

Social Interactions Under Algorithms: A Sociology of Privacy in Digital Societies

Mimouna BENAICHOUBA *

Djilali Bounaama University, Khemis Miliana- Algeria

m.benaichouba@univ-dbkm.dz

Received date 15/08/2025

Acceptance date 24/10/2025

Abstract:

This article focuses on the problem of privacy in the digital age from a critical socio-legal perspective and aims to deconstruct and interpret the relations between artificial intelligence, algorithms, and power in digital society. The aim of this article is to challenge the prevailing legal-technical framing of privacy and recast it as a constellational issue linked to a redistribution of power and knowledge within surveillance capitalism. The study has taken a multi-layered approach by tracing privacy through time, analyzing algorithms as social agents, parsing the rationale of data commodification in the surveillance economy, and analyzing the profound cultural and social consequences culminating in recommendations for privacy management and interaction in the digital age.

The study concludes that privacy is no longer an isolated individual right but has become a contested social domain that affects identity, discrimination, and digital justice. It also reveals that algorithms have evolved beyond technical tools to become new structures of power that reproduce social hierarchies. The study recommends the implementation of fair algorithmic legislation, critical digital literacy, and the deepening of sociological research in this rapidly evolving field.

Keywords: Digital Privacy; Artificial Intelligence; Algorithms; Algorithmic Culture; Algorithmic Justice.

* Corresponding author

Introduction:

Over the past two decades, the world has witnessed profound transformations in its social and communicative structures due to the rapid advancements in artificial intelligence and algorithmic technologies. The digital space is no longer merely a medium for communication or entertainment; it has become a comprehensive living environment that reshapes social interactions, behavior patterns, standards of acceptance and rejection, and even the individual and collective consciousness of people (Zuboff, 2019). This transformation is accompanied by the emergence of privacy as a central issue, reflecting a complex interplay between technological, social, and political-ethical dimensions (Lyon, 2018).

In today's world, privacy is more than simply meaning "the right to be let alone" (Warren & Brandeis, 1890), as the liberal tradition would have us think - a particular enactment of privacy that has existed since the late nineteenth century. It has become a complex notion that intersects with the algorithmic structures governing the contemporary digital space. Algorithms are not merely tools for data collection; they actively shape the entire digital experience. They classify people, direct attention, and shape everyday decisions - in ways often unnoticed.

According to Beer (2019), algorithmic power is not imposed, but rather operates through "pre-structured" processes that circumscribe the space of interaction and reformulate what is understood as natural, logical, or possible. This moves privacy away from an issue of "decision-making" on the part of the individual, and into a structural issue concerned with one's placement in a network of information flows governed by algorithmic systems of classification and filtering. The algorithmic systems subsequently create unequal social relations between users and the digital platforms that govern data (Beer, 2019).

This raises the main question of this article: how are algorithms transforming social interactions and what does this reconceptualization mean for privacy as a concept and sociality from a sociological standpoint in a digital society?

The crisis of digital privacy today is evident in the shift from an individual privacy model—where data is viewed as personal property—to a broader model of “collective exposure.” In this model, individuals' lives are continuously visible to intelligent surveillance systems that analyze, categorize, and guide behavior without their awareness or consent. These systems, often promoted as neutral and rational, in fact conceal algorithmic biases that reflect economic and political priorities—biases that frequently exacerbate inequality and discrimination (O'neil, 2017).

This suggests that algorithms don't fix injustice, they amplify the existing state of affairs—in all its historical biases and social inequalities. Eubanks (2018) also argues to this end in her analysis of "digital poverty," in which AI tools are used to decide whose eligibility is taken into account, and whose isn't. Algorithms become mechanisms of control over the fate of individuals, communities, rather than tools to improve academic, financial, health, and social outcomes (Eubanks, 2018).

In this situation, privacy violations are no longer single instances nor accidental technology failures, but part of structural practices that reproduce new forms of social inequality and increase the gulf of control and accountability between everyday users on one hand, and digital platforms and algorithmic controllers on the other side (Zuboff, 2019).

According to Eubanks (2018), technology is not always meant to further social justice. Rather, in many instances, it is used as a mechanism by which those who live well below the poverty line and those most vulnerable in society are watched, monitored, categorized, and sanctioned within what she calls “digital poverty.” And these forms of practice are a part of exacerbating structural inequities and deepening social inequalities (Eubanks, 2018).

The objective of this analysis is to examine privacy as a sociological concept in the digital society by setting out to make sense of the social relationships that occur under algorithmic processes while exposing the inequitable relationships developed from an algorithms structure.

