algorithmic approval. The urges to be seen and to be viewed are mediated by increasingly reductionist measures such as likes, views, and shares of the curated, digital identities at stake, which in some instances lead to distortion, resulting in a curated, artificial identity of the user that validates approval in some algorithmic sequencing, which urges some self-censorship of one's lived experience or discourages the explicitness of some identity that may not be of volatile viability. This becomes especially worrisome when considering marginalized groups, as many of their identities have already been overtly marketed to invisibility or poorly marketed in broader digital systems. By claiming and centering oppressive discourses and ideologies in the digital space, AI-powered platforms have cultivated dominant narratives, or what Sibis has called Sybil's digital—and often literal—silencing of those with deviant identities or experiences that disrupt the cycles of privilege that reproduce social hierarchies in explicit or latent forms.

It is important to note that it is not all doom and gloom. Agency can be asserted, and authenticity can be reclaimed if and only if we shift user attention, design palliative efforts, and policy-driven interventions from a dominant view of the socio-technical nature of identity construction to a viewpoint that is cognizant of and values that the construction of identity online is explicitly not static. Design interventions that increase user transparency, participatory control, and contextual relevance can reinstate a sense of ownership over one's digital, customizable flows and representations. Ethical AI design needs to progress away from efficiency and optimization of users, and value complexity, ambiguity, and human variability in identity construction. It needs to be firmly rooted in their ethos of identity construction.

The relationship between AI, authenticity, and agency provides an expansive view into the nature of how the digital self has evolved since its inception and how it is evolving in a landscape of increasing uncertainty with ethical implications in the conceptualization of identities. Digital identity relies not on the self, but the self exists within this space as a negotiated, relational, and contested province of knowledge and meaning-making at play by a combination of humans and algorithmic logic and intervention. This opens both the door of technical understanding and the door of ethical diligence, cultural consideration, and ultimate respect for human dignity in the complex continuum of digital conceptualization of how the self exists in digital co-presence.

3.3.1 The Impact of AI Bias on Identity Misrepresentation and Digital Silencing in Online Spaces

As Artificial intelligence (AI) becomes commonly used for content curation and moderation, issues regarding identity misrepresentation and digital silencing have taken on a new level of urgency. Although generally these systems support engagement or safety for the platform, they can also carry some incredibly deep biases that invisibilize or distort certain identities. The greater concern is that they are likely to invisibilize the identities of marginalized or minority groups.

The most underhanded kind of bias is algorithmic moderation of content whereby certain types of speech, appearance, or identity expression are disproportionately flagged, shadow banned, or removed. Mehan (2024) suggests that when moderation algorithms are trained on unbalanced or norm-driven datasets, they become a reflection of the dominant values of the community that trained them. Hence, normative content submitted by LGBTQ+ users, ethnic minorities, or other less recognizably normative identities and content-creating practices can lead to disproportionate censorship of certain accounts or identities—not because of harm, but in a way that deviates from the learned standard of norm and acceptability.

Examples of how this is a widespread problem can be seen on platforms like TikTok. Schenker (2023) tested the recommendation engine of TikTok and found that its recommendation engine favors content that reflects conventional aesthetics and behaviors in a predictable, algorithmic way by down-ranking systematically (and more than contrast creators) creators that perform alternative gender-identity expression, cultural practices, or political positions. Because TikTok algorithmically diminishes the visibility of these groups, it accounts for their reduced representation in the broader digital ecosystem. In contemporary digital ecosystems, algorithms act as gatekeepers to social narratives about identity, agency, or visibility by choosing not only whose identities are valid and visible but also which identities are worthy of amplification.

