# Postpandemic Technopolitical Democracy: Algorithmic Nations, Data Sovereignty, Digital Rights, and Data Cooperatives

**Igor Calzada**

**Abstract** COVID-19 has hit citizens dramatically during 2020, not only creating a general risk-driven environment encompassing a wide array of economic vulnerabilities but also exposing them to pervasive digital risks, such as biosurveillance, misinformation, and e-democracy algorithmic threats. Over the course of the pandemic, a debate has emerged about the appropriate democratic and technopolitical response when governments use disease surveillance technologies to tackle the spread of COVID-19, pointing out the dichotomy between state-Leviathan cybercontrol and civil liberties. The COVID-19 pandemic has inevitably raised the need to resiliently and technopolitically respond to democratic threats that hyperconnected and highly virialised societies produce. In order to shed light on this debate, amidst this volume on "democratic deepening", this chapter introduces the new term "postpandemic technopolitical democracy" as a way to figure out emerging forms and scales for developing democracy and citizen participation in hyperconnected and highly virialised postpandemic societies. Insofar as the digital layer cannot be detached from the current democratic challenges of the twenty-first century including neoliberalism, scales, civic engagement, and action research-driven coproduction methodologies; this chapter suggests a democratic toolbox encompassing four intertwined factors including (i) the context characterised by the algorithmic nations, (ii) challenges stemming from data sovereignty, (iii) mobilisation seen from the digital rights perspective, and (iv) grassroots innovation embodied through data cooperatives. This chapter elucidates that in the absence of coordinated and interdependent strategies to claim digital rights and data sovereignty by algorithmic

I. Calzada (✉)
Fulbright Scholar-In-Residence (SIR), US-UK Fulbright Commission, California State University, Bakersfield (CSUB), Institute for Basque Studies, Bakersfield, CA, USA

WISERD (Wales Institute of Social and Economic Research and Data), Civil Society ESRC Centre, SPARK (Social Science Research Park), Social Science Department, Cardiff University, Cardiff, Wales, UK

Diaspora Postgraduate Course, University of the Basque Country, Faculty Humanities, Paseo de la Universidad, Vitoria-Gasteiz, Spain
e-mail: calzadai@cardiff.ac.uk



J. Zabalo et al. (eds.), *Made-to-Measure Future(s) for Democracy?*,
Contributions to Political Science, https://doi.org/10.1007/978-3-031-08608-3_6

nations, on the one hand, big tech data-opolies and, on the other hand, the GDPR led by the European Commission might bound (negatively) and expand (positively) respectively, algorithmic nations' capacity to mitigate the negative side effects of the algorithmic disruption in Western democracies.

**Keywords** Technopolitics · Democracy · Postpandemic · COVID · Citizenship · Algorithmic nations · Data sovereignty · Digital rights · Data cooperatives · Social innovation · GDPR · Cooperatives · Vulnerabilities · Brexit · Biosurveillance · Misinformation · Technological sovereignty · Digital sovereignty · Cybercontrol · Civil liberties · Foundational economy

## 1 Introduction: Amidst Postpandemic Technopolitical Democracy

Citizens worldwide have likely been pervasively surveilled during and probably as a result of the COVID-19 crisis by further exacerbating neoliberalism-driven data extractivist global patterns (Aho & Duffield, 2020; Csernatoni, 2020; Hintz et al., 2017; Kitchin, 2020; Zuboff, 2019). Alongside this pervasive global process, despite the fact that vaccination programmes have sped up, its equitable distribution globally cannot be ensured yet (Burki, 2021). As such, the coronavirus does not discriminate and affects citizens translocally, yet it has unevenly distributed economic and social impacts across and within state borders, producing a new pandemic citizenship regime that exposes health, socio-economic, cognitive, and even digital vulnerabilities (Calzada, 2020c).

By contrast, the COVID-19 pandemic has also shown that digital platforms and transformations can offer opportunities to connect with local communities even during times of crisis for subnational and city-regional entities that attempt to ensure data commons (Tommaso, 2020) and data sovereignty (Calzada, 2020b; Hummel et al., 2021). But how can e-democracy be ensured for all citizens while also creating further democratic citizenship (Bridle, 2016; Lucas, 2020) to avert the algorithmic and data-opolitic (data oligopolies; Hand, 2020; Rikap, 2020; Stucke & Grunes, 2017) extractivist hegemonic paradigm as well as Orwellian cybercontrol through massive contract-tracing apps that serve as a digital panopticon of the Leviathan (Datta et al., 2020; Gekker & Hind, 2019; Kostka, 2019; Nichols & LeBlanc, 2020; Taylor, 2020)? How can citizens from stateless city-regional nations react to these unprecedented challenges and equip themselves with the best tools (Calzada, 2018b; Delacroix & Lawrence, 2019) to claim digital rights and data sovereignty (Calzada, 2019a)? What does sovereignty mean for stateless citizens (Calzada, 2018a, b; Zabalo et al., 2016; Zabalo & Iraola, 2020) amidst the pandemic crisis wrapped in an algorithmic global disruption (Dixson-Declève, 2020)?