This analysis considers the changes around the changes of interaction, and unpacks the circumstances of digitally controlled behaviour, relying on a critical approach that reconstructs privacy not simply as an indivisible right to the individual, but a social and political construct that requires collective cognizance and the enacting of appropriate and effective forms of resistance to the "algorithmic society" (Andrejevic, 2020) .

To support this approach, the essay utilizes contemporary sociological theorists, including David Lyon and his concept of the "surveillance society" (Lyon, 2018) ; Shoshana Zuboff and her concept of "surveillance capitalism" (Zuboff, 2019). The analysis also draws on some recent academic field-based research concerning privacy and digital surveillance practices (with respect to a considerably wide variety of domains: education, healthcare, social work, etc.) providing a direct understanding of the implications of surveillance for the lives of specific individuals and communities.

The importance of this article is in its exploration of what selfhood and social relations mean in a world where data has supplanted land as the primary resource and algorithms have become the unseen arbiters of our interactions and everyday lives. Thus, sociology must immediately reconceptualise privacy not just as an individual right, but as a collective right and site of struggle in the face of digital colonialism and its social consequences.

1. Privacy as a transforming social concept

In the digital age and moving forward, privacy has dramatically changed and will continue to change with the increased efficiencies of digital technologies becoming more commonplace and with the ongoing advancements in AI. Privacy is no longer strictly understood as simply the freedom from interference - whether in the home or in private communication (Warren & Brandeis, 1890), but rather, privacy increasingly appears to be situated with the individual as a controller of identity, personal data, and digital behaviors in vastly un-nested algorithmic systems (Zuboff, 2019) .

1.1. Change of the Concept of Privacy Over Time

The changing concept of privacy illustrating the social changes that accompanied the digital revolution is one of the best examples. Privacy first appeared socially and legally as a personal right of protection against direct intrusion in individual private life. We see it clearly in (Warren & Brandeis, 1890) who made it locality clear and articulated the need to have one's personal life removed from unwanted outside interference in the form of media and press, for example to have protection from the intrusion viewed in a public space.

With advances in communication technologies, together with an entrenched set of digital tools that permeate daily life, privacy has undergone very deep changes both to its content and social and political meanings. The term "digital privacy" emerged for a new state now encountered, whereby individuals are kept in a constant state of being surrounded (unwanted; without knowledge or consent) by devices, and services that routinely capture, compile, and repurpose personal data (Lyon, 2018).

This evolution in privacy, from mere protection to total control of personal data, signifies a serious shift in (social) power relations. As Zuboff (2019) points out, personal data is now a core raw material of the surveillance capitalism economy. Corporations can collect and analyze this data to design new forms of interactions that change consumer behavior and decision making.

Now, privacy is no longer just an individual right; it is also an arena of social and economic struggle.

1.2 The Dimensions of Digital Privacy

The increasing complexity about the topic of digital privacy has resulted in multiple dimensions of privacy that overlay various aspects of an individual's digital and social existence. The dimensions of digital privacy include some more traditional areas of privacy including:

Figure 1: Dimensions of Digital Privacy



Source: Adapted from (Solove, 2008)

In total, the dimensions provide a comprehensive and complex portrait of digital privacy that require legal, ethical, and technological responses. They also demonstrate a profound entanglement with the lived experience of daily living, arguably, rendering digital privacy as more of a social than a technological problem

1.3 Privacy as a Social Relationship: The Distribution of Digital Power

The contemporary understanding of privacy shifts from the standard way of viewing privacy as simply an individual right to one that focuses on the distribution of digital power and control over information, which is defined as a social relation. As Andrejevic (2020) states, the ability to control one's personal data became a social power marker in determining an individual's access to privacy or deprivation of it.

O'neil (2017) is an example of this social relation because she claims the concern is not about data collection, but about data classification (and subsequent judgement) through anonymized opaque and unaccountable algorithmic systems that affect people's access to work, loans, education, etc. O'neil (2017) and therefore discriminatory practices and social inequalities.

As Eubanks (2018) notes, digital privacy has become a class issue in which poor people and minority groups often face algorithmic surveillance, unfair classification, and ultimately, social gaps, producing an automated, digital analogue to social and economic discrimination, disguised as "algorithmic neutrality."

Consequently, digital privacy becomes an issue of social justice, not merely a matter of individual rights. Those with the least ability to protect their data or understand how it is exploited are often the most vulnerable to the negative consequences of privacy loss.

Thus, privacy shifts from being a strictly legal or ethical concern to a social issue that demands collective awareness and organized resistance against surveillance and digital

classification practices that empower technological elites at the expense of individuals and communities.

