Resistance Under Infrastructural Rule

Stefania Milan

Contemporary digital societies rely ever more on Artificial Intelligence (AI)-mediated systems to organize participation, communication, and governance. Consider the now-familiar experience of interacting with public institutions through AI-operated chatbots. From welfare agencies to municipal administrations, citizens are able to ask questions, provide direct feedback, contest decisions, or obtain information through automated and always-available digital interfaces (Kaun & Männiste, 2025). Yet this mode of participation is mediated not only by bureaucratic procedures, but also by proprietary interfaces, algorithmic triage, and opaque (even if seemingly user-friendly) infrastructures that shape who is heard, how quickly, and under what conditions.

A similar dynamic can be observed in the growing use of facial recognition technologies in smart urban environments (Luusua et al., 2023). These AI-enabled biometric systems analyze facial and other bodily features to identify and track individuals. Introduced in the name of security or convenience, they regulate access to mobility and public space while rendering individuals continuously legible to computational forms of identity verification and monitoring. Thus, emerging grassroots acts of resistance and contestation—from anti-surveillance makeup to coordinated digital rights activism (Kazansky & Milan, 2021) and the sabotage of smart infrastructure (Ting, 2024)—must adapt to infrastructures that anticipate, classify, and modulate behavior in real time.

These developments reveal a broader paradox of contemporary digital societies: they multiply possibilities for engagement, expression, and dissent (for instance through forms of social media activism), while simultaneously intensifying asymmetries of visibility, editorial and algorithmic curation, and infrastructural dependency. While earlier work has mapped forms and tactics of contestation in data-driven societies (e.g., Flesher Fominaya et al., 2024; Gutierrez, 2018; Milan & van der Velden, 2016), this essay asks a different question: how are the very conditions, forms, and logics of resistance reshaped when power operates through algorithmic systems and AI-mediated environments? Rather than merely cataloguing resistant practices, the focus here is on the changing nature of resistance itself.

This chapter starts from the observation that, as AI reshapes the relationship between citizens and the state, it also transforms citizenship, democratic participation, and the conditions under which resistance becomes possible and meaningful. In digital societies, power no longer resides exclusively in identifiable institutions or sovereign actors. Instead, it operates through distributed arrangements embedded in everyday life, where technologies (such as AI chatbots and algorithmic systems for risk prediction), institutions (including welfare agencies and data infrastructure operators), and social practices (from surveillance to political protest) shape one another. This transformation alters both what people are able to do as political subjects (commonly referred to as "political agency") and how democratic contestation can be enacted.

Under these conditions, resistance becomes at once more necessary, more ambiguous, and more difficult to sustain. As we shall see, it becomes ever more

infrastructural and anticipatory, unfolding within privately governed computational environments that simultaneously enable and constrain political action. So, visibility becomes ambivalent, participation is mediated by algorithmic systems, and resistance often shifts away from direct public confrontation toward strategies of opacity, evasion, contestability, and infrastructural intervention.

The chapter brings into dialogue digital sociology and critical data studies, two fields concerned with the societal consequences of digital technologies. It is organized as follows. First, it illustrates the transformation of power in contemporary digital societies, illustrating three shifts in governance. Second, it explores the transformation of political agency, distinguishing also between political agency, contestation, and resistance. Third, it examines how resistance, as a specific and oppositional expression of political agency, is reshaped under AI-mediated governance. Fourth, it reflects on the implications of these transformations for democratic systems. Democracies are a particularly important site of analysis because they are expected to guarantee accountability, transparency, and the protection of fundamental rights. If even democratic societies struggle to govern AI-mediated systems in ways that remain fair, contestable, and publicly accountable, this raises broader concerns about the future of democratic life under infrastructural rule.

Power under Infrastructural Rule

The computational turn inaugurated in the 1950s paved the way for the digitalization of society that accelerated in the 1990s. Information was progressively transformed from analogue to digital formats, enabling the storage and circulation of unprecedented quantities of data. In the 2010s, the advent of datafication (the transformation of social activities and behaviors into quantifiable data) marked a further acceleration in the scale at which states and private actors could collect, process, and operationalize information, to the point that observers have described it as a fundamental paradigm shift in how our social system is organized (Kitchin, 2014). These developments should not be understood as isolated technological shifts, but as cumulative and mutually reinforcing transformations that progressively expand the capacity to capture, process, and govern social life through data. Fast forward to the present, the spread of AI, from Machine Learning (ML) systems to Large Language Models (LLMs), coupled with the dramatic advances in computational power and data storage capacity, has further expanded the ability to analyze, predict, and even generate social reality from data.

AI technologies are now woven into the infrastructures of contemporary digital societies, shaping everyday life in ways that often remain invisible until they hit close to home. In the “data welfare state” (Kaun & Masso, 2025), access to public services and welfare provisions is progressively more regulated through biometric identification systems that may however augment inequality (Masiero, 2024). Decisions in the policy domain are often delegated to, or guided by, sophisticated ML systems (Starke & Lünich, 2020). Automated facial recognition is gradually deployed in schools, for example to control access to entrance gates and monitor pupils’ attention in classrooms (Andrejevic & Selwyn, 2020). And digital identity systems or algorithmically curated public communication on social media, among others, alter how individuals

interact with public institutions and participate in civic life. AI systems are no longer confined to discrete technological applications but embedded in the mundane infrastructures through which societies are governed and populations managed.