The COVID-19 pandemic has stressed the growing democratic impact of digital technologies in political and social life (Cheney-Lippold, 2011; Datta, 2020). Contact-tracing applications—and more recently though vaccine passports and biometric technologies—on mobile phones have raised a vibrant debate and epitomised the magnitude of contemporary trends to incorporate algorithmic computation into the government of citizenry. Thus, this crisis has accelerated the need to increase human and social understanding of potential and risk of "*techno-politics*"—the entrenchment of digital technologies in political and governmental practices (Calzada, 2020d, 2021)—for "pandemic citizens" in the stateless algorithmic nations of Europe.

Over the last two decades, the euphoria of the "digital renaissance" and the advent of the Internet as a free network of networks have characterised the dawn of the new millennium. Recent years have witnessed widening concerns about the "surveillance" effects of the digital revolution (Allam, 2020; Andersen, 2020; Christensen, 2019; Christl, 2017; Christl & Spiekermann, 2016; Levy & Barocas, 2018; Lightfoot & Wisniewski, 2014; Lupton & Michael, 2017; Maxmen, 2019; Morozov, 2020; van Dijck, 2014). Expressions like "algocracy", "digital panopticon", and "algorithmic surveillance" have revealed a spreading scepticism about the rise of new governance models based on big data analysis and artificial intelligence (AI; Berditchevskaia & Baeck, 2020; Delipetrev et al., 2020; Dyer-Witheford et al., 2019; Lutz, 2019). The Cambridge Analytica scandal in the United Kingdom, on the one hand, and the Chinese Social Credit System (SCS) tracking, controlling, and scoring citizens, on the other hand, have offered dystopian representations of our digital present (Pilkington, 2019). They have exposed the urge to systematically address the question of whether and to what extent ubiquitous "*dataveillance*" is compatible with citizens' digital rights and democracy (Lupton & Michael, 2017; Smuha, 2020; van Dijck, 2014; Wong, 2020).

Against this backdrop, the EU's General Data Protection Regulation (GDPR) can be understood as a first attempt to pave the way for a specific European model of ruling on these matters and to take the lead globally in favour of an explicit strategy towards digital rights (Calzada & Almirall, 2020; Cities Coalition for Digital Rights, 2019). A rights-based approach to techno-politics can be articulated by connecting the digital transformation that is reshaping our urban spaces to the notion and institution of citizenship, which has been the main carrier of rights in European societies over the last two centuries (Arendt, 1949). This raises the question of how the algorithmic disruption can redefine citizenship through the incorporation of new digital rights related to the status of a citizen in cyberspace—access, openness, net neutrality, digital privacy, data encryption, protection and control, data sovereignty, and so on (Calzada & Almirall, 2020).

Hence, this chapter suggests a democratic toolbox encompassing four intertwined factors including (i) the postpandemic context characterised by the algorithmic nations, (ii) postpandemic challenges stemming from data sovereignty, (iii) postpandemic mobilisation seen from the digital rights perspective, and (iv) postpandemic grassroots innovation embodied through data cooperatives. This chapter elucidates that in the absence of coordinated and interdependent strategies to claim

digital rights and data sovereignty by algorithmic nations, on the one hand, big tech *data-opolies* and, on the other hand, the *GDPR* led by the European Commission might bound (negatively) and expand (positively) respectively, algorithmic nations' capacity to mitigate the negative side effects of the algorithmic disruption in Western democracies. In doing so, this chapter aims to provide a substantial contribution in this direction by articulating an in-depth investigation into how algorithmic disruption can bring about a new generation of human rights belonging to the digital sphere and how they can be unfolded to address the democratic challenges raised by the spread of claims towards data sovereignty in stateless "algorithmic nations" (Calzada, 2018a).

## 2 Towards a Postpandemic Technopolitical Democracy: A Democratic Toolbox

Nominally, over the last few decades, globalisation has led to a new class of global citizenship (Calzada, 2020e; Nguyen, 2017). While the access to this global citizenship remains uneven, many have enjoyed unlimited freedom to move, work, and travel. However, COVID-19 has drastically slowed down this global citizenship regime and introduced a new level of ubiquitous vulnerability in global affairs by inciting a new "pandemic citizenship" regime in which citizens—regardless of their locations—share fear, uncertainty, and risks (Taylor, 2020). Furthermore, COVID-19 is deeply and pervasively related to data and AI governance issues, which expose citizens' vulnerabilities in a potential surveillance state and market (Hintz et al., 2017; Morozov, 2020). Under these extreme circumstances, "pandemic citizenship" thus could be described as follows: The postpandemic era has both dramatically slowed down several mundane routines for citizens, such as mobility patterns, and exponentially increased professional pressures, emotional fears, life uncertainties, algorithmic exposure, data-privacy concerns, direct health-related risks, and socio-economic vulnerabilities. These factors depend eminently on the material and living conditions shared by a wide range of citizens regardless of their specific geolocalisation. Pandemic citizenship (Calzada, 2020f), along with the way it should evolve towards a postpandemic technopolitical democracy, inevitably intersects with the content of this volume regarding (i) austerity policies implemented by global neoliberalism, (ii) urban and city-regional scales (Calzada, 2017c), and essentially (iii) demands resilient responses from the bottom-up embodied by grassroots innovation processes.

