Routledge
Taylor & Francis Group

Urban Geography

Crisis as Catalyst, Infrastructure as Legacy: Post-pandemic Governance by Data Infrastructure and the Quiet Rewriting of Democracy

Submission ID	265194621
Article Type	Research Article
Keywords	regulatory data infrastructures, governance by data infrastructure, digital identity, facial recognition technology, normative foundations of democracy
Authors	Stefania Milan

Crisis as Catalyst, Infrastructure as Legacy: Post-pandemic Governance *by* Data Infrastructure and the Quiet Rewriting of Democracy

Stefania Milan
Department of Media Studies, University of Amsterdam
&
Florence School of Transnational Governance, European University Institute

Address:
Department of Media Studies
University of Amsterdam
Turfdraagsterpad 9
1012XT Amsterdam, The Netherlands

Email: s.milan@uva.nl

ORCID: 0000-0002-9314-2889

LinkedIn: https://www.linkedin.com/in/stefania-milan/

Abstract
Crises have long acted as catalysts for institutional change, reshaping how power is organized and exercised across territories, jurisdictions, and urban spaces. In this vein, the COVID-19 pandemic prompted the rapid deployment of digital tools for public health, safety, and efficiency, while serving as a beta-testing ground for new modes of urban governance. This article examines the deployment and afterlives of digital infrastructures introduced in Europe under conditions of crisis. It asks how COVID-era data infrastructures reshape democratic governance in cities and how their normalization recalibrates the normative foundations of democracy.

Dialoguing with critical data studies, urban geography, digital sociology, and democratic theory, the article develops the concepts of *regulatory data infrastructures* and *governance by data infrastructure* to trace how emergency technologies become durable fixtures of public administration and urban governance. Empirically, it draws on two pandemic-accelerated domains—digital identity systems and facial recognition in urban public space—as illustrative cases for theory development. Based on desk research, it shows how these systems reorganize state–citizen relations through spatialized practices of visibility, classification, and automation, and how they subtly rework democratic norms by embedding data-driven rationalities and private actors into everyday urban governance, thereby reshaping democracy from within the city.

Keywords
regulatory data infrastructures, governance by data infrastructure, digital identity, facial recognition technology, normative foundations of democracy

1. Introduction: The COVID-19 Crisis as Institutional Catalyst

At a Schengen border crossing in late 2025, non-European Union (EU) travelers step up to new self-service kiosks. Instead of a passport stamp, the EU's Entry/Exit System (ESS) records their fingerprints and facial image, adding another entry to a database that will track their movements for years (European Commission's Directorate-General for Migration and Home Affairs, 2025). Originally promoted as part of a broader turn to contactless border controls during the COVID-19 pandemic, biometric checks have now become routine infrastructure for governing mobility in Europe (eu-LISA, 2021). The emergency language has faded, but the systems remain, quietly reorganizing the everyday encounter between traveler and state.

Crises and emergencies have long functioned as catalysts for institutional change (Beckett, 2013). Mobilized as a technique of liberal governance (Anderson et al., 2019) and a diagnostic category for understanding the present (Roitman, 2013), crises expose the limits of existing governance arrangements while creating openings for (or even foreclosing) institutional and policy innovation. The COVID-19 pandemic (2019–2023), caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), was no exception. As the first pandemic to unfold under conditions of advanced datafication—marked by the pervasive transformation of social life into machine-readable data—COVID-19 not only exposed the limits of existing approaches to societal governance but also reconfigured the very means through which crisis governance was enacted. It functioned as an "all-encompassing stress-test of the cultural assumptions and foundations of society as a whole" (Milan & Di Salvo, 2020). It prompted the rapid deployment of data-centric digital tools, often powered by Artificial Intelligence (AI), to govern public health, social interaction, and urban mobility. Dashboards monitoring infection rates, wearable medical devices, contact-tracing apps, biometric systems like thermal cameras, vaccination certificates, and predictive analytics were rolled out at speed, frequently under conditions described as "innovation under pressure" (Newlands et al., 2020). In this context, concerns over privacy,

accountability, and democratic scrutiny were often temporarily suspended in favor of efficiency, safety, and problem-solving capacity (Kitchin, 2020).

While many of these measures were framed as exceptional and temporary, their afterlives often tell a different story. Although most national contact-tracing applications in Europe—such as Germany's *Corona-Warn-App* or Italy's *Immuni*—were decommissioned or placed in "hibernation" after the acute phase of the pandemic, the digital infrastructure underpinning them has persisted. For example, the Google/Apple Exposure Notification (GAEN) framework, which provided the proximity-tracking protocols for many European apps (Autoriteit Persoongegevens, 2020), remains embedded within dominant smartphone operating systems and continues to be maintained, constituting a durable technological substrate that can be rapidly reactivated at need.

This persistence reflects a form of infrastructural inertia, whereby crisis-built capacities are retained and rendered available for redeployment beyond their original purpose. In some cases, such redeployment occurred already during the pandemic itself. In both Singapore (Sato, 2021) and Germany (Pannett, 2022), data collected through contact-tracing applications were subsequently shared with law enforcement for crime prevention or investigation, contradicting earlier privacy guarantees (cf. Liu, 2021). Together, these cases illustrate how emergency digital infrastructures can exceed their original scope and become normalized within everyday governance, extending exceptional powers into the ordinary. Similar dynamics unfolded across other domains of pandemic governance, including the regulation of access and movement in cities.

A telling example is the expansion of QR-code–based access control systems. Technologies initially introduced during the pandemic to regulate entry to public venues such as restaurants, workplaces, and transport hubs, were rapidly scaled up to monitor compliance with health and safety measures. Beyond their immediate regulatory function, QR codes became woven into everyday urban routines, functioning as "public placemaking practices" shaping how access, presence, and legitimacy in space were negotiated (Davies et al., 2023). As with ESS, what began as an extraordinary response to an emergency thus contributed to the consolidation of data-driven infrastructures of rule. The pandemic operated as a large-scale beta-testing ground for governance innovations that now persist beyond the emergency context, embedding data-driven rationalities into core state functions.

This article offers a conceptual and theoretical analysis of the introduction and afterlives of crisis-induced data-centric interventions in the European context. Using pandemic-accelerated digital identity systems and facial recognition in urban public space as illustrative cases for theory development, and drawing on desk research, it examines how data-intensive infrastructures deployed during the pandemic have reshaped urban governance and state–citizen relations. It asks how the normalization of these infrastructures recalibrates the normative foundations of democracy as they become entrenched in everyday municipal administration and spatial regulation. Rather than treating these tools as discrete technologies, the article foregrounds their infrastructural and institutional effects, showing how emergency-driven digitalization and automation reconfigure accountability, participation, equality, and the rule of law through the governance of mobility, access, and visibility in the city.
To address these questions, the article advances two conceptual lenses—*regulatory data infrastructures and governance by data infrastructure*—using the COVID-19 pandemic as a case through which to further specify these concepts. Situated at the intersection of critical data studies, digital sociology, and urban geography, with selective engagement with democratic theory, it traces how crisis-driven infrastructures become durable components of urban governance, and how democracy itself is quietly rewritten from within urban space.

The article is organized as follows. First, it outlines the conceptual framework by introducing working definitions of regulatory data infrastructures and governance by data infrastructure, and by reflecting on crises as catalysts for institutional transformation and their consequences for democratic norms. Second, it presents the research approach. Third, it introduces the two empirical domains used to illustrate the claims. Finally, foregrounding the social costs of these two technologies, the article analyzes the shift from technology-centered interventions to institutional change in post-pandemic European democracy and reflects on the implications of this transformation for democratic quality and norms.

2. Conceptual Framework: Data, Crisis, and Democratic Governance

This article departs from the observation that technologies introduced to manage an extraordinary situation like the coronavirus pandemic became domesticated as routine instruments of public administration and spatial management, contributing to the consolidation of what can be described as governance by data infrastructure—with tangible consequences for urban governance and for democracy more broadly. This section outlines the analytical lenses underpinning the article, introduces its conceptual contribution, and situates them within broader debates on emergency governance and democratic norms.