These developments give rise to what can be described as governance *by* data infrastructure: a mode of governance that operate through interconnected digital systems, data architectures, and computational infrastructures. These, alongside and beyond laws, institutions, or direct intervention, increasingly organize access to services, participation, mobility, and ultimately rights (Milan, 2024a).

Infrastructural rule therefore describes a form of power exercised not primarily through direct coercion or visible institutional authority, but *through the design and everyday operation* of data infrastructures that shape participation, access, and behavior. As these systems become embedded in the ordinary functioning of society, they operate as unavoidable infrastructures through which social and political life must pass. Crucially, many of these infrastructures are operated or controlled by a small number of powerful private corporations, such as Amazon, Meta, and Google, thereby further blurring the boundaries between public governance and corporate power.

There transformations are at the origins of three broader shifts in the governance of the social:

- from industrial forms of power to informational and infrastructural forms of power
- from citizen surveillance centered on observation to predictive systems aimed at behavioral modulation
- from data extraction alone to forms of generative and "synthetic" governance.

The first shift in contemporary governance points to the growing centrality of information (Braman, 2006) and digital infrastructures such as undersea cables, data centers, and LLMs as sources of economic and even political power in contemporary digital societies, gradually displacing more traditional industrial logics centered on material production. This transformation affects both private actors and states, whose capacity to govern now depends on the ability to collect, process, and operationalize data at scale. This dynamic underpins what has been termed "surveillance capitalism", a political-economic model based on the large-scale extraction and monetization of behavioral data (Zuboff, 2019). Rather being merely passive supports for pre-existing forms of authority, these data infrastructures actively organize and mediate power relations by enabling, constraining, or redirecting action in particular ways, and may have geopolitical consequences (De Goede & Westermeier, 2022).

The second shift that characterizes governance in digital societies concerns the changing dynamics and functions of surveillance. If population-level surveillance has long been central to modern statecraft—from census infrastructures that rendered populations administratively legible and governable (Scott, 1998) to today's digital monitoring systems (Lyon, 2001)—contemporary AI systems move well beyond observation, quantification, and monitoring alone. Specifically, they seek to anticipate behavior, classify risks, and shape conduct in advance through predictive analytics, recommendation systems, nudging architectures, and automated decision-making processes (Amoore, 2018). Governance thus becomes anticipatory, intervening not only

on present behavior but also on possible future actions (Aradau & Blanke, 2022), often with significant social costs. Welfare fraud detection systems, for example, now combine administrative records, behavioral indicators, and ML models to identify individuals considered "high risk" before any wrongdoing has occurred. In the Netherlands, algorithmic risk profiling disproportionately targeted low-income and migrant families for fraud investigations in the *toeslagenaffaire* (childcare benefits scandal), resulting in wrongful accusations, severe financial hardship, family separation, and a profound erosion of trust in public institutions (van Schie et al., 2025).

The third shift highlights the move from extracting and analyzing data to generating synthetic forms of governance through AI systems themselves. "Synthetic" points to forms of governance in which AI systems do not merely process information about social reality, but actively shape the classifications, representations, decisions, and knowledge through which social reality becomes governable, including the data used to model social processes and craft adaptive policy responses. "Digital twins" are emblematic of this development insofar as they generate computational environments through which urban settings, infrastructures or populations can be simulated, optimized, and governed before interventions occur in physical space itself (Korenhof et al., 2025). Governance thus relies more on simulations of possible futures, raising important questions about accountability, participation, exclusion, and whose representations of reality become authoritative. AI systems no longer simply process and "make sense of" existing social realities; they contribute to administrative decision-making, public communication, classification, simulation, and knowledge production, (co-)shaping the realities they are meant to manage. Yet institutions are often ill-equipped to govern these transformations, with significant implications for democratic legitimacy and accountability (Beckman et al., 2024).

These transformations profoundly reshape the conditions under which individuals and groups act, participate, and understand themselves as political subjects. This is a core challenge for contemporary digital societies and is explored next.

Political Agency under Infrastructural Rule

The advance of intelligent systems in digital societies quietly but dramatically rewrites the relationship between citizens and the state in worrying directions, leading to what has been strikingly described as a state of "digital unfreedom" (Feldstein, 2019). In practical terms, people now navigate systems that monitor, predict, and shape their behavior, often without their full awareness or meaningful consent. As more decisions are delegated to data-driven systems, the very meaning and practice of citizenship are transformed (Hintz et al., 2018), reshaping in turn the conditions under which political agency is exercised. These transformations also alter the possibilities for political contestation and resistance.

To clarify this argument, it is useful to distinguish between political agency, contestation, and resistance, which stand in a nested relationship to one another. Political agency constitutes the broadest category, referring to the capacity of individuals and groups to interpret their conditions and act as political subjects within collective life (Emirbaye & Mische, 1988; Milan, 2018). Contestation identifies practices

that challenge, negotiate, or dispute existing arrangements of power, authority, and social ordering. Resistance refers to a more explicitly oppositional form of contestation, involving acts of refusal, disruption, evasion, or subversion directed at forms of governance perceived as unjust or harmful. Political agency makes contestation possible, and resistance is one possible form contestation can take. Yet not all political agency under AI-mediated governance is resistant, and not all contestation is overtly oppositional. For example, adapting strategically to algorithms can be understood as an expression of political agency; demanding transparency or accountability from algorithmic systems as a form of contestation, and tactics of obfuscation or sabotage as forms of resistance proper. Figure 1 illustrates this nested relationship.