Actually, the democratic responses to this pandemic emergency have varied extremely from location to location, even within the same nation-state in Europe. It is true that the pandemic has caused many nation-states to lock down, which then boosted online work and the delivery of goods via online platforms, putting further pressure on citizens. But it also allowed many communities and particularly civic groups and activists in stateless city-regional nations in Europe to respond resiliently, pushing forward cooperatives and reinforcing social capital (Calzada, 2020c; Scholz & Calzada, 2021). Among the resilient strategies adopted by governments in

Europe, collective intelligence stemming from a proactive citizen-level response has been highly considered to greatly avoid further dystopian measures that could exacerbate existing social inequalities and technopolitical vulnerabilities among pandemic citizens (Bigo et al., 2019). A particular collective intelligence response emerging in Europe has been the creation of digital cooperatives (Borkin, 2019; Cherry, 2016; McCann & Yazici, 2018), also known as *platform cooperatives* (Scholz, 2016) and data cooperatives (Pentland et al., 2019). However, this is not the only resilient strategy adopted within data-governance models by subnational entities or particularly by stateless nations to devolve data powers for technological sovereignty.

There is a growing consensus in Europe that it is urgent for governments to start filling the same role in the information society that they have traditionally taken in the post-industrial society (Chiusi et al., 2020), not only fixing market failure caused by austerity neoliberal policies but also regulating digital power relations and supervising actual economic interplay among stakeholders (Calzada, 2020a). This does not just mean demanding fair tax payments by the big tech companies and imposing fines when they violate the GDPR or when they abuse their market power (European Commission, 2020). More fundamental issues are at stake that call for government attention beyond public intervention; this chapter refers to it as fostering social innovation among stakeholders in civil societies (Moulaert & MacCallum, 2019) in stateless algorithmic nations (Calzada, 2018b). The COVID-19 crisis has clearly shown that citizens in stateless algorithmic nations are not only highly dependent on data and the economic value it creates but also directly influenced by the technopolitical biosurveillance it generates through the massive control of data by global extractivist and neoliberal platforms (Calzada, 2020g, h, i). The COVID-19 crisis has thus led to an explicit, necessary revaluation in society of the roles of both state governments and their citizens in extending economic and socially innovative alternatives to digitisation and datafication by devolving data powers to subnational and city-regional levels to ensure civil digital rights and overcome state-centric cybercontrol (Calzada, 2017a, b; Loukissas, 2019). In doing so, this chapter introduces and contextualises the democratic toolkit consisting of (i) the context seen from the lenses of algorithmic nations (Calzada, 2018a), (ii) challenges stemming from data sovereignty, (iii) the necessary mobilisation characterised by digital rights, and (iv), ultimately, grassroots innovation processes embodied through data cooperatives.

## *2.1 Postpandemic Context: Algorithmic Nations*

In the global political arena driven by the extractive algorithmic kind of governance, big data companies such as Google and Facebook have already assumed many functions previously associated with the nation-state, from cartography to the surveillance of citizens, which deterritorialised pandemic citizenship.

Against this present backdrop, historians contend that the tension between civil liberty and collective health has existed since the early days of disease surveillance,

while how such a controversy comes to an end has been historically contingent. As new technologies that collect and archive personal data from citizens have become available in modern societies, the deployment of information and communication technologies (ICT) in public health has reshaped not only the techniques but also the rationalities upon which disease surveillance is built. Such a shift coincides with the convergence of the fields of public health and security in the post-9/11 era, in which health risks such as infectious pathogens are considered national security threats. Consistent with the security trend, disease surveillance efforts have concentrated on border vigilance to identify and prevent risky entrants that are suspected of carrying deadly viruses.

A traditional public health approach has been pursued to combat COVID-19, involving phases of containment (taking steps to prevent the virus from spreading), delay (implementing measures to reduce the peak of impact), mitigation (providing the health system with necessary support), and research (seeking additional effective measures and care). According to Kitchin (2020), in the early response to COVID-19, there was no sufficient consideration of the consequences on civil liberties, biopolitics, or surveillance capitalism, whether the supposed benefits outweighed any commensurate negative side effects, or whether public health ambitions could be realised while protecting civil liberties. The contact-tracing apps have shown profound implications for privacy, governmentality, control creep, and citizenship, and they reinforce the logic of global neoliberalism through surveillance capitalism.