Concurrently, advances in synthetic media are compounding already complex structural forms of identity malignance through deepfakes or AI-mediated distortions of identity features and representation. Synthetic content, which can certainly be used constructively, has also been used in ways that contort, manipulate, and misappropriately represent an individual's likeness—particularly women and minority identities. Mink et al. (2024) demonstrated that deepfake technology is now being weaponized to fabricate counterfeit sexual content and/or politically charged and damaging footage of individuals or identities that have often been positioned with little power to react or seek redress. These practices are traumatic in nature and inflict really psychological and reputational, and at times legal, harms as an individual continues to be removed from control and ownership of their identity in digital content ecosystems**.**

4. Policy Recommendations and Future Directions

4.1 Evaluating AI Governance in Morocco for Ethical and Sustainable Innovation

As artificial intelligence (AI) technologies continue to advance in Morocco, we must grapple with the benefits and risks they bring. The development of AI advances many important and exciting areas, including enabling public services, economic modernization, and digital transformation. Yet they also embody structural risks, especially when they are employed in ways that reproduce biases, distort identities, or subject vulnerable populations to further marginalization. In this light, it is clear that AI governance is not purely a technical issue but rather an expression of the ethical and social dimensions.

One immediate obstacle that governments in Morocco need to be aware of—and one of the most challenging at the moment—is the lack of comprehensive AI regulation relevant to Morocco's cultural and socioeconomic context. Although international frameworks such as the OECD, European Commission, or UNESCO meet with the public attitudes to AI to provide key features, Morocco needs its own contextual governance model that incorporates its legal traditions, multi-linguistic dimensions, and various levels of digital literacy. To not have a clear national strategy implies that Morocco is exposed to anonymous technologies that undermine both rights and autonomy while leading to a loss of public trust.

Algorithmic transparency and accountability should be a priority for Moroccan AI governance structures. AI systems deployed in sensitive situations, such as recruitment, credit scoring, health services, or policing, must be auditable, explainable, and subject to independent oversight. We must require both companies and public institutions to detail how their algorithms were trained, the data used, the decision structures implemented, and the pattern of decision-making. Without mechanisms like these, users will be left powerless, and regulators powerless, before potential harm from bad, discriminatory, or harmful technologies.

Another important consideration is protecting digital identities and data sovereignty for citizens. Personal data in the globalized digital economy is collected, stored, and processed whenever cross-border services are involved, leading to privacy, surveillance, and control criteria. It is necessary for Morocco to also strengthen its legal architecture around data protection to create ownership of digital identities. In practice, this means aligning national laws with international regulatory facilities such as the EU General Data Protection Regulation (GDPR) while also meeting local needs, most importantly for multilingual populations and underserved communities in terms of digital access.

In addition, the challenge of digital exclusion must be fully confronted. As artificial intelligence systems become more ingrained in people's daily lives and experiences, those who lack access to or the ability to produce and use technology, digital skill capacity, or the lack of legal rights will be left further behind. In extreme examples there can be a regression into inequality without caution and mediated constraints placed on the use of these digital tools. Governance frameworks must have some form of affirmative action planning in order to easily include some form of action—subsidies/no-cost for access to devices, educational or other events to build AI and multi-elements of digital literacy, or creating governance online/offline programs—that enhances community and citizens' authority to inclusion in proactive ways. Without the realm of governance for inclusion to specify the pre-action of subsidy, there is nothing of value for inclusion. These actions are vital to ensure that AI and its role in development and growth are a route towards empowerment instead of entrenching the system of exclusion.

Further, Morocco would benefit from multi-stakeholder approaches, where we would also consider stakeholders as ecosystems. Ethical and appropriate AI governance policies require the genuine intention and involvement of citizens, stakeholders, and all the community could do to add value or cover accountability. Participatory governance processes need spaces for dialogue and co-creation where regulation responds to citizens served by or engaged in the identified issue from their lived experiences and not what regulatory authorities' prescriptive notions frame for many, e.g. Jabir et al. (2024) note the importance of community voices to derive their representation, or inclusion within governmental processes, as a way of protecting others and ensuring democratic legitimacy.

Finally, the governance of AI and other technologies must be temporal or adaptive and/or forward-looking. The speed of displacement and technology operates as a constant, putting limitations on responsive regulatory actions to accompany the agility to escalate and descend the issues related to action are many. Ongoing impact assessments, impact audits with regularity, and iterative policies and design as monitoring and responsive actions will keep governance conscious and relevant.