Analytical Lenses for Data-Driven Urban Governance

This article dialogues primarily with critical data studies, digital sociology, and urban geography, seen as three complementary traditions concerned with how data-driven technologies reorganize power, space, and governance. Together, they enable an analysis of data-intensive digital systems as sociotechnical arrangements—configurations in which technological artefacts, institutional practices, and political rationalities are jointly produced (Bijker, 1997)—that reshape institutional practices and everyday life, particularly in the urban environment, where infrastructures, populations, and governance intersect most visibly.

Critical data studies (Dalton et al., 2016; Kitchin, 2025) foreground the social and political consequences of datafication and automation, emphasizing how data-driven systems encode values, redistribute authority. This perspective draws attention to the "politics of" data infrastructures across their life course, highlighting tensions between deployment, stabilization, and post-crisis normalization (Ruppert et al., 2017). Digital sociology (Marres, 2017) focuses on how technologies are enacted in practice and how, through everyday arrangements, they organize participation and accountability and become incorporated into social institutions and routines (Lupton, 2015). In this article, it contributes to understanding how citizen agency is constituted in relation to the structural logics of both technological systems and state institutions. Finally, urban geography adds a crucial spatial and infrastructural perspective by treating cities as key sites of experimentation, scaling, and normalization of governance arrangements, including surveillance (Graham & Marvin, 2001; McFarlane, 2021). It centers infrastructural power (Easterling, 2016) and the governance of circulation across the urban environment (Wiig & Wyly, 2016). From this multidisciplinary vantage point, the digital tools examined here can be seen as sociotechnical infrastructures of urban ordering: (politically contested) systems that materialize data-driven rationalities through everyday practices, embed themselves within state and urban institutions, and reorganize the governance of mobility, visibility, access, and public space.

Within this framework, the article advances two closely connected analytical concepts, namely *regulatory data infrastructures* and *governance by data infrastructure*, developed to capture emerging modes of crisis-induced, data-driven governance.

Regulatory data infrastructures are combinations of software, hardware, standards, institutional arrangements, and social practices through which data are generated and operationalized to exercise regulatory power (Milan, 2024a). They increasingly take up functions once performed by public authorities and human decision-makers, including population monitoring, public safety, access to services and rights, and administrative decision-making. Here, regulatory power refers to the capacity to govern conduct by embedding rules, norms, and decision logics into infrastructures that monitor, classify, and intervene in social life. Exercised through data-driven systems rather than exclusively through law or policy, this form of regulatory power shapes how individuals and populations are rendered (in)visible, governable, and actionable within institutional and spatial arrangements. In this respect, it operates through what Isin and Ruppert term "sensory power": the ability of "detecting, identifying, and making people sense-able" through infrastructural means (Isin & Ruppert, 2020, p. 2). Simultaneously, it functions as a modality of governmentality (in the Foucauldian sense), through which power is exercised via the coordination of knowledge, infrastructure, and administrative routines rather than overt coercion (Rahman et al., 2024)—though not without social costs.

Governance *by* data infrastructure refers to a broader mode of governing in which regulatory data infrastructures become the preferred means for managing complexity (Milan, 2024b). It is characterized by reliance on real-time data generation and analysis, automated processes, and anticipatory logics (Aradau & Blanke, 2017), alongside the growing penetration of private vendors—who develop and operate regulatory data infrastructures—into state institutions, including welfare, security, and urban management. In this context, regulatory power is increasingly operationalized through system architectures rather than articulated through deliberative or territorially bounded forms of rule (Yeung, 2017). This reflects "a shift toward a special form of design-based governance, with power exercised ex ante via choice architectures defined through protocols, requiring lower levels of commitment from governing actors" (Gritsenko & Wood, 2020, p. 1). As a result, regulatory authority is often embedded in technical arrangements that bypass routinized checks and balances, weakening democratic accountability and the capacity for public contestation. Typically forged under emergency conditions, this mode of governance tends to outlast the crises that gave rise to it, becoming embedded in everyday administrative routines.

Crisis, Emergency Logics, and Infrastructural Change

Crises point to "overwhelming situations and elements of urban life that individuals and societies are forced to cope with everyday" (Dimitrakou & Ren, 2025, p. 2). They are not merely external shocks but critical turning points that expose the limits of existing modes of regulation and knowledge: "moments of truth" that evoke a moral demand for a break between past and future (Roitman, 2013). They create conditions under which new forms of governance—today more often than not infrastructural and data-driven—can be rapidly introduced and stabilized. In this sense, crises operate as both openings and closures for institutional innovation, lowering barriers to technological and policy adoption. Under conditions of radical uncertainty, governing rationalities shift from managing what is probable to anticipating what is possible, privileging surveillance, prediction, and automation as means of navigating risk (Aradau & Van Munster, 2011; Beck, 1992). Crises may also legitimize intensified surveillance and the delegation of public functions to private actors (Lyon, 2022). Measures introduced as temporary responses to exceptional circumstances often persist, becoming normalized within administrative routines and infrastructural arrangements (Agamben, 2005), thereby extending emergency governance into routine urban administration.

Crises are discursively constructed and politically mobilized through narratives that frame situations as requiring immediate action, and renew the authority of policymakers to intervene

decisively (Rahman et al., 2024). While such narratives help mobilize resources and focus attention, they do so at the expense of complexity (Roe, 1995), narrowing the range of legitimate responses and privileging solutions that are readily actionable. Crisis narratives also have a performative function: when confronted with "mega hazards" that escape established institutional practices of administrative management, institutions continue to act as if they are in control (Mythen & Walklate, 2016, p. 405).

The coronavirus pandemic functioned as a large-scale testing ground for an unprecedented digitalization of the social sphere (Yan, 2020), spearheading data-centric governance and accelerating the consolidation of this infrastructural mode of governing. COVID-19 crisis narratives activated emergency logics and "states of exception" that suspended or reordered established political and legal safeguards (Pellizzoni, 2020), thereby legitimizing rapid techno-solutionist interventions. These interventions foregrounded techno-infrastructural fixes while sidelining democratic deliberation and constraining public scrutiny (Bigo, 2020; Milan, 2020). At the same time, the crisis lowered thresholds for both the adoption and social acceptance of such fixes by reframing privacy trade-offs as necessary or unavoidable (Madianou, 2020).

Cities emerged as privileged sites for experimentation, scaling, and normalization, as municipal authorities mobilized regulatory data infrastructures, including pandemic technologies such as QR codes, thermal cameras, and facial recognition systems, to manage circulation, enforce health measures, and render populations legible in real time. In doing so, these infrastructures reordered visibility, mobility, and access, embedding emergency rationalities into the everyday governance of urban space and populations, with particularly severe consequences for marginalized communities within racialized assemblages, as well as for the urban poor, informal economy workers, older adults, and people with disabilities (for a selection of case studies, see Milan, Treré, et al., 2021; Mukogosi, 2021; Pelizza et al., 2021).

Fast forward to today, the institutionalization of crisis-driven regulatory data infrastructures in European post-pandemic democracy marks a shift from discrete technological interventions to a more enduring mode of governance by data infrastructure, with consequences that extend well beyond efficiency or effectiveness. These developments transform not only the modalities of governance, but also the democratic norms through which such arrangements are assessed and contested—raising questions about the normative foundations of democratic governance.

Democratic Norms at Stake?

Democracies depend not only on formal institutions (e.g., parliaments and legal frameworks) but also on shared informal norms (i.e., unwritten conventions guiding behavior and practices in democratic societies) that constrain the exercise of power (Levitsky & Ziblatt, 2018). The normative foundations of democracy refer to the fundamental standards, ethical principles, and values that define how democracy should function, including equality, justice, civil liberties, political participation, public deliberation, and the rule of law. Together, these foundations provide a framework for assessing whether a political system or decision is democratic and fair, while shaping expectations about how power is distributed and exercised in a democratic society (cf. Dahl, 1998; Diamond & Morlino, 2004; Rawls, 1999).