The COVID-19 pandemic caused something akin to a real social experiment (Prainsack, 2020). It has exposed citizens to unforeseen and unprecedented conditions, forcing them to react in ways unimaginable a few months ago. In relation to AI, data, and the digital infrastructure, which have to be considered together as a sociotechnical package, the pandemic is acting as a boost to AI adoption and digital transition, creating new questions and amplifying doubts over data governance, security, rights, cybercontrol, liberties, and increasing social inequalities. These democratic concerns have produced a debate about not only the bounce-back to pre-COVID-19 normality but also the bounce-forward to a more resilient and fair citizenship through foundational economic principles (Foundational Economy Collective, 2020).

According to a review of literature in surveillance studies and the sociology of public health, contemporary surveillance technologies used for biosecurity purposes largely share three characteristics. First is the logic of preemption: While traditional methods of infectious disease management have mainly rested on the reactive logic of identification and response, health surveillance today operates predictively by modelling possible futures with past and real-time data taken directly from citizens' devices. Second, contemporary public health surveillance technologies invite diverse actors and partnerships in the act of surveilling, along with the widespread institutionalisation of "dataveillance", which operates via decentralised and ubiquitous tracking of digitised information and algorithmic analysis. Third, related to this point, disease surveillance today heavily involves self-tracking practices. The plethora of wearable devices, self-tracking mobile applications, and

digital tools have shifted the relationship between self and body and between those who surveil and those being surveilled. Critical works on self-tracking often pay attention to both its biopolitical and self-care capabilities, which render citizens into pixelated, abstract bodies that can be disciplined as neoliberal subjects, but at the same time provide users a sense of control over their bodies via a playful mode of self-surveillance. Such a perspective relates to this chapter's interest in pandemic citizens' digital rights concerning data sovereignty (Hobbs, 2020). Data sovereignty through well-informed, transparent public action and active social engagement emerges therefore as a crucial issue related to the digital rights of citizens.

As an amplifier of pre-existing concerns about digital rights, the COVID-19 crisis has underlined the absolutely critical role of the governance of digital data in modern societies. Without well-structured and semantically rich data, it is not possible to harness the opportunities afforded by AI, digital transformations, and frontier technologies as such. How data is collected, by whom, for what purpose and how it is accessed, shared, and reused have become central questions during the COVID-19 crisis in relation to citizens' digital rights.

Another critical aspect of data sovereignty relates to cybersecurity. The crisis has shown how threats to stakeholders are taking advantage of the situation, which initially led to a significant increase in observed cyberattacks on both crisis-relevant infrastructure and citizens, clearly affecting the European cybersecurity landscape.

A further element of sovereignty exposed by the lockdown is the dependency on non-European collaborative platforms (Muldoon & Stronge, 2020). These platforms have become a critical layer of the digital infrastructure connecting users, processes, applications, and content. Through their use, citizens provide valuable intelligence to the platform operators for profiling, targeting, and potential manipulation (Mazzucato et al., 2020). Digital and data sovereignty need to include this technological layer as well (Floridi, 2020). A dimension amplified by COVID-19 is the extent to which the AI and the digital transformation exacerbate existing social, economic, political, and geographical inequalities, even within the same nation-state, affecting in particular the most vulnerable segments of society but without providing the appropriate digital tools to empower the elderly, youth, and people from social or economically disadvantaged groups in stateless city-regional algorithmic nations.

Hence, "*algorithmic nations*" in the postpandemic context is presented as a conceptual assemblage, blending technopolitical and city-regional imaginaries, scales, infrastructures, and agencies. An assemblage is not just a mixture of heterogeneous elements (Calzada, 2018a). Assemblage emphasises the different processes that historically produce nation-state rescaling and the possibilities for those conditions for devolution to be reimagined and reimplemented.

Very little has been explored with regard to the mediation of what the algorithmic disruption may mean for city-regional politics and its internal nation-building processes in terms of nation-states being assembled and reassembled by different actors who jostle one another to gain advantage (Zabalo & Iraola, 2020). "Global civil society" assemblages between the binary national and global while overlooking the emergent city-regional technopolitical manifestations by stateless and liquid

citizens supplied with decentralised access, interconnectivity, and simultaneity of transactions demanding direct representation in international fora, even bypassing national-state authority. This is a longstanding cause that has been significantly enabled by global electronic decentralised networking and increasingly filtered through blockchain ledgers. The concept of "algorithmic nations" points to the emergence of a particular type of territoriality in the context of imbrications of digital and non-digital conditions, the fusing of the "algorithmic" with the "national" (seen from a metropolitan rather than an ethnic standpoint; Calzada, 2018b).