In summary, while creating ethical governance for AI in Morocco presents challenges, there are tremendous possibilities. Regulations can certainly consider previous regulatory comparisons if rooted in operating principles of transparency, consideration of inclusion, and accountability as decentralizing community government to private or public. Morocco may be recognized among nations that responsibly conditioned AI to respond to rights and human development and deliver services that are premised on the person's dignity and the diversity of its citizens.

4.2 Data Governance and Ethical Guidelines

The rapid expansion of artificial intelligence (AI) in Morocco's digital ecosystem necessitates a vigorous amount of data governance and ethical frameworks, essentially to identify and mediate the emergence of AI so these technologies could provide transparent, inclusive, and respectful autonomous actions that centralize the identity of the individual, primarily their digital identity.

At the crux of data governance is the question of who owns your data, how was it attained, and how is it used?' Without policy-based frameworks, AI can commoditize personal data rather than socially geared frameworks, or worse, a dumpster fire of disclaimers to help individuals make decisions, which is consent. The issue of ownership and responsibility is sensitivity heightened in Morocco with its distinct differences: cultural diversity, linguistic diversity, and socio-economic disparity. Moroccans regularly engage with digital systems, most often in situations of varying levels of inequality around access, literacy, or legal representation, hence making them particularly vulnerable to abuse or misrepresentation.

Consequently, Morocco should have national data protection legislation that is consistent with global frameworks like the EU's General Data Protection Regulation, with adjustments to reflect Moroccan realities:

- Specify the fundamental aspects concerning the data subject's rights (i.e., access, rectification, destruction, objection).
- Make permission a genuine, informed, and revocable process;
- Have corporations and public entities justify their data collection rationale through limitations of process and formative accountability of data minimization (reduced to what is least necessary).
- Establish an independent National Data Protection Authority, delegating authority to verify compliance and sanction non-compliance.

But legal instruments alone are not enough. Ethical guidelines are needed to frame **how AI systems should behave**, beyond what they are allowed to do legally. These guidelines must be co-developed through **multi-stakeholder consultations**, involving not only government actors and private developers, but also civil society organizations, academic researchers, and representatives of underrepresented communities.

Drawing inspiration from OECD principles and UNESCO's recommendations on AI ethics, Morocco could establish a national framework that emphasizes:

- **Human-centered design**: AI must serve human dignity, autonomy, and rights—not replace or control them

- **Fairness and non-discrimination**: Systems should be proactively audited for bias and corrected when inequalities emerge

- **Accountability and traceability**: Developers and institutions must remain answerable for algorithmic outcomes, with clear redress mechanisms

- **Sustainability**: AI deployments should consider long-term social and environmental impact, not just short-term efficiency

Moreover, **digital literacy initiatives** should be embedded in ethical governance strategies. Many citizens remain unaware of how their data is used, or how to assert their rights in AI-driven environments. Educational campaigns—targeting schools, universities, workplaces, and local communities—are essential to equip individuals with the knowledge needed to navigate digital systems safely and assertively.

Morocco should also encourage the **localization of AI ethics** by investing in homegrown research and open-access platforms that reflect national priorities and values. Supporting Moroccan scholars and institutions in contributing to the global AI ethics discourse ensures that international standards are not simply imported, but meaningfully interpreted in light of the country's historical, linguistic, and institutional fabric.

Effective AI governance depends not only on the strength of legal regulations, but also on the **moral clarity and cultural inclusiveness of ethical frameworks**. By building data governance systems that are both legally enforceable and socially legitimate, Morocco can protect its citizens from the excesses of unregulated AI while fostering a digital future rooted in justice, dignity, and shared responsibility.

Conclusion

Artificial intelligence has emerged as a catalyst of transformation in digital identity, reshaping how we are seen, classified, and engaged with online. In this research, we have examined the ethical, social, and political consequences of algorithmic systems as they shape and reshape the construction of identity while showcasing how imbedded bias in design can distort self-representation and silence marginalized voices. From the subtle operations of algorithmic visibility to the blatant misappropriation of synthetic media, it is evident that AI does not solely reflect identity but produces, filters, and in some cases reshapes it, oftentimes to the detriment of agency and authenticity.