In crises, these norms are particularly vulnerable, as governments tend to expand executive authority and intensify domestic surveillance, among other exceptional measures (Scheppele, 2004). When emergency responses are operationalized through data-driven infrastructures, these s often become embedded in administrative routines and material arrangements that are difficult to contest or reverse. In this way, crisis-induced infrastructural

governance recalibrates democratic norms by reshaping how accountability is exercised, how participation is organized, and how rights are mediated in practice.

Much like the incorporation of AI into state machinery (Allen & Weyl, 2024), governance by data infrastructure alters the normative foundations of democracy not through overt institutional reform but through incremental shifts in how power is exercised, mediated, and legitimized. Rather than replacing democratic institutions—or constituting the "end of government" (Araya, 2019)— data infrastructures increasingly operate within them, reworking core democratic norms as decision-making, classification, and enforcement are inscribed into sociotechnical systems. These transformations extend beyond formal guarantees to reshape the informal conventions and expectations through which democratic life is enacted, reworking everyday state–citizen relations and raising questions about state sovereignty.

3. Methodological Note

This article adopts a qualitative, theory-driven research and primarily conceptual design. It mobilizes digital identity systems and facial recognition in urban public space, both expanded during the pandemic, as illustrative sites for theory development. These sites are used analytically to refine and substantiate the article's conceptual argument, illustrating how governance by data infrastructure materializes in practice and how crisis-induced digital interventions acquire institutional afterlives. They are not treated as full-fledged empirical case studies, but as analytically generative examples that help trace the normalization of data-intensive infrastructures and their implications for democratic norms in urban governance.

The analysis draws on desk research, including analysis of policy, advocacy, media, and industry material released in the period 2019-2025, to examine how data-driven technologies are framed, justified, and gradually institutionalized over time, surfacing, among others, the rationales accompanying their deployments.

4. Domain I: Digital Identity Systems

Digital identity (ID) systems refer to digital infrastructures designed to verify and authenticate individuals through software-based processes, typically without direct human involvement at the point of verification. They are commonly built upon registration procedures linked to official credentials (e.g., national ID cards or passports) and may incorporate biometric authentication mechanisms such as fingerprints or iris scans. They are often promoted as balancing data security with portability and interoperability, enabling identities to be reused across institutional contexts.

In democratic systems, digital identity infrastructures play a central mediating role by governing access to both public and private services. They condition interactions with government institutions, including access to healthcare, welfare provision, taxation, and education, while also increasingly serving as gateways to commercial services such as banking and insurance. In this sense, digital identity systems do more than record or represent identity: they perform acts of certification and denial, linking individuals to opportunities, entitlements, and forms of participation, while simultaneously excluding those who cannot be verified or authenticated. As such, they constitute a key site where regulatory power—specifically the state's power of classification (Cheesman, 2022)—is exercised through infrastructural means.

Examples include nationwide systems such as the publicly operated Dutch DigiD (digid.nl), the Italian *Sistema Pubblico di Identità Digitale* (spid.gov.it, which, contrary to its name, is operated by accredited contractors in exchange for a fee), the Swedish BankID (bankid.com, a banking-sector system requiring users to be customers of a participating bank), and India's Aadhaar (uidai.gov.in). At the supranational level, efforts to establish a unified digital ID infrastructure are

underway in the EU through the proposed EU Digital Identity Wallets (EUDI), envisioned as interoperable infrastructures enabling citizens to prove their identity and credentials across member states (European Commission, 2021). Commercially issued initiatives, supported by multilateral organizations like the World Bank's Identification for Development programme or public-private partnerships like ID2020 (with Microsoft and Accenture, among others), promote digital identification as the basis for service delivery in a response to inefficient public administrations in developing countries (Center for Human Rights & Global Justice, 2022).

Digital identity infrastructures vary substantially in theirs design and governance, ranging from publicly operated systems to privately intermediated, commercially supported, and hybrid arrangements, and may be introduced through administrative rollout, executive degree, or parliamentary debate (Lawani et al., 2026). These systems support a wide range of uses. They are often linked to biometric technology, such as fingerprint identification, in the administration of voting rights—a practice prevalent in many developing countries, particularly in Africa (Passanti, 2025). Digital ID infrastructures are also used by state entities and humanitarian organizations to manage refugees and migration flows (Schoemaker et al., 2020). During the COVID-19 pandemic, the scope expanded further through vaccination certificates, which linked identity verification to public health status and conditioned access to services and public spaces (Milan, Taylor, et al., 2021).

In fact, while digital identity solutions predated COVID-19, the pandemic accelerated their adoption and institutionalization by creating practical pressures and political justifications, especially where physical access to services was limited. According to industry reporting, 72 percent of online marketplaces adopted identity verification systems during the first seven months of the pandemic alone ("COVID-19 Driving an Acceleration in Adoption of Identity Verification," 2020). Governments likewise intensified their engagement with digital ID infrastructures. In Canada, for instance, the pandemic created what observers described as "the right conditions for excuses to be removed" (Nardi, 2020), prompting policymakers to pilot and expand digital identity solutions as part of broader digital government strategies (Government of Canada, 2023). Similarly, the European Commission advanced plans for EUDI, framing it as essential infrastructure for secure access to services and cross-border mobility in a post-pandemic digital single market (European Commission, 2021).

5. Domain II: Facial Recognition Technologies

Automated facial recognition technology is a form of biometric identification that enables "identifying people with machines" (Breckenridge, 2014). It works by establishing a probabilistic link between bodily features, most commonly the human face, and images stored in databases such as passport or social security registries. As an AI application, facial recognition relies on machine learning models trained on large datasets to detect and compare selected facial markers, producing likelihood scores rather than definitive identifications. This probabilistic logic is central to both the appeal and, as we shall see, the democratic risks of the technology.

Although facial recognition technologies were already diffusing prior to COVID-19, the pandemic accelerated their expansion in urban public space and beyond (Van Natta et al., 2020). For example, US schools used facial recognition software to scan foreheads for elevated temperatures and detect when students aren't wearing masks (Barber, 2020); across the world, "proctoring" software relying on facial recognition and environment monitoring was adopted by universities worldwide to invigilate exams (Swauger, 2021). More broadly, systems that had previously been tested through limited pilots were rapidly scaled up and deployed in strategic sites of public assembly—transport hubs, conference centers, concert halls, and football stadiums—to monitor compliance with health and safety measures. Often, facial recognition was

combined with thermal scanning technologies, justified by emergency logics of risk management. As the crisis subsided, these systems were folded into routine forms of spatial regulation, where they continue to be used for surveillance, security, and population management.

In urban contexts, facial recognition today is mainly used to grant access to spaces or services, such as access control or payment systems. In Europe, typical deployment scenarios include transport hubs, where facial recognition is used to authenticate passengers; schools, where it is used at entrances or for cashless payments; and squares to monitor passers-by (Christakis et al., 2022; Solarova et al., 2023; Kayali, 2023). But the technology is also well integrated into everyday policing practices: it is central to the EU Prüm II framework regulating automated data exchange for police cooperation (European Parliament, 2024), although the AI Act has introduced limits to its adoption in public space, including prohibitions on "the untargeted scraping of facial images from the internet or CCTV footage" and on certain forms of emotion inference (Article 5, EU Artificial Intelligence Act, 2025).

Facial recognition technologies thus provide a critical lens on how regulatory data infrastructures quietly reconfigure the boundaries of acceptable state intervention in public space. They foreground how emergency logics can legitimize intrusive forms of data-driven governance, how temporary measures become embedded in routine administrative practices, and how citizens are positioned, often retrospectively, in relation to infrastructures that profoundly affect rights, freedoms, and participation in democratic life.