This chapter suggests this new factor to refer to the way stateless nations need to approach the postpandemic digital revolution by deepening the technopolitical and democratic perspective: *Algorithmic Nations.* "Algorithmic nations" (Calzada, 2018a, p. 268) refers to "a novel notion, which goes beyond internal discord around plurinationality and quasi-federalism" defined as "(i) a non-deterministic city-regional and technopolitical conceptual assemblage (ii) for a transitional strategic pathway (iii) towards the nation-state rescaling (iv) through three drivers—metropolitanisation, devolution, and the right to decide" (p. 270). This volume revolves in other chapters around democratisation, urbanisation/metropolitanisation, the right to decide, inclusiveness, and resilient collective action networks, among others. This chapter essentially provides a democratic toolkit to incorporate by enhancing a technopolitical perspective that is required in the postpandemic hyperconnected societies.

## *2.2 Postpandemic Challenges: Data Sovereignty*

Against the postpandemic backdrop, data sovereignty has transcended global geopolitics and economic to acquire a digital dimension. This is due to the rise of the technology giants whose influence is now impossible to deny, which inevitably rises several democratic concerns. The demise of democracy is clearly already one of the biggest policy challenges of our times, and the undermining of citizens' digital rights is part of this issue. These include a wide of complex technopolitical issues related to data sovereignty.

When did we lose control over our data and how could we get it back? In the age of digitisation, coping responsibly with data poses a substantial dilemma: on the one hand, there is individually tangible and easily comprehensible added value of personal data processing by public and private-sector institutions. On the other hand, there is more or less abstract idea that individuals, specific groups, or communities should retain control over the handling of their data.

This dilemma shows the need for a debate on data sovereignty in full consideration at the subnational level—namely, stateless algorithmic nations. How are data sovereignty related to claims for further data devolution of stateless algorithmic nations (Calzada, 2021)?

COVID-19 responses have shown the importance of the motto *small is beautiful* (Calzada, 2020i; Thorhallsson, 2006, 2016). Highly decentralised city-regions have

demonstrated the ability to cope better with resilient pandemic responses in established small-state cases, such as New Zealand, Iceland, Ireland, Denmark, Netherlands, Singapore, South Korea, and Slovenia. However, there is an open question regarding how these small entities integrate claims in favour of their citizens' digital rights. More urgently, non-established stateless algorithmic nations may have already started from their main urban drivers to claim these digital rights in order to establish a strategy for their data sovereignty. This is the case in Glasgow and Barcelona, respectively, in Scotland and Catalonia. Having said that, intermediary cities or city-regions lack full sovereignty about digital readiness, infrastructure, and services (cellular and broadband connectivity), which significantly limit their access to financial and non-financial services and more broadly to legislate on matters that directly affect their fellow citizens. The lack of data sovereignty may impact young people in intermediary cities, denying them financing, employment, entrepreneurship, education, and training opportunities offered on digital platforms and locking out many young people and key stakeholders from participating directly in the digital economy and governance.

Against this backdrop, in the data-driven European economy, AI, big data, machine learning, and blockchain technologies are reshaping the notion of citizenship by, on the one hand, pervasively challenging the rescaling of nation-states' fixed dynamics and, on the other hand, demanding a counter-reaction from stateless algorithmic nations to bring the control of data to citizens. Claims to data sovereignty through data commons policy programmes are increasingly emerging in several locations. In the post-GDPR scenario, citizens' data privacy, security, and ownership ultimately need to be protected by localising personal data via grassroots innovation and cooperative platforms as has been the case of Barcelona and Catalonia overall (Calzada, 2018c). How citizenship in small algorithmic stateless nations will be influenced and shaped by the geopolitical dynamics between established big nation-states and big firms is still unfolding. Consequently, how could citizens' liquid data and digital rights be protected through further empowerment to avoid digital dissent and dystopia? How will stateless nations face the uneven interaction between AI devices and citizens without having the appropriate sovereign digital tools to protect their fellow citizens? Full democracy in stateless nations can only survive as long as citizens are able to make better choices than machines owned by big techs that actually are becoming more powerful than even established nation-states. Newly emerged global geopolitics, known as AI nationalism, should inevitably have full consideration in this debate as a way to shape the lives of citizens in stateless algorithmic nations. In this direction, new versions of the e-state in Estonia may already offered interesting ways to deal with these uncertainties, taking the lead from the public sector. However, the civilian push is a component that should not be omitted, as the grassroots innovation element actually legitimates a technopolitical claims around digital rights. Another aspect is the impact of the disruptive algorithmic technology called *blockchain* on state-governance schemes. Is it possible to foresee stateless algorithmic nations claiming their technological sovereignty through decentralised governance schemes such as *blockchain*? Amidst the deep influence of *dataism*, stateless

algorithmic nations should establish an alternative technopolitical discourse on citizens' digital and data rights.