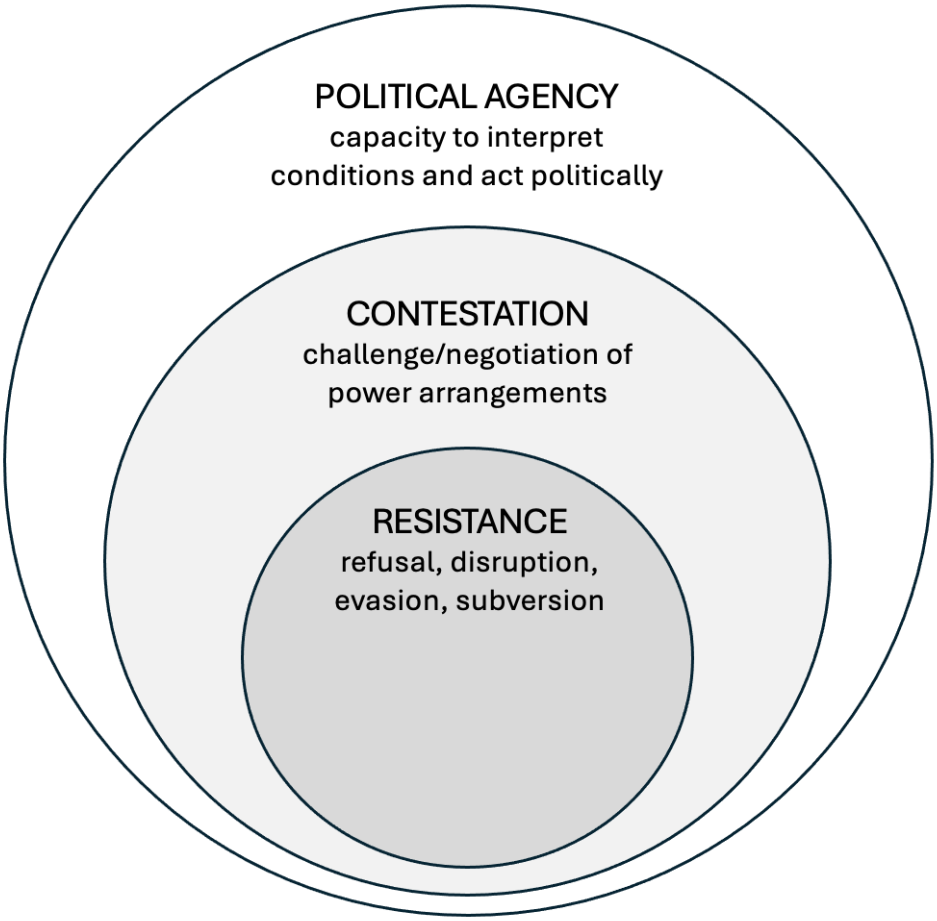

Figure 1. Nested relationship between political agency, contestation, and resistance under infrastructural rule.

AI-mediated governance reshapes political agency in multiple and interconnected ways, altering how citizens understand themselves, how they are governed, and how they relate to democratic institutions. Processes of subjectivation (through which institutions shape how people understand themselves and are recognized socially, Foucault, 1982) now configure citizens primarily as data subjects rather than political subjects. This is because social life is translated into categories, scores, and behavioral profiles that shape how individuals are understood by institutions (Dencik et al., 2018). As a result, recognition as a rights-bearing subject depends on scoring, profiling, and classificatory fit rather than being treated as an inherent condition of citizenship.

Meanwhile, new forms of governmentality emerge, that is, ways of governing populations by shaping behavior, managing risks, and steering conduct through data and prediction rather than through policy and coercion (Foucault, 1991; Rouvroy et al., 2013). Furthermore, the horizon of possible action narrows as citizens are channeled into predefined categories, risk profiles, and behavioral expectations, potentially constraining the capacity to imagine and enact alternative political futures. This dynamic becomes visible, for example, in the city of Amsterdam, where predictive approaches were used to identify 400 minors and young adults "whose behaviour is considered a nuisance to the city", enabling interventions based not on committed acts but on anticipated future risk, with the unintended effect of "draw[ing] more minors into the criminal justice system at an even earlier age"(Public Interest Litigation Project, 2022). In other words, the anticipatory labeling of individuals as potential offenders ended up reinforcing the very trajectories of criminalization it sought to prevent.

These developments also reconfigure trust in democratic institutions, a recognized challenge in digital societies augmented even further by the advance of AI (Altman, 2026). While data-driven governance may promise efficiency, objectivity, and evidence-based policymaking, it can also distance citizens from public authorities while undermining accountability and fairness through increased surveillance, opacity, and automated decision-making (Bradford et al., 2025; Huyskes, 2025). Yet trust is not merely an outcome of democratic governance; it is also a precondition for meaningful political agency, as citizens must be able to understand, contest, and rely upon the institutions that govern them.

These transformations alter not only the conditions under which political agency is exercised, but also the very logic of democratic contestation and resistance. Yet people are not merely passive recipients of AI-mediated governance. Despite the growing difficulties of articulating and enacting political agency under these conditions, such transformations also give rise to new forms of resistance (Bonini & Treré, 2024; Milan, 2024b), contestation (Beraldo & Milan, 2019), and rights-claiming (see Isin & Ruppert, 2020), ranging from everyday refusals to organized campaigns for transparency, accountability, and data justice (Dencik et al., 2019), as illustrated in the next section.