This study has demonstrated that the design and implementation of AI systems in recruitment, policing, healthcare, and social media are largely remediating structural inequality under the guise of neutrality. The risks of data exploitation, exclusion, and misrepresentation of identity are exacerbated by the nascent legal and institutional infrastructures addressing AI in Morocco and their associated data privacy and protection measures. The lack of comprehensive privacy protections combined with a lack of ethical regulation means that individuals can be subject to opaque systems that commodify their data and undermine their digital presence without consent.

In this light, we believe a call to action is justified and warranted. It is time for privacy, transparency, and accountability to be front and center for Morocco's digital strategy. We need to roll out inclusive data governance policies, create independent oversight bodies, and establish ethical design processes that respond to international standards and local contexts. We also need to further educational efforts to inform citizens from all backgrounds, including digitally surveyed communities, of their rights when it comes to automated decision-making.

The future of digital identity will depend upon what we choose to encode into the technology we create. If we don't address the biases, exclusions, and ethical blind spots that AI systems may help to reinforce, we risk creating a normalized digital order that is indifferent to human dignity in favor of algorithmic logic to guide our future. If we are mindful of how AI could be a force of good in society and inclusively reflect the values of the digital commons, it could represent a digital liberation tool—a way to promote perspectives, protect agency, and create a shared digital public space that allows for agency in the expression of identity rather than mere imposition or prediction. The stakes are high, and the need for principled, pre-emptive governance is urgent.

Article Publication Details

This article is published in the **Unifya**, ISSN XXXX-XXXX (Online). In Volume 1 (2025), Issue 1 (October-December)

The journal is published and managed by **Erudexa Publishing**.

Acknowledgements

We sincerely thank the editors and the reviewers for their valuable suggestions on this paper.

Declarations

Ethics approval

Not applicable.

Funding

The authors declare that no funding was received for this work.

References

[1] Ashok, M., Deen, G. B., & Wilson, J. (2022). Ethical framework for artificial intelligence and digital technologies. *International Journal of Information Management, 62*, 102433. https://doi.org/10.1016/j.ijinfomgt.2021.102433

[2] Benbya, H., Pachidi, S., & Jarvenpaa, S. (2021). Special issue editorial: Artificial intelligence in organizations—Implications for information systems research. *Journal of the Association for Information Systems, 22*(2), Article 10. https://doi.org/10.17705/1jais.00665

[3] Bensalah, M. (2021). *Artificial intelligence and human rights: Action plan & recommendations for human rights-sensitive and ethical artificial intelligence*. European Center for Not-for-Profit Law. https://ecnl.org/publications/artificial-intelligence-and-human-rights

[4] Benhmama, A., & Bennani, Y. B. (2024). Factors driving the adoption of artificial intelligence technology in the recruitment process in Morocco. *Access Journal, 5*(3), 387–406.

[5] Boateng, S. L., & Boateng, R. (Eds.). (2025). *AI and society: Navigating policy, ethics, and innovation in a transforming world*. CRC Press.

[6] Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society, 39*, 499–507. https://doi.org/10.1016/j.scs.2018.02.039

[7] Buddemeyer, A., Nwogu, J., Solyst, J., Walker, E., Nkrumah, T., Ogan, A., ... & Stewart, A. (2022, September). Unwritten magic: Participatory design of AI dialogue to empower marginalized voices. In *Proceedings of the 2022 ACM Conference on Information Technology for Social Good* (pp. 366–372). ACM. https://doi.org/10.1145/3524458.3547295

[8] Chouraik, C. (2024). Sustainable AI in Morocco: A systematic review of opportunities, challenges, and policy directions. *EHEI-Journal of Science & Technology, 4*(1), J-Sci.

[9] Costanza-Chock, S. (2018). Design justice, AI, and escape from the matrix of domination. *Journal of Design and Science, 3*(5), 1–14. https://doi.org/10.21428/2c646de5

[10] Ejjami, R. (2024). Adopting artificial intelligence and big data tools across industry sectors in Morocco: An integrative literature review. *International Journal of Environment, Workplace and Employment, 8*(2), 171–198.