## *2.3 Postpandemic Mobilisation: Digital Rights*

In the backdrop of these subtle reactions in stateless nations, a wide range of stakeholders in cities and regions are debating the digital rights of citizens through accountable data ethics. This chapter distinguishes 15 digital rights as follows: (i) the right to be forgotten on the Internet, (ii) the right to be unplugged, (iii) the right to one's own digital legacy, (iv) the right to protect one's personal integrity from technology, (v) the right to freedom of speech on the Internet, (vi) the right to one's own digital identity, (vii) the right to the transparent and responsible usage of algorithms (Janssen et al., 2020), (viii) the right to have a last human oversight in expert-based decision-making processes, (ix) the right to have equal opportunity in the digital economy, (x) consumer rights in e-commerce, (xi) the right to hold intellectual property on the Internet, (xii) the right to universal access to the Internet, (xiii) the right to digital literacy, (xiv) the right to impartiality on the Internet, and (xv) the right to a secure Internet.

In order to provide evidence of such examples of digital rights in cities and regions in the times of COVID-19, the Coalition of Cities for Digital Rights (CCDR), encompassing more than 50 global cities (www.citiesfordigitalrights.org), is worth mentioning as the key advocacy group at the global level pushing an ambitious and highly relevant policy agenda on digital rights (Calzada & Almirall, 2020; Cities Coalition for Digital Rights, 2019). Barcelona and Glasgow are part of this Coalition of Cities for Digital Rights.

In the following summary, this chapter has gathered ongoing policy actions about digital rights taking place in these two stateless algorithmic nations by analysing their core and flagship cities. This analysis has been conducted through a direct survey of city representatives carried out in November 2020 among different CCDR (Cities Coalition for Digital Rights) global cities, such as Barcelona and Glasgow:[1]

(i) Barcelona in Catalonia: Barcelona has been focusing on digital inclusion as the main priority to implement digital rights. In addition to this, open technologies and accountable decision-making in AI are presented as second and third priorities. The city of Barcelona is putting value on projects that are already occurring in civil society and at universities. A specific contextual aspect that has leveraged the relevance of digital rights in Barcelona has been the strong civil society alongside the fact that the Mobile World Congress has allowed Barcelona to lead the paradigm of "technological humanism". In this direction, universal

[1] The author of this article acknowledges the collaboration implemented with the Core Team of the CCDR.

and equal access to the Internet and digital literacy are seen as the main priority alongside transparency; accountability; non-discrimination of data, content, and algorithms; and participatory democracy, diversity, and inclusion. In Barcelona, the most critical stakeholder group to achieve more protection for digital rights is the private companies, especially those providing public services. However, according to the city representatives, without the engagement of civil society, it is rather difficult to achieve an inclusive data-governance model. Moreover, according to them, certain entrepreneurs, activists, and innovators are pushing ahead Barcelona's ecosystem of data. In addition, they acknowledge that COVID-19 and its effects have already modified their initial priorities on digital rights by altering their strategic plan towards digital inclusion. For Barcelona, a good data commons strategy could be defined as one based on transparency, accountability, pedagogy, and the data sovereignty of citizens. In Barcelona, there are initiatives related to platform and data cooperatives sharing health data to tackle COVID-19. Finally, citizens have so far reacted positively to the City Hall's adoption of AI that particularly focuses on social services, transport, and mobility. The way in which the claim for digital rights could be scaled up towards further data sovereignty at the regional level remains to be seen.

(ii) Glasgow in Scotland: Glasgow has been focusing on digital inclusion and essential digital skills. However, Glasgow is not actively working on raising citizens' awareness of the need to protect their digital rights yet. As such, Glasgow has been focusing on establishing their own actions for digital rights and engaging with elected officials to raise their awareness. Having said that, Glasgow is keen to learn from the CCDR to raise awareness with citizens. Given that tackling social inequalities is the most pressing need for the city of Glasgow, local authorities have been actively implementing measures to achieve universal and equal access to the Internet and digital literacy. According to the city representative, the most critical stakeholder in the city to achieve more protection for digital rights is the leader of the council (equivalent of mayor), who positioned digital rights as a human right. Consequently, the public sector is leading the data-governance model of the city. Regarding COVID-19 and its effects on the priority of digital rights, city representatives acknowledge that they have witnessed much greater data sharing within the city and with national public bodies, which in itself may reinforce the idea that sooner than later data sovereignty will be claimed at the national level in Scotland. For the city of Glasgow, a good data commons strategy could be defined as one that provides value to all stakeholders in the city. Yet, citizen-driven data initiatives and projects lack consistency and leadership. In Glasgow, platform and data cooperatives could assist the city in tackling COVID-19-driven economic and social vulnerabilities among pandemic citizens. Regarding existing data cooperative initiatives in the city, interestingly, there are more general data-sharing agreements being established between public bodies that could provide the basis for data cooperatives. In response to the main challenges and obstacles for the public sector to implement AI, the Glasgow city