2. Algorithms as a New Social Actor

Algorithms are not just a technical tool that runs behind user interfaces anymore, they are a new form of social actor that is shaping the environments where human interactions are produced and reconfigured. In the age of artificial intelligence, algorithms have a substantial existence in terms of decision-making, filtering information, guiding behaviors and even creating the very forms of social organizations.

2.1 Algorithms as Regulatory Mediators of Social Relations

Recent academic works demonstrate that algorithms do not exist in a purely technical context where they express their essence away from cultural and political representations, or economic imperatives that have been coded into the algorithms. Specifically, Taina Bucher (2018) undertakes an examination of Facebook algorithms and notes that algorithms are not simply tools that prioritize posts on a timeline; they directly affect feelings and attitudes and create a consistent and perpetual submission to a black-boxed technical logic that is impossible to know or push back against (Bucher, 2018).

This feeling of inferiority relates to not just our lack of algorithmic literacy but to the asymmetric relation between the creators of the rules and those who must adhere to those rules—without transparency, negotiation and a right to object.

In line with this, contemporary critical literature has emerged analyzing algorithms as post-bureaucratic forms of governance, exercise a new genre of symbolic and material power—not exercised by or through the state, but through digital infrastructure and corporate-run networks. As (Couldry & Mejias, 2019) highlight, "data collection and analysis have become ... infrastructure. It has gone from being a tool to gather evidence to being an infrastructure that produces a new form of social control" (p. 1) and where life is organized around the imperatives of value extraction and surveillance (without democratic accountability).

Zuboff (2019) reinforces this analysis with an extraordinary idea she calls "surveillance capitalism," in which individual data is used to anticipate and shape individual behavior for purely commercial goals. This gives power to algorithms as regulatory and controlling agents no less powerful than bureaucratic authority—but far more pernicious due to their invisibility and lack of public accountability (Zuboff, 2019).

This shift now places algorithms as new social intermediaries that shape our routine relation: Who sees whom? Who interacts with whom? Who is visible, and who is invisible? Classical bureaucracies reproduced class hierarchies in its systems; algorithms reproduce class hierarchies as well, now in a digitized, automated and obscured manner—buried under a discourse of efficiency and neutrality.

2.2 The Sociology of Algorithmically-Modified Interactions

Following Erving Goffman in *The Presentation of Self in Everyday Life*, especially his idea of the "symbolic interaction order" (Goffman, 1956), present-day researchers like Donald MacKenzie (2019) wish to trace how algorithms disrupt the symbolic interaction system of people.

The social interactions we have become pre-fabricated and governed by laws we cannot potentially negotiate our way around when accounting for recommendation systems and classification algorithms, diminishing individuals' symbolic flexibility and spontaneity often associated with natural human interactions (MacKenzie, 2019).

As Kallinikos (2010) argues, digital platforms do not only structure social interaction but they amass symbolic capital by producing the very infrastructure of information. Digital platforms create controls for who, what, when and how visibility occurs in their ecosystem. This regulatory power is something we could think of as 'algorithmic meta-capital', capital

from control of the logic of visibility, access and interaction in a governable digital medium. This also creates a new form of symbolic domination dominated by algorithmic regulation and determines our scepticism about our interaction and values of social mutual recognition (Kallinikos, 2010).

This systemic pivot in the logic of interaction not only inhibits the human dynamics of communication with one another, it invisibly shifts the dynamics of human communication as an automated process governed by classifications and guidance. The implications are grave when we think about the fundamentals of freedom of action, identity, and self-representation in the digital ecology.

2.3 Automation and Algorithms: From Interaction to Behavioral Guidance

Milan (2015) research on protest movements highlights the usage of algorithmic methodology to broker crowd control and provide guidance for political interactions, as seen in the digital affordances associated with the Occupy movement and the notion of cloud protesting. In these mechanisms, algorithms do not simply function as passive display instruments; rather algorithms determine when political content is displayed, for whom, and in what order - making them implicated in either mechanisms of mobilization or mechanisms of suppression and political control.

The argument is further advanced by Lyon (2018) and Shoshana Zuboff (2019), who both regard algorithms as a primary tool in the extraction of value from social interaction. The production of personal data has become a commodity for analysis, predicting, and guiding behavior. Zuboff in particular, utilizes the term "surveillance capitalism" to argue that people's lives are transformed into a series of measurable, predictable and ultimately economic power forms of engagements, often without awareness or individual agency (Zuboff, 2019).