6. The Quiet Rewriting of Democracy: From Technology to Institutional Change

This section advances the core argument of the paper: crises function as catalysts for institutional change, and that what may appear as infrastructural transformation in fact signals a deeper reconfiguration of democratic governance. To substantiate this claim, the following section examines the social costs of two pandemic-accelerated regulatory data infrastructures—that is, how harms are experienced by individuals and social groups—and then extends to the analysis of democratic harms, understood as the effects these technologies have on democracy as a system. In-between, this part of the paper reflects on the role of crises in this process.

The Social Costs of Regulatory Data Infrastructures

Across both empirical domains, the quiet rewriting of democracy materializes through a set of recurring social costs. These costs are not incidental side effects but arise from how regulatory data infrastructures condition access, redistribute power, and reorganize everyday encounters between citizens and the state.

a. Conditional Inclusion and Exclusion

Regulatory data infrastructures reconfigure inclusion and exclusion by conditioning access to rights, services, and public space on successful identification and authentication. In the case of digital identity systems, individuals lacking documentation, digital literacy, or reliable connectivity, or whose data are inaccurate, incomplete, or contested, risk exclusion from essential services, often reinforcing existing inequalities (Masiero, 2024). Pandemic vaccination certificates illustrate how identity infrastructures can operate performatively, producing real-time distinctions between legitimate and illegitimate access and transforming public health status into a gatekeeping mechanism for social participation (Milan, Taylor, et al., 2021). As urban scholarship on smart governance suggests, such data-driven systems tend to produce conditional and uneven forms of urban citizenship, amplifying existing social hierarchies by making marginalized residents selectively visible, governable, or excludable within digital infrastructures (Datta, 2018).

Facial recognition technologies enact similar dynamics through spatialized forms of identification. Their technical functioning is marked by well-documented problems of accuracy and bias, undermining the democratic principle of equality before the law. Because these systems rely on measurements between selected facial points rather than holistic analysis, errors are structurally embedded and unevenly distributed across populations. Biased training datasets have repeatedly resulted in higher misidentification rates for racialized and marginalized groups, as well as gender non-conforming individuals, producing differentiated exposure to surveillance and sanction (Buolamwini & Gebru, 2018). A Dutch university, for instance, was accused of discriminating against non-White students through its proctoring software (Damen, 2022). In both domains, inclusion becomes conditional upon machinic legibility, with profound consequences for social participation and recognition.

b. Scope Creep and Functional Expansion

Once established for a limited purpose, regulatory data infrastructures are prone to scope creep: they are extended to new domains, linked to additional datasets, or repurposed for functions beyond their original mandate (Center for Human Rights & Global Justice, 2022). As these expansions unfold, infrastuctures introduced as temporary of exceptional measures often solidify into durable institutional arrangements, frequently without renewed democratic debate, robust oversight, or meaningful opportunities for citizen contestation. In the case of digital identity systems, this process is often mediated through municipal platforms, smart city infrastructures, and service delivery systems, incrementally embedding identification into everyday practices of urban governance and intensifying forms of surveillance urbanism. What begins as an administrative convenience or emergency measure thus becomes a routine feature of governance.

Facial recognition technologies display similar patterns of functional expansion. Initially framed as experimental or exceptional tools, they have been progressively normalized across urban management contexts, security, and policing, a development critics have linked to the "reinvention of suspicion and discretion" in law enforcement (Fussey et al., 2021). Notably, this normalization has sometimes occurred despite well-documented performance limitations. In London—one of the earliest urban adopters—live facial recognition was deployed via CCTV cameras even though early evaluations reported an accuracy rate of only 19 percent (Fussey & Murray, 2019). Taken together, these cases illustrate how emergency-driven technological experimentation translates into enduring infrastructures of governance, exemplifying function creep whereby provisional measures become embedded institutional practices.

3. Diminished Accountability and Contestability

Regulatory data infrastructures also raise fundamental concerns about accountability and contestability. As rules, classifications, and access decisions are encoded into technical systems and delegated to software-mediated processes, opportunities for oversight, redress, and democratic deliberation are curtailed. Inclusion, exclusion, and verification are increasingly enacted through infrastructural arrangements that are difficult to interrogate or contest, particularly where private vendors and transnational actors play a central role in system design and operation. As Madianou (2019, p. 10) observes, such systems risk "ossify[ing] discrimination by turning soft data into a permanent, 'scientific' record that is hard to contest."

In the domain of facial recognition, accountability is further weakened by automation bias, whereby human operators defer to algorithmic outputs even when these conflict with their own judgment (Gebru, 2020). This deference shifts authority from accountable public officials to opaque technical systems, undermining transparency, due process, and avenues for redress in high-stakes decision-making contexts. Moreover, facial recognition enables forms of

"generalized, population-level monitoring" (Andrejevic & Selwyn, 2020), chilling the exercise of fundamental democratic rights such as freedom of expression, assembly, and dissent. Through continuous identification and tracking, urban public space risks being transformed from a site of civic encounter into a zone of anticipatory compliance, reshaping the relationship between citizens and the state (Andrejevic & Selwyn, 2022).

The contested nature of these infrastructures underscores these accountability gaps. Digital identity systems have been challenged for their intrusiveness, as in Aadhaar's biometric authentication (Chaudhuri & König, 2018), and for design choices—such as those underpinning the EUDI framework—that raise concerns about fairness, privacy, security, and stakeholder input (Royo, 2025). These vulnerabilities are not merely theoretical. In 2025, the bid by the US firm Kyndryl to acquire the Dutch company Solvinity, which operates the platform underpinning DigiD, sparked public debate in the Netherlands over digital dependency, sovereignty, and infrastructural vulnerability ("Dutch Governments Caught off Guard by American Tech Firm Buying Dutch Cloud Company," 2025). Similarly, in the context of facial recognition, the normalization of these systems has equated "arsenic in the water supply of democracy" (Sample, 2019) by the British non-profit Liberty, and prompted growing public criticism and mobilization, including the EU-wide *Reclaim Your Face* campaign (reclaimyourface.eu) and calls for a ban by Amnesty International on the ground that it "amplifies racist policing" (2021).

The social costs associated with regulatory data infrastructures are not merely distributive or technical side effects; they constitute the pathways through which democratic harms take shape. Exclusion from services, heightened surveillance, and the opacity of automated decision-making are experienced unevenly across social groups, yet their cumulative effect is systemic. As these costs become embedded in routine governance, they normalize unequal access to rights, weaken mechanisms of accountability and redress, and reshape participation along infrastructural lines. In this sense, social costs operate as the everyday manifestation of deeper democratic harms, translating infrastructural change into durable transformations of democratic life. This reconfiguration takes place through the gradual sedimentation of crisis-induced infrastructures, quietly rewriting democratic governance from within.

Negotiated Afterlives of Crisis Infrastructures: From Crisis to Institutional Change

A central mechanism through which this quiet rewriting unfolds is crisis-driven digitalization. A report by civil society organizations has denounced the expansion of executive powers and the suspension of the rule of law during the COVID-19 pandemic, noting that these developments have been accompanied by an intensification of security protocols and the rapid scaling of surveillance technologies, with implications for fundamental rights (European Center for Not-For-Profit Law et al., 2022). Across both empirical domains, this critique resonates with the persistence of infrastructures introduced as temporary, exceptional, and ostensibly proportionate responses to the pandemic, which have endured well beyond their initial justification.

The infrastructural inertia of facial recognition technology offers a particularly instructive illustration of how promises of temporariness and proportionality tend to unravel in practice. Framed as a tool for efficiency and control (Security Industry Association, 2023), once established the technology generates institutional dependencies, sunk costs, and political incentives for reuse and expansion. While European advocates—most notably those united under the umbrella of *Reclaim Your Face*—have contributed to the gradual emergence of new vocabularies of fairness, rights, and democratic control, these efforts also expose persistent blind spots regarding the broader social costs of infrastructural governance. Both media outlets and policymakers tend to emphasize modernization and innovation, frequently amplifying industry marketing while sidelining concerns about exclusion, discrimination, and chilling effects. The

installation of thermal facial recognition cameras in the Olympic Stadium in Rome in 2021, for instance, was publicly celebrated as a "symbolic moment" and "the light at the end of the tunnel" for the country as a whole (Bianchi, 2021).