The New Logics of Resistance

Resistance is one expression of contestation, emerging when individuals or social groups oppose actions, norms, or forms of governance imposed by more powerful actors. It refers to intentional acts of opposition that stem from a refusal to conform to the status quo or to transformations perceived as unjust or harmful; it can take many forms, varying in visibility, organization, and degree of conscious intent (Hollander & Einwohner, 2004). Under conditions of infrastructural rule, however, resistance itself is transformed by the data infrastructures, predictive systems, and computational environments through which contemporary governance operates. As power becomes infrastructural, predictive, and synthetic, resistance also changes: it becomes more infrastructural and dependent, more anticipatory and evasive, and epistemic in orientation. The question is therefore not simply what forms resistance takes in digital

societies, but how the underlying conditions of resistance are reorganized when governance operates through infrastructural, predictive, and synthetic systems.

The following sections analyze three interconnected transformations of contemporary resistance that broadly mirror the transformations of governance discussed earlier in the chapter. Figure 2 summarizes this relationship.

It is important to note that resistance is not inherently democratic or emancipatory. The same infrastructures that enable democratic mobilization may also facilitate conspiratorial counter-publics, extremist mobilization, or AI-generated disinformation (e.g., Wack et al., 2025). While such anti-democratic forms of resistance are not the primary focus of this chapter, they remind us that resistance under infrastructural rule may serve both democratic and anti-democratic projects.

Governance transformation	Resistance transformation
Infrastructural governance	Infrastructural/dependent resistance
Predictive governance	Anticipatory/evasive resistance
Synthetic governance	Epistemic resistance

Figure 2. Relationship between transformations of contemporary governance and transformations of resistance.

i. Resistance to Infrastructural Power Turns Infrastructural and Dependent

As power becomes embedded in data infrastructures, resistance itself becomes infrastructural, that is, mediated by the very same infrastructures it seeks to contest. It no longer targets only identifiable institutions such as state agencies or corporations, but also the platforms, interfaces, data architectures, and computational systems through which visibility, participation, and access are organized in everyday life. Importantly, resistance is often *co-produced* by the very systems it seeks to challenge, as political action unfolds within privately governed computational environments that simultaneously enable and constrain dissent. Under AI-mediated governance, resistance thus becomes deeply ambivalent: it is enabled by the infrastructures through which contemporary political life unfolds (and that are difficult to avoid altogether), yet simultaneously constrained by their logics of surveillance and platform dependency. The 2019 Hong Kong pro-democracy protests, for example, relied heavily on online forums and platform-based coordination to organize collective action while simultaneously confronting pervasive digital surveillance, platform moderation, and facial recognition technologies deployed in public space (Y.-T. Li & Whitworth, 2023).

Some struggles target platform governance directly, challenging the concentration of power in privately owned digital ecosystems that mediate communication, participation, and access to information. This is well exemplified by the 2020 #StopHateForProfit campaign against Meta, which exposed the platform's role in amplifying hate speech and disinformation while urging corporations to suspend advertising on Facebook in protest against its permissive approach to harmful and misleading content (Y. Li et al., 2025). Concerns over the concentration of infrastructural power became visible also in campaigns opposing two Google-initiated projects, a Campus in Berlin and the Sidewalk Labs urban development project in

Toronto, both accused of extending corporate control and data collection over urban space (Charitsis & Laamanen, 2022). Contestation may also target the interfaces and algorithms through which users interact with digital systems, recognizing that seemingly mundane design choices shape visibility, accessibility, and possibilities for participation, thereby transforming platform architectures into political sites in their own right. Browser extensions and activist audits that reveal hidden recommendation logics seek to politicize platform interfaces themselves by exposing how public attention and perceptibility are computationally organized (e.g., Beraldo et al., 2021).

At the same time, infrastructural resistance also emerges through practices of refusal, evasion, and attempts to reclaim autonomy from systems that increasingly demand continuous participation and data extraction. Local mobilizations against data centers, for example, contest the environmental costs, resource consumption, and political concentration associated with large-scale computational infrastructures (Velkova, 2023). Acts of refusal range from opting out of data collection in the case of COVID-19 digital contact tracing (Lavorgna et al., 2021) to campaigns against biometric identification systems such as the pan-European *Reclaim Your Face* (2020). Relatedly, "algorithmic aversion", namely the reluctance to rely on automated systems in place of human judgement, particularly after perceived technological failures (Dietvorst et al., 2018), illustrates growing skepticism toward automated forms of governance and decision-making. Encryption technologies and privacy-enhancing practices similarly function as forms of infrastructural resistance as well, enabling users and activists to evade surveillance, evade machine detection, and protect spaces of communication from state and corporate monitoring (Ermoshina & Musiani, 2022). At the same time, struggles for data justice seek to expose and contest the unequal distribution of harms and benefits generated by data-driven systems, particularly for marginalized populations disproportionately targeted by surveillance, predictive policing, or automated welfare systems (for an overview, see Dencik et al., 2022).