2.4 From Individual to Pattern: Algorithms as Mechanisms of Social Classification

Algorithms help to shift the axis of gravity from the subjective individual to the "pattern" as a computed model. People get categorized by their data, then followed by attributes that are not often made available, making people susceptible to backwards-looking algorithmic decisions (Eubanks, 2018; O'neil, 2017). In many instances, those backwards-looking algorithmic decisions can equate to deception: the minimization or outright rescindment of individuals' opportunities to an employment opportunity, loan opportunities, or political participation.

To demonstrate how these algorithms classify those needy individuals, through case studies in the United States, (Eubanks, 2018), Homeless Services Integration (HSI) system in Los Angeles—describes how these algorithms classify those needy individuals through examples of standardized indicators deemed objective, even though those systems overwhelmingly recombinant class and race discrimination. Individuals are not given any social assistance labeled as "low priority" for support based on data they possibly never have access to that may or may not be completely accurate, reinforcing structural marginalization.

In addition to the classificatory consequences of digital infrastructure on already marginalized populations articulated by (Bonini & Tréré, 2024; Eubanks, 2018) note that algorithmic platforms not only classify, but also automate and reproduce power relations. Users are engaged in ongoing, full-time evaluation, around when they can work, whether they can work, and for whom they can work. This is most evident in the delivery platform and gig economy services (Bonini & Tréré, 2024) which are evaluated upon cost-optimal, algorithmic, non-transparent evaluative criteria to whom they do not even know exist or what they could appeal against. This could be termed "algorithmic blame," or blaming individuals for the outcomes of processes they do not actually control.

In this sense, algorithms serve as vessels of symbolic regulation: once absorbed into the activities of the individual, they regulate the person's appearance within the system of expected social behavior.

2.5 Algorithms as a Source of Social Power

Referring to their sociological approach, Couldry and Mejias (2019) conceptualize algorithmic power as embedded within the digital infrastructures of major platforms, rather than solely exercised through conventional state apparatuses. In this context, algorithms can be seen as means for obtaining value and knowledge from human interaction, primarily by an ongoing cycle of data collection and processing.

This type of power is soft, often imperceptible, and appears to be horizontal, yet continues to reproduce relations of control and exploitation at an invisible level. Instead of traditional forms of authority and its predictable hierarchical verticality, new modes of governance based on the constant flow of data emerge, making it a new kind of digital colonialism, where human interaction is rendered a useful, exploitable resource through the operational logic of connectivity.

A sociological exploration of the second axis shows that algorithms are not only technical instruments that mostly work in the background of digital interfaces. Algorithms have moved from being a mere technical instrument to a new social actor that reorganizes our interactions while reinterpreting notions of centrality, merit and visibility. Through its multiple identities as regulatory intermediaries, classification processes, and purveyors of symbolic power, algorithms have acted as social actors that shape digital social structures that support a logic of control, even when they appear decentralized and tacit.

3. Surveillance Capitalism and the Commodification of Social Life

With the increasing dependence on digital and AI-based media, social relations and practices have ceased to exist or unfold in neutral or natural spaces (Boungab & Aït Mouhoub, 2025). They are now mediated by complex algorithmic infrastructures that extract data, redirect action, and control a novel type of economic and epistemic domination. These new forms of domination have led many theorists to grapple with the new economic system driven by technology companies, which is founded on the transformation of personal experiences of social life into marketable data.

3.1 The Idea of Surveillance Capitalism

The idea of Surveillance Capitalism was systematically elaborated in the works of Shoshana Zuboff, especially in her widely read book *The Age of Surveillance Capitalism* (2019). In that book, she elaborated the thesis that the big tech companies, especially Google and Facebook, do not just provide users with digital services as we think of products in a classical economic sense, but actually use the data they collect on us to track, model, analyze, and predict behaviors (our behavioral surplus), and then monetize those predictions into economic profit.

Zuboff goes on to say that this new economic model differs from classical industrial capitalism because it produces products we traverse via space/time (consistent digital experiences) with land, labor, or raw materials as inputs, as it turns our experience of living into behavioral surplus, which the tech companies then consume to create products which they sell in newly created prediction markets. Furthermore, Zuboff adds that this process occurs without people knowing what's happening to their data, so the imbalance between the ethical principles popularized in the structure of the digital economy is more prominent than what would naturally occur in a circular economy based on; land, labor, or raw materials (Zuboff, 2019).

To put this another way, it likely is clear now that the logic of capitalism (since the inception of neo-liberal capitalism) has gone through a qualitative change; from producing

goods to producing value from human behavior itself. This new capitalism is not selling products—it (in conjunction with algorithmic systems) is selling control over human beings without any transparency or accountability.

Consequently, resisting surveillance capitalism is much more than just resisting the appropriation of a person's data and consists of a deep rethinking of the relationship between technology, the economy, democracy, and human freedom.