These dynamics are particularly visible in urban governance, where crisis-driven systems are most likely to be introduced and subsequently normalized. Cities have long functioned as key sites for experimentation with data-driven governance, with urban management increasingly organized around data collection, platformization, and real-time monitoring (Wiig, 2015). In this context, regulatory data infrastructures operate not merely as administrative tools but as spatialized instruments of power, shaping how urban populations are seen, sorted, and governed. As Pickren (2016) argues, power in data-driven cities circulates through infrastructural assemblages rather than residing in single institutions or actors. Crisis infrastructures such as digital health certificates and facial recognition systems become embedded in these assemblages, intersecting with transport systems, policing practices, and public–private partnerships. Their negotiated afterlives reconfigure urban governance by redistributing authority across municipal agencies, technology vendors, and security actors, while simultaneously constraining the capacity of urban residents to contest—or even opt out of—these infrastructural forms of regulation. This dynamic is evident in cases such as Como (Italy), where the local administration unlawfully deployed facial recognition cameras, sponsored by the Chinese firm Huawei, across parks, stations, and squares (Carrer et al., 2020). In this sense, the afterlives of crisis infrastructures reveal how urban governance becomes a privileged site for the quiet rewriting of democracy: a domain where exceptional measures sediment into routine practices, where democratic norms are enacted through spatialized data systems, and where the cumulative effects of infrastructural governance become most acutely felt—particularly in the configuration of state–citizen relations.

From Technologies to State–Citizen Relations

Across both empirical domains, governance increasingly operates through data-intensive infrastructures that make citizens visible, classifiable, and "actionable" in ever more comprehensive ways. Visibility is produced through continuous data capture; classification through algorithmic categorization of identity, risk, and eligibility (Bowker & Star, 1999); and automation through the delegation of regulatory functions to computational systems (Bellanova & de Goede, 2020). Individuals and groups that are remain illegible to these infrastructures—think of undocumented migrants (Pelizza et al., 2021)—become the new "data poor", effectively excluded from rights claims and forms of political recognition (Milan & Treré, 2020).

These shifts do not merely optimize existing practices; they reshape how state authority is exercised and experienced, *altering the terms on which citizens encounter the state* in at least two ways. At a basic level, this concerns the channels through which state–citizen interaction is organized. As advocate Denis Royo (2025) notes with respect to EUDI, "The motivation behind EUDI is that of achieving strategic autonomy for our public and social services, but its realization goes in the opposite direction, effectively putting in the hands of mobile OS [Operating System] manufacturers core interaction channels with the institutions governing our society". Infrastructure design choices matter, since "by changing the design of the networks (…), its politics are affected—the balance of rights between users and providers" (Musiani, 2013). Millimeter wave scanning, a biometric-adjacent technology used in airport security checks, exemplify the downstream effects of this dynamic: systems optimized around binary, gendered body-shape assumptions tend to flag non-binary individuals as deviant, with such deviations interpreted within security logics as potential risk indicators (Costanza-Chock, 2018). Yet the implications of these developments extend well beyond questions of access and interface design.

On the one hand, democratic systems are not optimized for infrastructural mediation, and we lack adequate processes and tools to contend with decisions taken seemingly independently by technology itself. This becomes particularly problematic when state–citizen relations are no longer mediated primarily through law, discretion, and face-to-face interaction, but increasingly through system architectures, databases, and automated decision-making (Hintz et al., 2018). Infrastructural mediation often entails greater opacity in decisions affecting individuals and increased difficulty in seeking redress, as data infrastructures obscure how decisions are made and where responsibility lies (Eubanks, 2018).

On the other hand, infrastructural mediation subtly reconfigures the balance between trust, control, and accountability that underpins democratic governance. Trust and control are redistributed both within the state and beyond it, since regulatory data infrastructures are often developed and operated by private contractors. Accountability is thereby weakened, since forms of "regulation by contract" (cf. Bygrave, 2015) introduce actors that fall outside established democratic mechanisms of oversight and control, such as parliamentary oversight and electoral processes.

Trust nonetheless plays a central role in the justificatory narratives surrounding these systems. In the documents reviewed for this research, the EUDI framework is consistently presented as a means to enhance trust and security for e-commerce and e-government (European Commission, 2021). This framing reveals a paradox: the state reasserts itself as provider and guarantor of trust vis-à-vis the market, yet does so through infrastructures largely supplied by private actors. Framed as a "trust framework", EUDI positions the state as an intermediary between citizens and third parties, while effectively displacing trust from institutional relationships onto technical systems. Crucially this shift is not limited to state–citizen relations; it signals a broader epistemic transformation of the state itself.

Political Rationalities and Epistemic Transformation

The expansion of regulatory data infrastructures reflects and reinforces *shifts in political rationalities*, reshaping how public problems are framed, which solutions are imagined and appear legitimate, and how authority exercised in practice. As regulatory capacity becomes anchored in technocratic expertise, governance priorities are increasingly shaped by infrastructural dependencies and expert systems, constraining political discretion and deliberation (cf. Friedman, 2019). This dynamic aligns with the predominant "smartness" agenda, whereby technical expertise, automated systems, and performance metrics come to dominate governance, narrowing the space for political deliberation and alternative problem framings (Mitchell and Halpern 2023).

Facial recognition technologies—described by privacy advocates as "inhumane" (Reclaim Your Face, 2020)— offer a concrete illustration of these shifts. Rather than responding to identified violations, such systems continuously scan and classify individuals to anticipate potential risks. Decisions rely on probabilistic matches, confidence thresholds, and risk scores, meaning that intervention is justified by what systems predict might occur rather than what has occurred. Hence, suspicion becomes embedded in infrastructure, and authority is exercised through technical systems that claim legitimacy based on predictive accuracy and operational efficiency.

These dynamics are especially visible where facial recognition is integrated into digital identity infrastructures. Here, access to rights, services, or transactions depends on automated identity verification processes that rely on probabilistic assessments rather than documentary evidence or human judgment. Identity is no longer established at discrete moments through legal or administrative procedures, but is continuously inferred through systems designed to prevent

fraud. As a result, regulatory data infrastructures privilege anticipation, risk management, and optimization in everyday governance (see also Aradau & Blanke, 2022), reshaping not only formal decision-making but also informal democratic norms such as transparency, reason-giving, and contestability. Taken together, these dynamics point to a longer-term transformation of democratic life, conceptualized here as democratic harms.

Democratic Harms of Regulatory Data Infrastructures

Evaluated against core democratic norms, regulatory data infrastructures generate a set of interrelated democratic harms that cut across both digital ID and facial recognition technologies.

First, *accountability is displaced and diffused* as regulatory functions are delegated to data infrastructures designed, maintained, or operated by private actors, obscuring lines of responsibility. Decisions are increasingly enacted through system architectures, automated routines, and vendor contracts rather than through transparent legal or deliberative processes. As a result, citizens and public officials alike may struggle to identify who is responsible for decisions affecting rights, access, or mobility, weakening mechanisms of democratic oversight and redress. Nissenbaum (1996) already diagnosed this erosion of accountability as a structural consequence of delegating consequential functions to computerized systems, pointing to difficulties in attributing moral responsibility across multiple actors, the normalization of software error, the treatment of computers as moral agents, and the reluctance of industry actors to accept liability.