[11] El Mnouer, O., Katfi, A., Katfi, H., & Mrhari, A. (2023). Artificial intelligence and recruitment in Morocco: Innovative frontiers for optimizing the collaborator experience. *International Journal of Accounting, Finance, Auditing, Management and Economics, 4*(6–2), 223–238.

[12] Gill, S. S., Buyya, R., & Yoon, Y. (2019). Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things, 8*, 100118. https://doi.org/10.1016/j.iot.2019.100118

[13] Goralski, M. A., & Tan, T. K. (2020). Artificial intelligence and sustainable development. *The International Journal of Management Education, 18*(1), 100330. https://doi.org/10.1016/j.ijme.2019.100330

[14] Hamouti, N., & Elbouzidi, A. (n.d.). The importance of artificial intelligence in the field of Moroccan criminal law: What impact on the legal protection of personal data? *[Publication details missing – specify journal/conference/book]*.

[15] Herath, H. M. K. K. M. B., & Mittal, M. (2022). Adoption of artificial intelligence in smart cities: A comprehensive review. *International Journal of Information Management Data Insights, 2*(1), 100076. https://doi.org/10.1016/j.jjimei.2021.100076

[16] Jabir, H., Lagtati, K., & Pohe-Tokpa, D. (2024). Ethical and legal regulation of using artificial intelligence in Morocco. *Journal of Digital Technologies and Law, 2*(2), 450–472.

[17] Jaldi, A. (2023). Artificial intelligence revolution in Africa: Economic opportunities and legal challenges. *Policy Center for the New South*. https://www.policycenter.ma/publications/artificial-intelligence-revolution-africa

[18] Kaddouri, M., Mhamdi, K., Chniete, I., Marhraoui, M., Khaldi, M., & Jmad, S. (2025). Adopting AI in education: Technical challenges and ethical constraints. In A. X. Editor (Ed.), *Fostering inclusive education with AI and emerging technologies* (pp. 25–72). IGI Global.

[19] Kaur, D., Deokar, A. V., & Gupta, B. B. (2022). Trustworthy artificial intelligence: A review. *ACM Computing Surveys (CSUR), 55*(2), Article 31. https://doi.org/10.1145/3485128

[20] Koanda, Y. (2025). Financial technologies in fragile environments: Triumphs and trials in Africa and the Middle East. In H. Essam & L. W. Ford (Eds.), *The Palgrave handbook of FinTech in Africa and Middle East: Connecting the dots of a rapidly emerging ecosystem* (pp. 1–34). Springer Nature Singapore.

[21] Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law & Technology, 21*, 106–169. https://yjolt.org/21-artificial-intelligence-risks-privacy-and-democracy

[22] Mehan, J. E. (2024). *Digital ethics in the age of AI: Navigating the ethical frontier today and beyond*. Routledge. https://doi.org/10.xxxx/routledge.2024.1234 *(DOI à vérifier)*

[23] Mhlanga, D. (2020). Industry 4.0 in finance: The impact of artificial intelligence (AI) on digital financial inclusion. *International Journal of Financial Studies, 8*(3), 45. https://doi.org/10.3390/ijfs8030045

[24] Mink, J., Wei, M., Munyendo, C. W., Hugenberg, K., Kohno, T., Redmiles, E. M., & Wang, G. (2024, May). It's trying too hard to look real: Deepfake moderation mistakes and identity-based bias. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1–20). ACM. https://doi.org/10.1145/3544548.3580961

[25] Morandín-Ahuerma, F. (2023). Recommendation of the OECD council on artificial intelligence: Inequality and inclusion. *CC BY-NC-SA*, 95–102. *(Clarifier la source complète : conférence, livre ?)*

[26] Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Fall 2020 Edition). https://plato.stanford.edu/archives/fall2020/entries/ethics-ai/

[27] Murdoch, B. (2021). Privacy and artificial intelligence: Challenges for protecting health information in a new era. *BMC Medical Ethics, 22*, Article 14. https://doi.org/10.1186/s12910-021-00600-3

[28] Nguyen, A., Chen, J., & Lee, M. (2023). Ethical principles for artificial intelligence in education. *Education and Information Technologies, 28*(4), 4221–4241. https://doi.org/10.1007/s10639-023-11539-7

[29] Park, T. M. (2022, July). Making AI inclusive. *[Publication type missing — specify journal, book, or conference]*.