As a result, resistance today centers on contesting the very terms of access, visibility, participation, and recognition within AI-mediated environments—specifically, who is seen, recognized, prioritized, or excluded by computational infrastructures themselves. What unites these practices is not their political orientation or tactical repertoire, but the fact that resistance increasingly operates through the manipulation of visibility, legibility, and infrastructural access.

ii. Resistance under Predictive Governance Becomes Anticipatory and Evasive

As governance increasingly operates through prediction, risk profiling, and anticipatory intervention, resistance itself becomes adaptive, evasive, and future-oriented. First and foremost, the temporal logic of resistance changes: rather than reacting to visible acts of repression alone, resistant actors must now confront systems that seek to pre-empt dissent in advance. In response, people engage in what has been termed "anticipatory data practices", namely future-oriented practices that provide individuals with concrete ways of navigating and acting amidst the persistent uncertainties of datafied environments (Kazansky, 2021). Examples include activists engaging in "threat modelling" and risk assessment to anticipate potential surveillance harms and adapt their communication practices accordingly, for instance by selectively using encrypted

messaging apps, avoiding insecure channels, or modifying organizational routines in response to perceived monitoring risks (Kazansky, 2021).

This transformation has important implications for the politics of visibility. Classical democratic resistance often relied on becoming publicly visible through demonstrations, occupations of public space, symbolic displays, and collective public presence. Under predictive governance, however, visibility itself can become a source of vulnerability, exposing resistant actors to monitoring, classification, and anticipatory intervention. Consequently, resistance increasingly shifts from strategies of public visibility toward practices of opacity, obfuscation, evasion, and strategic invisibility aimed at disrupting the predictive capacities of algorithmic systems.

Such practices take multiple forms. Anti-surveillance camouflage, for example, seek to confuse facial recognition systems by disrupting machine-readable patterns of identification. Critics, however, have warned against the "aestheticization of resistance premised on individual avoidance" (Monahan, 2015, p. 159), noting the risk that such tactics may privilege individualized evasion over collective political transformation. Other forms of resistance rely on obfuscation tactics that deliberately generate misleading, excessive, or ambiguous data in order to undermine profiling and behavioral prediction (Brunton & Nissenbaum, 2015). Both approaches can be understood as "everyday forms of resistance" (Scott, 1985): subtle, often hidden, and creative practices through which individuals seek to renegotiate asymetrical relations of power in datafied environments.

Activists and users may also try to "game" algorithms by manipulating recommendation systems, engagement rankings, or platform rankings to evade moderation or amplify marginalized voices. Relatedly, forms of "algospeak" (emergent coded language, symbols, and altered spellings designed to circumvent automated content-filtering systems) have been widely used during the war in Gaza by pro-Palestinian activists who experienced suppression or demotion of content on Instagram and TikTok (Farag et al., 2026). In other cases, resistant actors refuse classification altogether, resisting the categories through which predictive systems seek to produce authoritative knowledge about populations. Campaigns against biometric identification systems often challenge the very premise that individuals should be reduced to machine-readable identities and continuously verifiable data subjects, as illustrated by *Reclaim Your Face*, which opposed the normalization of biometric mass surveillance in public space.

Under predictive governance, resistance thus increasingly concerns the capacity to remain partially illegible to systems that seek to anticipate and modulate behavior before political action fully materializes. Invisibility, ambiguity, and opacity become not merely defensive reactions, but political tactics in their own right.

iii. Against Synthetic Governance, Resistance Becomes Epistemic

We have seen how opacity can function as a tactic of resistance. Yet opacity is also an epistemic condition of contemporary AI-mediated governance. If predictive governance seeks to anticipate and pre-empt action, synthetic governance generates probabilistic knowledge claims based on synthetic data and computational modelling, redefining the terms through which social reality itself is interpreted, known, and rendered authoritative. Yet these AI-generated simulations inform institutional decision-making

while remaining difficult to interrogate or contest. As a result, resistance itself becomes increasingly epistemic, targeting not only political decisions or institutional authority, but also the legitimacy of the knowledge claims, inferential logics, and epistemic assumptions through which AI systems produce authoritative accounts of reality. Political struggle therefore increasingly concerns who has the authority to produce knowledge about society, how truth claims are generated and validated, and whose experiences become credible, authoritative, or dismissible.

Epistemic resistance takes multiple forms. First, actors may directly challenge the epistemic authority of computational systems themselves, including the datasets and classificatory logics through which automated decisions are justified. Algorithmic audits and investigative research seek to expose biases, discriminatory effects, and hidden assumptions embedded in AI systems used in domains such as policing (Fussey & Murray, 2019 on facial recognition in London) or welfare allocation (López, 2020 on algorithmic poverty reduction in Colombia). Demands for explainability and contestability similarly challenge the opacity of automated decision-making systems, as illustrated by the work of Algorithmic Justice League (United States), which exposes how facial recognition systems reproduce racialized and gendered biases through opaque classificatory processes (Hooberman, 2021).

Second, epistemic resistance may take legal form by exploiting existing rights and regulatory mechanisms. This is visible, for instance, in General Data Protection Regulation (GDPR)-based claims under Article 22 concerning profiling and automated decision-making in the European Union. Third, epistemic resistance may intervene directly in public debate, exposing the unfairness and potential distortions of AI-mediated governance while seeking to inform and mobilize broader publics. In the Netherlands, the public backlash following the childcare benefits scandal became a powerful example of epistemic resistance against opaque data-driven classifications and automated suspicion in welfare governance (Ruigrok et al., 2025). These campaigns are made possible by concerted efforts involving advocates, journalists, researchers, and civil society organizations (e.g., Guo et al., 2025).