Second, *participation is reconfigured from a political practice into a managed input*. Data-driven systems tend to privilege forms of engagement that are measurable, extractable, and compatible with computational logics, while sidelining modes of contestation, dissent, and deliberation that resist datafication. Participation thus risks becoming procedural rather than political, reinforcing asymmetries between those who design and operate infrastructures and those governed through them. Debates around India's Aadhaar system, for example, highlight concerns that such systems may depoliticize state–citizen relations by shifting "from inclusive citizenship of political subjects to exclusive citizenship of consumers" (Chaudhuri & König, 2018, p. 128).

Third, *equality is challenged through practices of classification and differential treatment* (Benjamin, 2019). Regulatory data infrastructures produce categories of risk, eligibility, and compliance that often reproduce existing social inequalities while presenting outcomes as neutral or objective (see also Pelizza, 2020). These effects are particularly pronounced in urban contexts, where infrastructures intersect with racialized, classed, and spatialized forms of governance, amplifying unequal exposure to surveillance and control.

Finally, *the rule of law is reworked* rather than eroded. Regulatory power migrates from legal texts and institutions to infrastructural arrangements, where norms such as legality, proportionality, and due process are enacted through code, standards, and system design, often outside established legal safeguards. The intermediation of private vendors further constitutes to the "de facto privatization" of public functions (Braman, 2006, p. 318), raising fundamental questions about transparency, contestability, and democratic legitimacy, the evolution and potential erosion of state sovereignty. Conceiving data-driven systems as institutions helps to clarify how this reworking of the rule of law occurs. As Mendonça et al. (2023) argue, algorithmic systems do not merely implement legal rules but actively structure norms, obligations, and permissions through technical design.

Taken together, these dynamics support the core claim of this article: the introduction of regulatory data infrastructures does not produce a sudden democratic rupture, but instead

incrementally recalibrates how democratic norms are enacted in practice. Because these transformations rarely take the form of explicit institutional reform, they are often difficult to detect. Rather, they unfold through the gradual reconfiguration of informal democratic norms, reshaping how accountability is exercised, how participation is organized, how equality is operationalized, and how the rule of law is enacted in everyday governance. As the preceding analysis has shown, crisis-driven expansions of digital identity and biometric infrastructures rework access, accountability, and rights by embedding rules, classifications, and decision logics into routine administrative practices. Democratic erosion, where it occurs, is thus cumulative and uneven, sedimented in the normalization of infrastructural governance rather than produced by sudden or spectacular institutional change—often justified in the language of technical necessity, administrative efficiency, or crisis response.

7. Conclusions: Infrastructures of Crisis as Infrastructures of Rule

Through a cross-disciplinary analysis, this article has examined the afterlives of crisis-induced digital interventions, understood as sociotechnical infrastructures of urban ordering, to show how measures introduced as temporary and exceptional become normalized and institutionalized over time. Focusing on digital identity and facial recognition as illustrative empirical domains, the analysis demonstrates how crises function as catalysts for durable infrastructural change, enabling the rapid deployment of data-driven systems that would likely have faced greater contestation under ordinary conditions. These developments contribute to a broader shift toward governance by data infrastructure, with uneven and lasting effects across urban populations.

Rather than treating digital ID and facial recognition systems as discrete technologies or policy tools, the article approached them as regulatory data infrastructures that reconfigure relations between the state and its citizens. Even as their immediate crisis-related functions receded, the infrastructures and practices they introduced were not dismantled but instead normalized and repurposed within routine forms of urban governance and spatial regulation. Far from merely optimizing administrative capacity, governance by data infrastructure reshapes how accountability is exercised, how participation is organized, how rights are mediated, and how inequalities are produced and distributed in the city.

What may appear as an infrastructural intervention—often framed in terms of efficiency, modernization, or improved service delivery—thus entails a deeper institutional transformation in which confidence in systems substitutes for political trust in institutions. Authority increasingly migrates from deliberative and legally articulated processes to data-driven forms of regulation embedded in system architectures. In this sense, infrastructures introduced during crises do not merely support governance; they become infrastructures of rule, reorganizing democratic governance through practices of visibility, classification, and automation while operating largely below the threshold of explicit institutional reform. Because these changes unfold incrementally, they often recede into the background of democratic life, quietly recalibrating accountability, participation, and equality.

By foregrounding these dynamics, the article reframes regulatory data infrastructures not merely as objects of regulation but as de facto political institutions in their own right—institutions that encode norms, allocate authority, and structure decision-making. This perspective moves beyond system-level concerns with fairness or bias to advance a systemic critique of how data-driven governance reshapes democracy from within.

Ultimately, safeguarding democracy in the digital age requires attention not only to moments of crisis but to the long-term trajectories and afterlives of crisis-induced infrastructures. This raises

a broader political question that extends beyond the cases examined here: who defines democracy in a data-driven society, and through which infrastructures is that definition enacted?

Acknowledgments

I thank the organizers of the workshop "Crisis-driven Digitalization and its Afterlives in Urban Governance"—Ola Söderström and Petter Törnberg, together with Sophie Oldfield, Jennifer Barella, and Saskia Geyling—held at the University of Neuchâtel on 28 May 2025 and funded by the Swiss National Science Foundation. I also acknowledge the Chair in AI and Democracy at the School of Transnational Governance of the European University Institute, held by Prof. Daniel Innerarity, of which I am a member, for the valuable discussions that informed this work.

Declaration of interest statement

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them. This work is supported by ERC grant DATAGOV, Grant No. 101142006.

References

Agamben, G. (2005). *State of exception*. Chicago University Press.

Allen, D., & Weyl, E. G. (2024). The Real Dangers of Generative AI. *Journal of Democracy*, *35*(1), 147–162. https://doi.org/10.1353/jod.2024.a915355

Amnesty International. (2021, January 26). *Ban dangerous facial recognition technology that amplifies racist policing*. https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

Anderson, B., Grove, K., Rickards, L., & Kearnes, M. (2019). Slow emergencies: Temporality and the racialized biopolitics of emergency governance. *Progress in Human Geography*, *44*(4), 621–639. https://doi.org/10.1177/0309132519849263

Andrejevic, M., & Selwyn, N. (2020, January 23). Facial recognition technology and the end of privacy for good. *Lens*. https://lens.monash.edu/@politics-society/2020/01/23/1379547/facial-recognition-tech-and-the-end-of-privacy

Andrejevic, M., & Selwyn, N. (2022). *Facial Recognition*. Policy Press.

Aradau, C., & Blanke, T. (2017). Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory*, *20*(3), 373–391. https://doi.org/10.1177/1368431016667623

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

Aradau, C., & Van Munster, R. (2011). *Politics of Catastrophe: Genealogies of the Unknown*. Routledge.

Araya, D. (2019, January 4). Artificial Intelligence And The End Of Government. *Forbes*. https://www.forbes.com/sites/danielaraya/2019/01/04/artificial-intelligence-and-the-end-of-government/

Autoriteit Persoongegevens. (2020, October). *Google/Apple Exposure Notification framework* https://www.edps.europa.eu/sites/default/files/publication/panel2-20201021_ap_on_gaen_publicvklos.pdf

Barber, G. (2020, March 11). Schools Adopt Face Recognition in the Name of Fighting Covid. *Wired*. https://www.wired.com/story/schools-adopt-face-recognition-name-fighting-covid/

Beck, U. (1992). *Risk Society: Towards a New Modernity*. Sage.

Beckett, G. (2013). The Politics of Emergency. *Reviews in Anthropology*, *42*, 101–185.