representative considers public trust as the main hindrance. However, positively, AI adoption is consequently being coordinated by the Scottish Government through their AI strategy, where Glasgow has an active role and a say in the data sovereignty-driven strategy on AI, which essentially shows what this article is attempting to depict: an interdependent joint effort between Glasgow's claim on digital rights and a strategy on data sovereignty by the stateless algorithmic nation of Scotland. Regarding how citizens would react to the adoption of AI for implementations in the public sector, the Glasgow city representative acknowledged that we do not know yet how citizens do or will respond to this adoption. In response to areas in which AI could contribute to delivering efficient and inclusive public services, Glasgow seems to focus on supporting their sustainability agenda.

In a broader context, as these cities and regions around the world try to cope effectively with the COVID-19 crisis, we are witnessing a wide variety of digital technology responses. Mobile phones, social media, and AI can play a substantial role in dealing with the spread of COVID-19. This includes the development of contact-tracing apps and the use of big data to analyse people's movements. For example, mobility data from Deutsche Telecom is being used to estimate the degree to which the German population is complying with requests to stay at home. In Singapore, the TraceTogether app uses Bluetooth to enable the health ministry to identify people who have been in close contact with infected individuals. Many of these kinds of solutions can be positive and help policymakers respond quickly and appropriately. They make it possible to monitor, anticipate the spread of the disease, and support mitigation. While the use of these applications might be effective in the short term, there may be a fine line between hurried implementation of new technologies in times of crisis and negative long-term impact on digital rights (Goggin et al., 2019). How do we adequately balance the values of privacy and autonomy with values of safety and security for citizens? A special focus on pragmatic examples with a privacy-first and inclusive tech approach could be utilised as follows, considering social innovation over technological innovation (Calzada, 2020a).

Privacy is one of our human rights, inalienable and non-negotiable in a democracy, and any decisions citizens make now will resonate for far longer than the COVID-19 virus will (Wong, 2020). Though the situation citizens are in provides a unique context, laws are not as context-specific as we would like in this situation. This presents us with the risk that regulations we pass now may later on be used for purposes more nefarious than battling a global pandemic. It is therefore especially prudent to create an open space where the debate about how to combine personal privacy and public health can exist. The right to a private life must be upheld. This means that any use of personal health data, geolocation data, or other personal forms of data must be limited, supervised, and temporary. Under these conditions, emergency measures can be created. How do cities and regions ensure a democratic, social, and humane use of technology in their communities? And more specifically, how can cities and regions use technology as an enabler to face the current

COVID-19 pandemic with citizens' digital rights at the centre of their design and application?

## *2.4 Postpandemic Grassroots Innovation: Data Cooperatives*

We have heard many times that data was the oil of the twenty-first century. But what nobody told us so far was the data sharing should be based on trust, social capital that emerged in communities from peer-to-peer interactions. This contrasts with the widespread neoliberal assumption that data should inevitably be monetised as one-size-fits-all solution. This factor related to postpandemic grassroots innovation humbly suggests another alternative pathway in light of several emerging and further promising practical cases to revert surveillance capitalism.

Big data—extremely large data sets that may be analysed computationally—originated with the increasingly advanced data collection capabilities of the Internet, social networks, the Internet of Things (IoT), artificial intelligence (AI), and sensors. But this AI-driven algorithmic phenomenon has led to new consequences—such as hyper-targeting through data analytics, facial recognition, and individual profiling—received by many with both helplessness and threat, and resulting in a not-so-desirable outcomes, such as massive manipulation and control via surveillance capitalism push in the USA and the Social Credit Systems in China. In contrast, these societal concerns raised a debate in Europe that crystalised into the General Data Protection Regulation (GDPR) coming into force since May 2018, becoming thereafter a fully fledged inspiration for several data regulations worldwide, including the California Consumer Privacy Act (CCPA). Yet, it seems the discussion around data governance has spurred fruitful debates, we must confess more nuanced and more humble cases grounded in practice are required to pave the way ahead. At present, most alternative initiatives stemming from platform cooperatives are based on services provided by Amazon Web Services (AWS), which shows in itself the insurmountable hindrances related to how hard.

Moreover, we are now witnessing the side effects of an uneven global vaccination and its aftermath. First, the paradox of vaccine passports supposedly being a tool meant to unite the world after lockdown could now instead end up balkanizing it into closed systems where only certain apps are accepted, only certain vaccine brands are welcome, and only some documentation is accessible to cross any border and get into a country. Second, the global race for doses has also affected which countries get which vaccines resulting in an extreme protectionism also known as vaccine nationalism. And third, it goes without saying that despite the fact that biometric technologies from facial recognition to digital fingerprinting have proliferated through society in recent years, the benefits they offer are clearly counterbalanced by numerous democratic, ethical, and societal concerns.