Conclusion: The Democratic Costs of Infrastructural Rule

This chapter has argued that in contemporary digital societies, resistance is transformed because power itself is transformed under conditions of AI-mediated governance. As governance becomes infrastructural, predictive, and synthetic, resistance also mutates, becoming more infrastructural and entangled with the systems it seeks to contest, more anticipatory and evasive, and increasingly epistemic in orientation. Resistance becomes more difficult not because dissent disappears, but because political action unfolds within privately governed computational environments that simultaneously enable and constrain contestation, while the conditions of public recognition and algorithmic detectability are continuously negotiated—often at democratic cost.

What becomes of democratic contestation when political agency and collective participation are increasingly shaped through computational infrastructures? More fundamentally, what happens to democracy itself when infrastructures begin to operate

as quasi-political authorities? Under infrastructural rule, democratic struggle no longer concerns only access to institutions, representation, or formal rights as we have known them thus far. It increasingly concerns the capacity to contest the computational systems through which social reality becomes actionable, interpretable, and governable, while reclaiming the conditions under which collective life itself remains politically imaginable.

These transformations carry significant democratic costs, which can be understood in relation to the three shifts in governance and the corresponding transformations of political agency, contestation, and resistance.

First, the growing dependence on privately owned and operated infrastructures contributes to an erosion of state sovereignty, as essential functions of governance increasingly rely on corporate platforms, proprietary systems, and external technical expertise. Relatedly, it also becomes more difficult to identify who governs, through which mechanisms, and according to which forms of legitimacy.

Second, predictive forms of governance contribute to the erosion of political agency and the narrowing of possible action. Political agency becomes infrastructurally mediated insofar as the capacity to participate, organize, communicate, and dissent depends on privately governed digital systems. Contestation itself becomes entangled with the infrastructures through which political life unfolds. Democratic contestation therefore increasingly unfolds around struggles over recognizability, epistemic authority, and political intelligibility: whose experiences become credible, whose knowledge counts, which forms of participation remain possible, and who becomes marginalized or computationally invisible within AI-mediated environments. At the same time, citizens are increasingly sorted into categories, risk profiles, and behavioral expectations that shape future opportunities and constraints.

Third, as governance enters the realm of synthetic and AI-generated forms of decision-making, democratic accountability and legitimacy are even further strained. Existing democratic institutions, built as they are around principles such as transparency, checks and balances, and separation of powers, are often ill-equipped to govern opaque, adaptive, and continuously evolving AI systems. Accountability becomes harder to sustain because power is distributed across complex socio-technical arrangements that frequently evade public scrutiny and democratic oversight.

Across all three dynamics, inequalities risk deepening as AI systems reproduce and amplify existing social biases, discrimination, and forms of exclusion (e.g., Benjamin, 2019; Eubanks, 2018; O'Neil, 2017). At the same time, societies increasingly become sites of continuous experimentation, where technical systems are effectively "beta-tested" (namely, deployed and refined through real-world use) in real-world conditions while simultaneously learning from and adapting to their own operation.

Figure 3 connects the transformation of governance and resistance to the related democratic implications.

Transformation in Governance	Characteristics	Transformation in Resistance	Illustrative Forms of Resistance	Democratic Implications
Infrastructural Governance	Governance operates through platforms, data architectures, and computational infrastructures	**Infrastructural /dependent resistance**	Opposition to data centers; platform governance activism; refusal of biometric systems; Encryption (…)	Dependence on private infrastructures; erosion of state sovereignty
Predictive governance	AI systems anticipate behavior, classify risks, and intervene pre-emptively	**Adaptive and anticipatory resistance**	Obfuscation; anti-surveillance camouflage; gaming algorithms; evasive tactics (…)	Erosion of political agency; narrowing horizon of possible action
Synthetic governance	AI systems generate simulations and knowledge claims that shape governable reality	**Epistemic resistance**	Algorithmic audits; challenges to AI-generated classifications; anti-AI campaigning (…)	Erosion of accountability and legitimacy; potential increase of inequality (*)

Figure 3. Transformations of governance, resistance, and democratic implications under infrastructural rule. (*) indicates that this item characterizes also infrastructural and predictive governance.

A central question remains how democratic institutions can preserve spaces for political agency, disagreement, and collective imagination in environments organized through prediction, computation, and synthetic forms of authority. The democratic challenge is no longer only how citizens resist power, but whether meaningful contestation remains possible when the infrastructures through which social and political life in digital societies unfold are themselves privately governed, predictive, and computationally opaque.

References

Altman, D. (2026). The AI Democracy Dilemma. *Journal of Democracy*, *37*(1), 32–44. https://doi.org/10.1353/jod.2026.a977942

Amoore, L. (2018). Cloud geographies: Computing, data, sovereignty. *Progress in Human Geography*, *42*(1), 4–24. https://doi.org/10.1177/0309132516662147

Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, *45*(2), 115–128. https://doi.org/10.1080/17439884.2020.1686014

Aradau, C., & Blanke, T. (2022). *Algorithmic Reason. The New Government of Self and Others*. Oxford University Press.

Beckman, L., Hultin Rosenberg, J., & Jebari, K. (2024). Artificial intelligence and democratic legitimacy. The problem of publicity in public authority. *AI & SOCIETY*, *39*(3), 975–984. https://doi.org/10.1007/s00146-022-01493-0

Benjamin, R. (2019). *Race After Technology*. Polity Press.