Bellanova, R., & de Goede, M. (2020). The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, *16*(1), 102–118. https://doi.org/10.1111/rego.12338
Benjamin, R. (2019). *Race After Technology*. Polity Press.
Bianchi, F. (2021, April 13). *Europei a Roma, c'è l'ok del Governo: "All'Olimpico con il 25% del pubblico."* https://www.repubblica.it/sport/calcio/nazionale/2021/04/13/news/europei_a_roma_c_e_l_ok_del_governo_figc_gravina_notizia_splendida_-296325592/?ref=search
Bigo, D. (2020, June 3). Covid-19 tracking apps, or: How to deal with a pandemic most unsuccessfully. *About:Intel. European Voices on Surveillance*. https://aboutintel.eu/covid-digital-tracking/
Bijker, W. E. (1997). *Of Bicycles, Bakelites, and Bulbs. Toward a Theory of Sociotechnical Change*. MIT Press.
Bowker, G. C., & Star, S. L. (1999). *Sorting Things Out. Classification and Its Consequences*. MIT Press.
Braman, S. (2006). *Change of state: Information, policy, and power*. MIT Press.
Breckenridge, K. (2014). *Biometric State: The Global Politics of Identification of Surveillance in South Africa, 1850 to the Present*. Cambridge University Press.
Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, *81*, 77–91. ttps://proceedings.mlr.press/v81/buolamwini18a.html
Bygrave, L. (2015). *Internet Governance by Contract*. Oxford University Press.
Carrer, L., Coluccini, R., & Di Salvo, P. (2020, June 9). Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale. *Wired*. https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/
Center for Human Rights & Global Justice. (2022). *Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID*. NYU School of Law.
Chaudhuri, B., & König, L. (2018). The Aadhaar scheme: A cornerstone of a new citizenship regime in India? *Contemporary South Asia*, *26*(2), 127–142. https://doi.org/10.1080/09584935.2017.1369934
Cheesman, M. (2022). Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. *Geopolitics*, *27*(1), 134–159. https://doi.org/10.1080/14650045.2020.1823836
Christakis, T., Bannelier-Christakis, K., Castelluccia, C., & Métayer, D. (2022). *Mapping the Use of Facial Recognition in Public Spaces in Europe*. Université de Grenoble Alpes.
Costanza-Chock, S. (2018). *Design Justice, A.I., and Escape from the Matrix of Domination*. https://jods.mitpress.mit.edu/pub/costanza-chock?version=c5860136-8a6c-424b-b07c-9c8c071615b0
COVID-19 driving an acceleration in adoption of identity verification. (2020, October 14). *The Paypers*. https://thepaypers.com/digital-identity-security-online-fraud/covid-19-driving-an-acceleration-in-adoption-of-identity-verification--1245131
Dahl, R. A. (1998). *On democracy*. Yale University Press.
Dalton, C. M., Taylor, L., & Thatcher, J. (2016). Critical Data Studies: A Dialog on Data and Space. *Big Data & Society*, *January-June*, 1–9. https://doi.org/10.1177/2053951716648346
Damen, F. (2022, December 9). Mensenrechtencollege: Discriminatie door algoritme voor het eerst 'aannemelijk', VU moet tegendeel bewijzen. *De Volkskrant*. https://www.volkskrant.nl/nieuws-achtergrond/mensenrechtencollege-discriminatie-door-algoritme-voor-het-eerst-aannemelijk-vu-moet-tegendeel-bewijzen~b66c072e/
Datta, A. (2018). The digital turn in postcolonial urbanism: Smart citizenship in the making of India's 100 smart cities. *Transactions of the Institute of British Geographers*, *43*(3), 405–419. https://doi.org/10.1111/tran.12225
Davies, H., Hjorth, L., Andrejevic, M., Richardson, I., & DeSouza, R. (2023). QR codes during the pandemic: Seamful quotidian placemaking. *Convergence*, *29*(5), 1121–1135. https://doi.org/10.1177/13548565231160623

Diamond, L., & Morlino, L. (2004). The Quality of Democracy: An Overview. *Journal of Democracy*, *15*(4), 20–31. https://doi.org/10.1353/jod.2004.0060
Dimitrakou, I., & Ren, J. (2025). Critical geographies of everyday crisis. *City*, 1–19. https://doi.org/10.1080/13604813.2024.2447688
Dutch governments caught off guard by American tech firm buying Dutch cloud company. (2025, November 12). *NL Times*. https://nltimes.nl/2025/11/12/dutch-governments-caught-guard-american-tech-firm-buying-dutch-cloud-company
Easterling, K. (2016). *Extrastatecraft. The Power of Infrastructure Space*. Verso.
EU Artificial Intelligence Act. (2025, February 2). *Article 5: Prohibited AI Practices* [Online post].
Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.
eu-LISA. (2021). *Contactless Travel in Post-COVID Times: Enhancing the EU Security Ecosystem.* European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). https://www.eulisa.europa.eu/sites/default/files/documents/IR_2021-06_Report.pdf
European Center for Not-For-Profit Law, International Network of Civil Liberties Organizations, & Privacy International. (2022). *Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 pandemic.* https://privacyinternational.org/sites/default/files/2022-12/ECNL%2C%20INCLO%2C%20PI-COVID-19-Report-Final.pdf
European Commission. (2021, June 3). *Commission proposes a trusted and secure Digital Identity for all Europeans*. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663
European Commission's Directorate-General for Migration and Home Affairs. (2025). *Entry/Exit System (EES). How will the EES work? What is new during the border checks?* https://travel-europe.europa.eu/ees/how-will-ees-work-what-new-during-border-checks?utm_source=chatgpt.com
European Parliament. (2024, August 20). *Regulation on automated data exchange for police cooperation (Prüm II)*. Legislative Train Schedule. https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-prüm-ii?sid=8301
Friedman, J. (2019). *Power without Knowledge: A Critique of Technocracy*. Oxford University Press.
Fussey, P., Davies, B., & Innes, M. (2021). 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. *The British Journal of Criminology*, *61*(2), 325–344. https://doi.org/10.1093/bjc/azaa068
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
Gebru, T. (2020). Race and Gender. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford Handbook of Ethics of AI* (pp. 253–270). Oxford University Press.
Government of Canada. (2023, January 30). *Digital credentials*. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/digital-credentials.html
Graham, S., & Marvin, S. (2001). *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. Routledge.
Gritsenko, D., & Wood, M. (2020). Algorithmic governance: A modes of governance approach. *Regulation & Governance*, *16*(1), 45–62. https://doi.org/10.1111/rego.12367
Halpern, O., & Mitchell, R. (2023). *The Smartness Mandate*. MIT Press.
Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital Citizenship in a Datafied Society*. Polity.
Isin, E., & Ruppert, E. (2020). The birth of sensory power: How a pandemic made it visible? *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720969208

Kayali, L. (2023, May 17). Top French court backs AI-powered surveillance cameras for Paris Olympics. *POLITICO*. https://www.politico.eu/article/french-top-court-backs-olympics-ai-powered-surveillance-cameras/

Kitchin, R. (2020). Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity*, 1–20. https://doi.org/10.1080/13562576.2020.1770587

Kitchin, R. (2025). *Critical Data Studies. AN A to Z Guide to Concepts and Methods*. Polity.

Lawani, A., Horwu-Christensen, A., Chakargi, M. J., Casucci, N., Castel, O., Uniwona, P., Coroneo, G., Campaioli, G., Bard, M., Vanguri, S., & Alum, K. (2026). *Dissecting digital ID(ea)s: Investigating the infrastructures and imaginaries of digital identity* [Digital Methods Initiative]. University of Amsterdam. https://www.digitalmethods.net/Dmi/WinterSchool2026DissectingDigitalIDeas

Levitsky, S., & Ziblatt, D. (2018). *How Democracies Die*. Crown Publishing.

Liu, C. (2021). Seeing Like a State, Enacting Like an Algorithm: (Re)assembling Contact Tracing and Risk Assessment During the COVID-19 Pandemic. *Science, Technology, & Human Values*, *47*(4), 1–28. https://doi.org/10.1177/01622439211021916

Lupton, D. (2015). *Digital sociology*. Routledge.

Lyon, D. (2022). *Pandemic Surveillance*. Polity Press.