3.2 Algorithms and the Commodification of Personal and Social Data

Under surveillance capitalism, personal data is no longer restricted to technical or cognitive data; it now also includes personal feelings and emotions, habitual behavior, and desires and preferences, including the most intimate aspects of daily life. This data is processed into digital "raw material" and is extracted, classified, and then spliced into actionable behavioral template, making algorithms the key agent in this process. In this construction algorithmic processes implement the gathering, connecting, analyzing, and re-make, human experience according to the logic of the market.

O'neil (2017) cautions us that these algorithms now exist as automated social classification tools, particularly if unaccountable. Algorithms then create new digital classes, segregating economic consumers from non-economic consumers. Consider an algorithm that can determine eligibility for a loan or employment based on previous digital data that is not even known to you and even without direct human involvement.

In this regard, Lyon (2018) argues that this capitalist exploitation of data turns human beings into commodities. The human individual becomes a digital being, policed, monitored, and measured as being in control according to inevitable algorithmic equations relating to the market. This abstraction of being renders the human a "digital commodity", subject to sale by advertisers, corporations, and everyone else to advertisers as a stream of marketable patterns rather than as sentient being with a right to be forgotten.

Our evaluation of the commodification of personal and social data through the lens of surveillance capitalism has established that the threat with data is not the act of collecting it, but when it is utilized to decide on critical matters in the lives of individuals (e.g., which candidates to offer jobs or loans, whether or not they can access healthcare). This allows for the suffusion of social bias by its automated form and locks in patterns of exclusion and inequality.

In this context, the human self is reduced from an expression of selfhood to that of a digital profile strictly governed by businesses and platforms. From the self, we create ourselves into forms that fit consumerist and commercial standards such that our individual identities are represented as a sellable and exhausted "item" made possible by algorithmic inclinations.

3.3 The Commercial Exploitation of Algorithms and the Decline of Privacy

The privacy condition (where individuals have control of their personal information) and how that concept maintains meaning, no longer applies where data continues to play an increasingly central role in the collective imaginary of digital economies. Most contemporary digital users, as a reflex, do not regularly question how their data is collected or used and for many people, there is no real ability to stop it—let alone bargain over it.

As reported by the Pew Research Center (2023), 70% of Americans do trust companies to use AI responsibly, while 81% are fairly certain that the companies are using data in a way that most people would not agree with. Faverio (2023) Numerous other reports and studies support these findings. In the Ipsos Global AI Trust Report (2024) and a report titled "Trust, Attitudes and Use of Artificial Intelligence: A Global Study", prepared by the University of Melbourne with KPMG (Gillespie et al., 2025) it was also noted that 61% of the general population did not trust AI typically, and only 53% saw it as not a direct threat to privacy. For those participants concerned about government and commercial uses of AI, only one-third of

participants trusted the public and private institutions in the development of AI either way to serve the public interest.

David Lyon (2018) argued that the data collected from users is not being used only to predict user behaviors, but also to influence the decisions and guide daily practices, personalizing a social issue of privacy around power relations in society. So, algorithms as tools of organization/technologies are not simply technical, but they embody invisible forms of actions on relations in society expressed or shaped by logics of commodification and the market.

In this case, we can better understand the impact of algorithmic accountability using the example of the “attention economy” where the collection of users' attention—and consequently their data—is predicated on the fate of digital platforms by capturing additional user attention. Knowing this the notifications alerts, short form content, and recommendation algorithms mark purposive applications towards capturing totality of user attention, limiting freedom, and user-led autonomous interaction.

These worries are already captured in the following statistics:

- 78% of consumer respondents stated AI should be used in ethical means.
- 84% of respondents who were familiar with generative AI supported labelling of AI-generated content as a compulsory legal requirement.

These three examples, capture a sense of attempts to regain a degree of control from a more obscured and automated information context.

As a result, we have a situation in which algorithms are invisible mechanisms of rule, and reproduce new forms of inequality and discrimination, especially when accountability and institutional transparency is not legally enforced. The real problem has the potential to create an infrastructure of digital connectivity that not only relies upon commercial logic, but reproduces the relationships social attachment and relationality within a market model built on economic globalization.

4. The Sociological and Cultural Implications of Algorithms

Amid the rapid digital transformations, algorithms are no longer merely silent technical tools; they have become a fundamental part of the cultural and social fabric of contemporary societies. They no longer merely manage data or accelerate processes, but deeply influence how values, symbols, and identities are shaped.