Beraldo, D., & Milan, S. (2019). From data politics to the contentious politics of data. *Big Data & Society*, *July/December*, 1–11. https://doi.org/https://doi.org/10.1177/2053951719885967

Beraldo, D., Milan, S., de Vos, J., Agosti, C., Nadalic Sotic, B., Vliegenthart, R., Kruikemeier, S., Otto, L. P., Vermeer, S. A. M., Chu, X., & Votta, F. (2021). Political advertising exposed: Tracking Facebook ads in the 2021 Dutch elections. *Internet Policy Review*. agosti

Bonini, T., & Treré, E. (2024). *Algorithms of Resistance: The Everyday Fight against Platform Power*. MIT Press.

Bradford, B., Kyprianides, A., Andrews, W., Aston, E., Clayton, E., O'Neill, M., & Wells, H. (2025). 'To whom am I speaking?'; Public responses to crime reporting via live chat with human versus AI police operators. *Policing and Society*, *35*(8), 1036–1052. https://doi.org/10.1080/10439463.2025.2453437

Braman, S. (2006). *Change of state: Information, policy, and power*. MIT Press.

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press.

Charitsis, V., & Laamanen, M. (2022). When digital capitalism takes (on) the neighbourhood: Data activism meets place-based collective action. *Social Movement Studies*, 1–18. https://doi.org/10.1080/14742837.2022.2123314

De Goede, M., & Westermeier, C. (2022). Infrastructural Geopolitics. *International Studies Quarterly*, *66*(3), sqac033. https://doi.org/10.1093/isq/sqac033

Dencik, L., Hintz, A., & Cable, J. (2019). Towards data justice: Bridging anti-surveillance and social justice activism. In D. Bigo, E. Isin, & E. Ruppert (Eds), *Data Politics. Worlds, Subjects, Rights* (pp. 167–185). Routledge.

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2022). *Data Justice*. Sage.

Dencik, L., Hintz, A., Redden, J., & Warne, H. (2018). *Data Scores as Governance: Investigating uses of citizen scoring in public services*. Data Justice Lab. http://orca.cf.ac.uk/117517/1/data-scores-as-governance-project-report2.pdf

Dietvorst, B. J., Simmons, J. P., & Massey, C. (2018). Overcoming Algorithm Aversion: People Will Use Imperfect Algorithms If They Can (Even Slightly) Modify Them. *Management Science*, *64*(3), 1155–1170. https://doi.org/10.1287/mnsc.2016.2643

Emirbaye, M., & Mische, A. (1988). What Is Agency? *The American Journal of Sociology*, *103*(4), 962–1023.

Ermoshina, K., & Musiani, F. (2022). *Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties*. Mattering Press. http://doi.org/10.28938/9781912729227

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Farag, T., Primig, F., & Badr, H. (2026). Algorithmic censorship, power, and resistance in the Arab region: A case study of pro-Palestinian content. *Communication, Culture and Critique*, *19*(1), 74–91. https://doi.org/10.1093/ccc/tcag003

Feldstein, S. (2019). The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression. *Journal of Democracy*, *30*(1), 40–52. https://doi.org/10.1353/jod.2019.0003

Flesher Fominaya, C., Milan, S., & Beraldo, D. (Eds). (2024). *Contentious Data in Movement*. Routledge.

Foucault, M. (1982). The Subject and Power. *Critical Inquiry*, *8*(4), 777–795.
Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon, & P. Miller (Eds), *The Foucault Effect: Studies in Governmentality* (pp. 87–104). University of Chicago Press. https://doi.org/10.7208/chicago/9780226028811.001.0001
Fussey, P., & Murray, D. (2019). *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf
Guo, E., Geiger, G., & Braun, J.-C. (2025, June 11). Inside Amsterdam's high-stakes experiment to create fair welfare AI. *MIT Technology Review*. https://www.technologyreview.com/2025/06/11/1118233/amsterdam-fair-welfare-ai-discriminatory-algorithms-failure/
Gutierrez, M. (2018). *Data activism and social change*. Palgrave MacMillan.
Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital Citizenship in a Datafied Society*. Polity.
Hollander, J. A., & Einwohner, R. L. (2004). Conceptualizing Resistance. *Sociological Forum*, *19*(4), 533–554. https://doi.org/10.1007/s11206-004-0694-5
Hooberman, L. (2021). The Coded Gaze: Algorithmic bias, facial recognition and beyond: How research can change the law and influence people. *Proceedings of the 13th ACM Web Science Conference 2021, WebSci '21*, 7–8. https://doi.org/10.1145/3447535.3468455
Huyskes, D. (2025). *Constructing Automated Societies. Socio-cultural Determinants and Impacts of Automated Decision-making in Public Services* [Università degli Studi di Milano]. https://air.unimi.it/handle/2434/1163995
Isin, E., & Ruppert, E. (2020). The birth of sensory power: How a pandemic made it visible? *Big Data & Society*, *7*(2), 2053951720969208. https://doi.org/10.1177/2053951720969208
Kaun, A., & Männiste, M. (2025). *Public sector chatbots: AI frictions and data infrastructures at the interface of the digital welfare state*. *27*(4), 1962–1985. https://doi.org/https://doi.org/10.1177/14614448251314394
Kaun, A., & Masso, A. (2025). *The Data Welfare State*. Sage.
Kazansky, B. (2021). 'It depends on your threat model': The anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society*, *8*(1), 2053951720985557. https://doi.org/10.1177/2053951720985557
Kazansky, B., & Milan, S. (2021). Bodies Not Templates: Contesting Mainstream Algorithmic Imaginaries. *New Media & Society*, *23*(2), 363–381. https://ssrn.com/abstract=3913234. https://doi.org/https://doi.org/10.1177/1461444820929316
Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big Data & Society*. https://doi.org/https://doi.org/10.1177/2053951714528481
Korenhof, P., Metcalfe, B., & Henschke, A. (2025). Cyber-governance of the natural world the implications of digital twins in environmental governance. *Earth System Governance*, *25*, 100276. https://doi.org/10.1016/j.esg.2025.100276
Lavorgna, A., Ugwudike, P., Carr, L., Benitez, Y. S., & Rekha, G. S. (2021). To app or not to app?: Understanding public resistance to covid-19 digital contact tracing and its criminological relevance. *Law, Technology and Humans*, *3*(2), 28–45. (informit.274942456322317).