Madianou, M. (2019). Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. *Social Media + Society*, *5*(3). https://doi.org/10.1177/2056305119863146

Madianou, M. (2020). A Second-Order Disaster? Digital Technologies During the COVID-19 Pandemic. *Social Media + Society*, *6*(3). https://doi.org/10.1177/2056305120948168

Marres, N. (2017). *Digital Sociology*. Polity Press.

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

McFarlane, C. (2021). *Fragments of the City: Making and Remaking Urban Worlds*. University of California Press.

Mendonça, R. F., Almeida, V., & Filgueiras, F. (Eds.). (2023). *Algorithmic Institutionalism: The Changing Rules of Social and Political Life*. Oxford University Press. https://doi.org/10.1093/oso/9780192870070.003.0002

Milan, S. (2020). Techno-solutionism and the standard human in the making of the COVID-19 pandemic. *Big Data & Society*, *July-December*, 1–7. https://doi.org/10.1177/2053951720966781

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). Talking to Machines: Knowledge Production and Social Relations in the Age of Governance by Data Infrastructure. In J. Jarke, B. Prietl, S. Egbert, Y. Boeva, H. Heuer, & M. Arnold (Eds.), *Algorithmic Regimes: Methods, Interactions, and Politics* (pp. 229–238). Amsterdam University Press.

Milan, S., & Di Salvo, P. (2020, June 8). Four invisible enemies in the first pandemic of a "datafied society." *Open Democracy*. https://www.opendemocracy.net/en/can-europe-make-it/four-invisible-enemies-in-the-first-pandemic-of-a-datafied-society/

Milan, S., Taylor, L., Gürses, S., & Veale, M. (2021). Promises made to be broken: Digital vaccine certification as hyperrealistic immunity theatre. *European Journal of Risk Regulation*, *12*, 382–392. https://doi.org/10.1017/err.2021.26

Milan, S., & Treré, E. (2020). The rise of the data poor: The COVID-19 pandemic seen from the margins. *Social Media + Society*, *July-September*, 1–5. https://doi.org/10.1177/2056305120948233

Milan, S., Treré, E., & Masiero, S. (2021). *COVID-19 from the Margins: Pandemic Invisibilities, Policies and Resistance in the Datafied Society*. Institute of Network Cultures.

Mukogosi, J. (2021, April 20). *Vaccine Passports and Pandemic Racism* [Data & Society: Points]. https://points.datasociety.net/vaccine-passports-and-health-racism-7e494e29bd9b

Musiani, F. (2013). Network architecture as internet governance. *Internet Policy Review*, *2*(4). https://doi.org/10.14763/2013.4.208

Mythen, G., & Walklate, S. (2016). Not knowing, emancipatory catastrophism and metamorphosis. *Security Dialogue*, *47*(5), 403–419.

Nardi, C. (2020, July 3). "Don't waste a good crisis": Experts push governments to create digital ID programs in wake of COVID-19. *National Post*. https://nationalpost.com/news/politics/dont-waste-a-good-crisis-experts-push-governments-to-create-digital-id-programs-as-covid-19-pushes-digital-transformation

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720976680

Nissenbaum, H. (1996). Accountability in a computerized society. *Science and Engineering Ethics*, *2*(1), 25–42.

Pannett, R. (2022, January 13). German police used a tracing app to scout crime witnesses. Some fear that's fuel for covid conspiracists. *The Washington Post*. https://www.washingtonpost.com/world/2022/01/13/german-covid-contact-tracing-app-luca/

Passanti, C. (2025). The division of biometric labor: Relations of production in African voter-identification technologies. In M. Quet, K. Kameda, J. Pourraz, & Y.-M. Rault-Chodankar (Eds.), *Technoscientific globalization from below* (pp. 272–297). Mattering Press.

Pelizza, A. (2020). Processing Alterity, Enacting Europe: Migrant Registration and Identification as Co-construction of Individuals and Polities. *Science, Technology & Human Values*, *45*(2), 262–288. https://doi.org/10.1177/0162243919827927

Pelizza, A., Milan, S., & Lausberg, Y. (2021). Understanding migrants in COVID-19 counting: Rethinking the data-(in)visibility nexus. *Data & Policy*, *3*(E18). https://doi.org/10.1017/dap.2021.19

Pellizzoni, L. (2020). The time of emergency. On the governmental logic of preparedness. *Sociologia Italiana*, *16*, 39–54. https://doi.org/10.1485/2281-2652-202016-3

Pickren, G. (2016). 'The global assemblage of digital flow': Critical data studies and the infrastructures of computing. *Progress in Human Geography*, *42*(2), 225–243. https://doi.org/10.1177/0309132516673241

Rahman, M. F., Lewis, D., Kuhl, L., Baldwin, A., Ruszczyk, H., Nadiruzzaman, Md., & Mahid, Y. (2024). Managed urban retreat: The trouble with crisis narratives. *Urban Geography*, *45*(1), 23–32. https://doi.org/10.1080/02723638.2023.2228094

Rawls, J. (1999). *A Theory of Justice. Revised Edition*. Harvard University Press.

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

Roe, E. M. (1995). Except-Africa: Postscript to a special section on development narratives. *World Development*, *23*(6), 1065–1069. https://doi.org/10.1016/0305-750X(95)00018-8

Roitman, J. (2013). *Anti-Crisis*. Duke University Press.

Royo, D. (2025, January 9). The Seven Sins of European Digital Identity (EUDI). *Dyne.Org*. https://news.dyne.org/the-problems-of-european-digital-identity/

Ruppert, E., Isin, E., & Bigo, D. (2017). Data Politics. *Big Data & Society*, *July-December*, 1–7. https://doi.org/10.1177/2053951717717749

Sample, I. (2019, June 7). Facial recognition tech is arsenic in the water of democracy, says Liberty. *The Guardian*. https://www.theguardian.com/technology/2019/jun/07/facial-recognition-technology-liberty-says-england-wales-police-use-should-be-banned

Sato, M. (2021, January 5). Singapore's police now have access to contact tracing data. *MIT Technology Review*. https://www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid/

Scheppele, K. L. (2004). Law in a Time of Emergency: States of Exception and the Temptations of 9/11. *University of Pennsylvania Journal of Constitutional Law*, *1001*. https://scholarship.law.upenn.edu/jcl/vol6/iss5/4

Schoemaker, E., Baslan, D., Pon, B., & Dell, N. (2020). Identity at the margins: Data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Information Technology for Development*, 1–24. https://doi.org/10.1080/02681102.2020.1785826

Security Industry Association. (2023, March 27). *Facial Recognition for Access Control: Efficient, Convenient and Accurate*. https://www.securityindustry.org/2023/03/27/facial-recognition-for-access-control-efficient-convenient-and-accurate/

Solarova, S., Podroužek, J., Mesarčík, M., Gavornik, A., & Bielikova, M. (2023). Reconsidering the regulation of facial recognition in public spaces. *AI and Ethics*, *3*(2), 625–635. https://doi.org/10.1007/s43681-022-00194-0

Swauger, S. (2021). Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education. In J. Stommel, C. Friend, & S. M. Morris (Eds.), *Critical Digital Pedagogy*. Press Books.

Van Natta, M., Chen, P., Herbek, S., & et al. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. *Journal of Law and the Biosciences*, *7*(1). https://doi.org/10.1093/jlb/lsaa038

Wiig, A. (2015). The empty rhetoric of the smart city: From digital inclusion to economic promotion in Philadelphia. *Urban Geography*, *34*(4), 535–553. https://doi.org/10.1080/02723638.2015.1065686

Wiig, A., & Wyly, E. (2016). Introduction: Thinking through the politics of the smart city. *Urban Geography*, *37*(4), 485–493. https://doi.org/10.1080/02723638.2016.1178479

Yan, Z. (2020). Unprecedented pandemic, unprecedented shift, and unprecedented opportunity. *Human Behavior and Emerging Technologies*, *2*(2), 110–112. https://doi.org/10.1002/hbe2.192

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society*, *20*(1), 118–136. https://doi.org/10.1080/1369118X.2016.1186713