4.1 Algorithmic Culture: New Forms of Power and Influence

Striphas (2015) introduced the idea of "algorithmic culture" - not simply identifying ways algorithms can act as agents of organization in culture (technically not merely managing content, but affecting taste, desires, and habits). For example, what we read, listen to or watch on different digital sites depends on automated suggestions based on meticulous behavioral analytics.

In this form of innovation, algorithms now exhibit a new type of symbolic power involving subtle influence and indirect control over our preferences and decisions in daily life. For example, Bogard (1996) has indicated that power is not wielded by prohibition or censorship but through regulation of flow of information - only permitting a few that are visible, or eligible for attention to deserve it (Bogard, 1996) .

In a similar manner, Bucher (2018) notes in her research on Facebook that algorithms can show or display but also shape the relationship and nuances associated with the emotional and behavioral interaction between the user and the platform - making the user an extension of the logic defined by the algorithm

4.2 Shaping Social Identities: From Digital Identity to Algorithmic Isolation

In the digital age, identity is no longer constructed solely through face-to-face social interaction but through digital interactions designed, filtered, and interpreted by algorithms.

Social identity components such as a one's profile, activity logs, and behavioral data create a digital identity, which may not be an accurate representation of oneself but is evaluated, classified, and used to make decisions.

Zuboff (2019) argues that the individual does not own this digital identity, the corporation owns and alters it without the individual's even knowing it exists. In this sense, Eubanks (2018) suggests that these identities, while protected, are sometimes used to exclude individuals in ways that do not accurately reflect the complexity of social reality, and are built using predictive models.

Psychologically and socially, these mechanisms may lead to a kind of "*existential disconnection*," where the individual feels that their identity is being shaped and controlled remotely. Some refer to this as "*algorithmic isolation*," where algorithms trap individuals in informational bubbles (filter bubbles), reproducing their convictions and excluding differences—thus weakening openness and deepening polarization.

Milan (2015) argues that **digital interaction**, guided by algorithms, has come to represent a new kind of virtual belonging, one that may replace—or distort—traditional social affiliations. This raises questions about the very nature of belonging in a society directed by invisible software.

4.3 Social Trust in Algorithmically-Managed Societies

In traditional societies, trust is built on direct interaction, repetition, and a pre-existing knowledge of social contexts. However, in digital societies, a large portion of interaction is being mediated by intelligent systems, the logic of which is not readily available to audiences. This weakens what Lyon (2018) calls "digital trust," or the trust we can develop in algorithms that make choices on behalf of audiences.

According to Andrejevic (2020), in establishing trust in these systems, efficiencies are not only involved, but also equitable, transparent, and accountable methods of operation. Algorithms can preclude trust by concealing their logic and functioning solely within market frameworks or as part of a "security" precept, thereby impacting on the basis of the social contract, and altering the relationship between citizen and institution.

As a result, establishing accountability of algorithms is not just an issue for designers or legislators. It is an issue for scholars across a wide range of disciplines, and also for activists and importantly for users who can demand accountability, a clear explanation, and clarity in established ethical boundaries that represent the dignity of all human beings.

Thus, if we examine the cultural and sociological implications of algorithms, we can see that they can be understood as a brand new and incredibly radical form of social power that does not simply influence behaviours, but rather, defines identity, belonging, and social trust. Algorithms have moved far beyond just being technical instruments. Algorithms have become a social structure that creates its own culture and enforces its own pace on everyday life, requiring us to generate new thinking about the foundations of social structures in a context where human relationships are subject to programming instructions and code more than people.

Ultimately, no society firmly committed to justice and dignity can let these structures operate without accountability, or worse, let their entrenched biases and self-interests hide behind the guise of neutral technology.

5. Surveillance Capitalism and the Commodification of Social Life

In today's world where algorithms and AI play an increasingly influential role, privacy, historically a technological systems issue, has transformed in the established discourses at the socio-cultural and political levels through attempts to reshape the relations among individuals, the state and digital private companies.

As individuals have begun to see the risks associated with digital tracking, profiling, and algorithmic discrimination, resistance to surveillance, as well as calls for international laws recognizing privacy as a human right, have intensified.

5.1 Strategies to Safeguard Privacy as Individuals and as Communities

Users are becoming more mindful of the harms of digital tracking and excessive exposure through online sites and their associated facilities; these facts prompt users to evolve defensive strategies for digital privacy. Users undertake various defensive activities including using ad blockers, using permission management apps, or everyday behaviours like sharing less, not submitting sensitive information, or creating many (or alternate) accounts.

Zuboff (2019) referred to these behaviours as "silent resistance"; this is a way to describe that users-while there is little choice-are trying to regain more control of their digital disposition.