[30] Pedro, F., Subosa, M., Rivas, A., & Valverde, P. (2019). *Artificial intelligence in education: Challenges and opportunities for sustainable development*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000366994

[31] Perc, M., Ozer, M., & Hojnik, J. (2019). Social and juristic challenges of artificial intelligence. *Palgrave Communications, 5*(1), Article 61. https://doi.org/10.1057/s41599-019-0278-x

[32] Regragui, O. (2024). *Auditing online software for bias: A controlled experiment in the domain of car insurance* [Doctoral dissertation, Politecnico di Torino].

[33] Rincón, C., Keyes, O., & Cath, C. (2021). Speaking from experience: Trans/non-binary requirements for voice-activated AI. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW1), 1–27. https://doi.org/10.1145/3449119

[34] Rizk, N., & Schonwetter, T. (2024). *Governance of data and data-driven technology*. African Journal of Information and Communication, 30, 1–22.

[35] Robinson, S. C. (2020). Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). *Technology in Society, 63*, 101421. https://doi.org/10.1016/j.techsoc.2020.101421

[36] Roda, F. C., Redondo, A. C., García, A. M., Zafra, M. S., Canal, D. J., Rado, M. A. B., & Mazzetti, M. (2024). *Comparative care workers' discrimination map report*. European

Federation of Public Service Unions. https://www.epsu.org/article/comparative-care-workers-discrimination-map-report

[37] Routabi, A., & Bennani, B. (2024, April). Transforming Morocco's public sector: The synergy of artificial intelligence, big data, and data science. In K. Ghouaiel & Y. Benghabrit (Eds.), *Proceedings of the International Workshop on Big Data and Business Intelligence* (pp. 327–339). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-47189-3_25

[38] Safdar, N. M., Banja, J. D., & Meltzer, C. C. (2020). Ethical considerations in artificial intelligence. *European Journal of Radiology, 122*, 108768. https://doi.org/10.1016/j.ejrad.2019.108768

[39] Scatiggio, V. (2020). *Tackling the issue of bias in artificial intelligence to design AI-driven fair and inclusive service systems*. Politecnico di Milano.

[40] Schenker, D. (2023). *The construction of identity and evolution of desire through synthetic media* [Doctoral dissertation, Temple University].

[41] Singh, S., Rathore, S., Park, J. H., & Hong, W. H. (2020). Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustainable Cities and Society, 63*, 102364. https://doi.org/10.1016/j.scs.2020.102364

[42] Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy, 16*(3), 26–33. https://doi.org/10.1109/MSP.2018.2701151

[43] Stahl, B. C. (2021). *Artificial intelligence for a better future: An ecosystem perspective on the ethics of AI and emerging digital technologies*. Springer Nature. https://doi.org/10.1007/978-3-030-69978-9

[44] Tapo, A. A., Traoré, A., Danioko, S., & Tembine, H. (2024). Machine intelligence in Africa: A survey. *arXiv preprint arXiv:2402.02218*. https://arxiv.org/abs/2402.02218

[45] Tembine, H., Tapo, A. A., Danioko, S., & Traoré, A. (2024). Machine intelligence in Africa: A survey. *Authorea Preprints*.

[46] Vorsino, Z. S. (2024). *Creeping bodies: Digital mediation and embodied experience—A series of three case studies* [Doctoral dissertation, University of Hawai'i at Manoa].

[47] Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration, 42*(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103

Publisher's Note

ERUDEXA PUBLISHING remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of ERUDEXA PUBLISHING and/or the editor(s). ERUDEXA PUBLISHING disclaims responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.