Li, Y., Bernard, J.-G., & Luczak-Roesch, M. (2025). Explaining Differential Involvement in Cross-Movement Coalitions on Social Media: The #StopHateForProfit Campaign. *Trans. Soc. Comput.*, *8*(1–2). https://doi.org/10.1145/3689368

Li, Y.-T., & Whitworth, K. (2023). Coordinating and doxing data: Hong Kong protesters' and government supporters' data strategies in the age of datafication. *Social Movement Studies*, 1–18. https://doi.org/10.1080/14742837.2023.2178404

López, J. (2020). *Experimentando con la pobreza: El Sisbén y los proyectos de analítica de datos*. Fundación Karisma. https://web.karisma.org.co/wp-content/uploads/download-manager-files/Experimentando%20con%20la%20pobreza.pdf

Luusua, A., Ylipulli, J., Foth, M., & Aurigi, A. (2023). Urban AI: understanding the emerging role of artificial intelligence in smart cities. *AI & SOCIETY*, *38*(3), 1039–1044. https://doi.org/10.1007/s00146-022-01537-5

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press.

Masiero, S. (2024). *Unfair ID*. Sage.

Milan, S. (2018). Political agency, digital traces, and bottom-up data practices. *International Journal of Communication, Special Section'Digital Traces in Context', Edited by Andreas Hepp, and Andreas Breiter*, *12*, 507–525.

Milan, S. (2024a). Afterword: From Number Politics to Infrastructure Politics: Notes on Context and Methods. *The Cambridge Journal of Anthropology*, *42*(1), 118–126. https://doi.org/10.3167/cja.2024.420108

Milan, S. (2024b). Resistance in the data-driven society. Internet Policy Review. *Internet Policy Review*, *13*(4). https://doi.org/10.14763/2024.4.1811

Milan, S., & van der Velden, L. (2016). The Alternative Epistemologies of Data Activism. *Digital Culture & Society*, *2*(2), 57–74. https://doi.org/10.14361/dcs-2016-0205

Monahan, T. (2015). The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance. *Communication and Critical/Cultural Studies*, *12*(2), 159–178. https://doi.org/10.1080/14791420.2015.1006646

O'Neil, C. (2017). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Broadway Books.

Public Interest Litigation Project. (2022). *Top400. A top-down crime prevention strategy in Amsterdam*. https://racismandtechnology.center/wp-content/uploads/20221101-data-justice-lab-top400-report.pdf

Reclaim Your Face. (2020). *The problem. Secretive. Unlawful. Inhumane*. https://reclaimyourface.eu/the-problem/

Rouvroy, A., Berns, T., & Carey-Libbrecht, L. (2013). Algorithmic Governmentality and Prospects of Emancipation: Disparateness as a Precondition for Individuation through Relationships? *Réseaux*, *No 177*(1), 163–196. https://doi.org/10.3917/res.177.0163

Ruigrok, N., Van Atteveldt, W., Velden, M. V. D., & Van Hoof, A. (2025). Beware of the watchdog: Politics-media-politics dynamics in the Dutch childcare benefits scandal. *Journalism*, 14648849251387851. https://doi.org/10.1177/14648849251387851

Scott, J. C. (1985). *Weapons of the Weak: Everyday Forms of Peasant Resistance*. Yale University Press.

Scott, J. C. (1998). *Seeing Like a State*. Yale University Press.

Starke, C., & Lünich, M. (2020). Artificial intelligence for political decision-making in the European Union: Effects on citizens' perceptions of input, throughput, and output legitimacy. *Data & Policy*, *2*, e16. Cambridge Core. https://doi.org/10.1017/dap.2020.19

Ting, T.-Y. (2024). The pitfalls of smart urban infrastructure during a period of unrest: Networked dissent against smart lampposts in Hong Kong. *Journal of Infrastructure, Policy and Development*, *8*(9), 8313. https://doi.org/10.24294/jipd.v8i9.8313

van Schie, G., Candidatu, L., & Huyskes, D. (2025). Motherhood in the Datafied Welfare State: Investigating the Gendered and Racialized Enactment of Citizenship in Dutch Algorithmic Governance. In J. Van Dijck, K. van Es, A. Helmond, & F. N. van der Vlist (Eds), *Governing the Digital Society: Platforms, Artificial Intelligence, and Public Values* (pp. 209–225). Taylor & Francis.

Velkova, J. (2023). Retrofitting and ruining: Bunkered data centers in and out of time. *New Media & Society*, *25*(2), 431–448. https://doi.org/10.1177/14614448221149946

Wack, M., Ehrett, C., Linvill, D., & Warren, P. (2025). Generative propaganda: Evidence of AI's impact from a state-backed disinformation campaign. *PNAS Nexus*, *4*(4), pgaf083. https://doi.org/10.1093/pnasnexus/pgaf083

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Profile Books.