Another pattern growing in practice is what has been unwittingly termed "symbolic disengagement"; that is, disengaging from all or certain aspects of one's digital biography motivated by a response to permanent exposure. Yet, these individual strategies are limited and cannot be more powerful than formalized processes (like legislation and public policy).

As a result, we must understand that gaining back our power over privacy, is more of a collective and institutional undertaking, not just a personal retreat. Protection can only be assured through the creation of legal and ethical frameworks to govern the use of algorithms, along with enforceable standards that can guarantee transparency and accountability of algorithmic models.

In addition, it will be necessary to develop a digital culture that includes applicability and critical literacies to change our resistance as a user from a disordered response, to that of coordinated collective action, that attacks the actual structure of algorithmic domination.

5.2 Public Policies and International Laws for Privacy Protection in the Age of Algorithms

Countries and international organizations are beginning to respond to violations pertaining to personal data by implementing stronger legislation around the use of AI systems. Some of the most well-known policy frameworks include the General Data Protection Regulation Act (GDPR) issued by the European Union in 2018, which placed strict obligations on companies around transparency, data collection, and an overall right to explanation for the user.

In 2024, the European Parliament voted to pass the Artificial Intelligence Act, which marks the first legally binding legislation to establish risk classifications for AI applications and regulate their use in sensitive fields like justice and health care (European Parliament, 2025).

According to the Stanford HAI report (2024) in the United States, the year 2023 was unparalleled in terms of artificial intelligence related legislation. In 2023, there were 181 federal Bills regarding artificial intelligence—a twofold increase from 2022 with 88 Bills. In addition, the federal regulations related to artificial intelligence increased to 25 regulatory measures in 2023, compared to one regulation in 2016. This indicates a legislative acceleration to keep up with the issues raised by this emerging technology.

Globally, the number of citations of AI in legislative proceedings worldwide nearly doubled, increasing from 1,247 in 2022 to 2,175 in 2023. AI appeared in the legislative proceedings of 49 countries in 2023, and the issue was discussed in at least one country on every continent, indicating the global level of policy dialogue about AI (Stanford HAI, 2024, p. 24).

The Center for AI and Digital Policy (CAIDP) has noted a near-universal consensus around the principles that should govern the development of AI, notwithstanding the difficulties in applying and enforcing those principles. The first international treaty of its kind on AI has become effective, the Council of Europe Framework Convention on Artificial

Intelligence, Human Rights, Democracy and the Rule of Law, which is open for signature by both member and non-member countries of the Council.

So far, 41 countries have signed the treaty including the United States, the United Kingdom, countries of the European Union, Japan, and Canada (Yoder & Randolph, 2025).

Several more recent legislations also include the necessity to empower people to challenge automated decisions and to safeguard marginalized groups from any biases algorithms may encode. This approach aligns to a call by Eubanks (2018) for a formalized "ethical charter for data engineers" to protect digital dignity and ensure algorithms do not reproduce social exclusion and discrimination through automation.

5.3 The Future of Privacy and Social Interaction given the Developments in Technology

As technological advances increase and surveillance and analytical tools proliferate, the future of privacy and social interaction may rest on our societies' ability to establish ethical models of sustainability for technological development. Especially with the rise of generative artificial intelligence (Generative AI) applications, the potential for digital identity to be recast into incoherence highlights a compelling need for "ethical data governance."

While there seem to be many users willing to share their anonymized data to improve products, commercial uses of AI functionality could foster conditions that contribute to further distrust. Moving from transactional human interaction to automated participation brings new challenges to building digital trust. As Andrejevic (2020) observed, "trust is about transparency and accountability, not simply technical performance.

Consequently, it has become necessary to reconceptualize privacy as a collective right rather than as an individual right. The notion of privacy a part of an individual identity has been redefined to impact each and every one of us socially and systematically. Each automatic decision and each algorithmic classification reshapes not just the individual, but our entire social world. So, the notion that we could design technologies with algorithmic justice is not a wishful demand of the elite, but a sociological necessity to redress the balance of the humane dignity and innovation.

Conclusion:

This article, through multi-level sociological analysis, identified artificial intelligence and algorithms as no longer merely technical instruments employed to 'serve' individuals or institutions. Rather, they exist as dynamic structures that affect social interactions, self-awareness and awareness of others, while redesigning power relations and inequality in social relations in the digital world. Algorithms categorize people, situate them in relation to data points and consent via 'algorithmic realities' where technical questions of authority enfold with social symbolism and power.

We have established that privacy has transcended to a social and political issue regarding trust, accountability and the power to 'see' or categorize individuals and the democratic rights of citizens, who are arguably the fount of authority in algorithmic structures, and that commercial and security applications of algorithms commodify 'life' and citizen institutional aspects of public and private arenas no longer exist.

All this leads to a challenge for new forms of thinking and reconsideration, that move past a technical solution point of view towards a social understanding of the algorithm environment. This understanding will need to evolve to become a socio-cultural critique, legal framework, to achieve digital justice and provide human dignity.

Recommendations: Based on these conclusions, we can advance the following recommendations:

- Integrating the topics of artificial intelligence and privacy into educational programs and training should happen in a manner that is consistent with studies in sociology, media studies, and/or law.
- Stimulate useful research: This means supporting field-based comparative studies in sociology that provide a unique, sociologically examined representation of how algorithms affect vulnerable populations, such as women, the poor and minorities in diverse positions of vulnerability in diverse societies.
- Revise legal and legislative provisions: In particular to establish regulations concerning privacy and transparency, requiring that digital companies give individuals means to contest automated decisions, and protective measures for vulnerable groups defining algorithmic discrimination.
- Develop an orientation toward "digital citizenship": This includes equipping people with the tools to essentially take charge of their own data, encouraging the development of critical thinking skills towards technology, and increasing civil oversight initiatives of digital platforms.

References:

- Warren, S., & Brandeis, L. (1890, December 15). The Right to Privacy. *Harvard Law Review*, IV(5).
- Andrejevic, M. (2020). *Automated Media*. New York: Taylor & Francis.
- MacKenzie, D. (2019). How algorithms interact: Goffman's 'interaction order' in automated trading. *Theory, Culture & Society*, 36(2), 39–59.
- Beer, D. (2017). The social power of algorithms. *Information, Communication & Society*, 20(1), 1-13. doi:<https://doi.org/10.1080/1369118X.2016.1216147>
- Bogard, W. (1996). *The simulation of surveillance: Hypercontrol in telematic societies*. Cambridge University Press.
- Bonini, T., & Treré, E. (2024). *Algorithms of resistance: The everyday fight against platform power*. London: MIT Press.
- Boungab, D., & Aït Mouhoub, M. (2025). Digital Communication Between Family And School And Its Role In Reducing The Phenomenon Of Student Absenteeism (a Case Study At Al-arabi Al-tabasi Middle School In Al-qolea). *Journal of Studies in Deviation Psychology*, 10(1), 394-411.
- Bucher, T. (2018). *If... then: Algorithmic power and politics*. New York: Oxford University Press.
- CISCO. (2025). *Cisco 2024 Consumer Privacy Survey: Privacy awareness: Consumers taking charge to protect personal information*. Retrieved from Cisco Systems, Inc: <https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html>
- Couldry, N., & Mejias, U. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford, California: Stanford University Press.
- Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: Picador, St Martin's Press.
- European Parliament. (2025, February 19). *EU AI Act: first regulation on artificial intelligence*. Retrieved from European Parliament: <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>
- Faverio, M. (2023, October 18). *Key findings about Americans and data privacy*. Retrieved from Pew Research Center: <https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/#:~:text=Many%20Americans%20have%20little%20trust,AI>
- Gillespie, N., Lockey, S., Ward, T., Macdade, A., & Hassed, G. (2025). *Trust, attitudes and use of artificial intelligence: A global study 2025*. Australia: The University of Melbourne and KPMG.
- Goffman, E. (1956). *The Presentation of Self in Everyday Life (Monograph No. 2)*. Edinburgh: University of Edinburgh, Social Sciences Research Centre.
- Kallinikos, J. (2010). *Governing through Technology: Information Artefacts and Social Practice*. New York: Palgrave Macmillan.
- Komnenic, M. (2025, May 9). *54 Revealing AI Data Privacy Statistics*. Retrieved from Termly : <https://termly.io/resources/articles/ai-statistics/>
- Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. London: Polity Press.
- Milan, S. (2015). From social movements to cloud protesting: the evolution of collective identity. *Information, Communication & Society*, 1-14.

- O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishing Group.
- Solove, D. (2008). *Understanding Privacy*. London: Harvard University Press.
- Stanford HAI. (2024). *Artificial Intelligence Index Report 2024*. California : Stanford University.
- Striphas, T. (2015). Algorithmic culture. *European Journal of Cultural Studies*, 18(4-5), 395–412.
- Yoder, A., & Randolph, C. (2025, May 2). *Key Findings from the Artificial Intelligence and Democracy Values Index*. Récupéré sur Tech Policy Press: <https://www.techpolicy.press/key-findings-from-the-artificial-intelligence-and-democracy-values-index/>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.