The amount of data and resulting power held by a small number of players, the so-called GAFAM (Google, Amazon, Facebook, Apple, and Microsoft), has already created a counterreaction in the European continent. The European Strategy for

Data and the Data Governance Act attempt to provide an alternative driven by the so-called data sovereignty (whatever it might mean not only in Europe but also elsewhere worldwide). Recent years have seen an emergence of this notion to claim data ownership in debates on the development, implementation, and adjustment of new data-driven technologies and their infrastructures. Despite its unclear territorial and technopolitical jurisdiction, data sovereignty is exemplified through national data sovereignty in cloud computing, indigenous data sovereignty, and (more intensively now) patient data sovereignty claims. At the end of the day, the concentration of power around data has been counterreacted from claims stemming from national and political interests, indigenous population' digital rights, and users-consumers-workers-citizens' digital rights.

In the European continent, data sovereignty has adopted a legal form of data altruism and donation, which means that individuals can chose the way their data can be stored. Although it remains to be seen how this data sovereignty enables citizen organisations to help us move from the current paradigm of individuals giving up data to large big tech to a system based on collective data rights and accountability, with legal standards and fiduciary representation. As such, we could argue that these cooperative forms known as data cooperatives are a subcategory of the widespread phenomenon called platform cooperatives (Calzada, 2020c).

As such, arguably, the current pandemic and democracy are pervasively related to data governance issues, exposing citizens' vulnerability in a potential surveillance state. But, how can job quality (or worker power) be ensured for all platform workers while also creating further democratic socio-economic platformised alternatives to revert algorithmic and data-opolitics (data oligopolies) extractivist business-as-usual hegemonic paradigm? At this stage, consequently, we may also ask whether it is possible to altern existing data governance extractivist models to incentivize the emergence of platform cooperatives and data cooperatives to protect pandemic citizens' labour and digital rights (Calzada, 2020c).

Data cooperatives are member-owned data management storages (e.g. credit unions) with fiduciary obligations to member, where all data usage is for the benefit of members and done only with their consent; it is driven by privacy preservation. Data cooperatives focus on data interactions among citizens and not essentially in the core social value behind them. There are several examples such as Salus, Driver's Seat, and MyData so far implemented (Scholz & Calzada, 2021).

According to Pentland and Hardjono, with 100 million people members of credit unions, the opportunity for community organisations to leverage community-owned data is massive. Nonetheless, data ownership or data sovereignty has been used so far for advocacy, and it seems now more a claim than something that can be achieved in practice very easily. Data flows in fact are complicated and not easy to be tracked as we are witnessing in the aftermath of COVID-19. Furthermore, the legal rights associated with data flows depict a complex set of boundaries when it comes to the ownership of data. While there exists a remarkable degree of harmonisation and coherence around the data protection core principles in key international and regional agreements and guidelines, there are diverging implementation practices around data flows. Besides this, Pentland and Hardjono advocate how financialising

personal data, data cooperatives might emerge at the community level. Actually, this is rather unlikely without any means for controlling data flows and ensuring data sovereignty for members of specific local communities.

Hence, data cooperatives being a voluntary collaborative pooling by individuals of the personal data for the benefit of the membership of the group or community present several shortcomings as well. Some advocates may only see the data pooling process as a purely technical process, whereas it is clearly a socio-communitarian process based on trust and related to social capital. As Loukissas argued, all data ultimately are local; thus, it cannot take from granted the territorial and local dimension of this discussion. It is key that the ability to balance the world's data economy inevitably depends on the fair interplay among stakeholders. Consequently, it is very clear that citizens and workers by themselves have no direct representation, yet consumers who were able to control their data would be a force to be acknowledged as long as their data would be localised/territorialised in certain data ecosystems.

Communities using their own data requires decentralised and federated data ecosystems arranged by sectors (health-related data, environmental data, transport and mobility data, energy and consumption data, etc.) being clearly located in certain places and allowing to interoperate among each other, unless members of the community decide not to do it. This would mean owning data and being sovereign about their own data the produce. We are suggesting that data should be co-operativised among members (citizens or workers) of communities. For co-operativising data, we consider that localising data require at the same time translocal federated data ecosystems (via blockchain) to scale up the potential of the cooperative action and outreach (Calzada & Almirall, 2020). Citizens in communities will be thus using their own data gathered in local repositories own by them while contributing to the data sharing if they would allow doing it (Calzada, 2021). Actually, this is the case of Eva.coop, a Montreal-based data cooperative: They provide an infrastructure for groups but without accessing local data about passengers. Some data are shared, however. Eva.coop is built on the EOSIO blockchain protocol as a way to show how the cooperative model could mark a new blockchain-based iteration of the sharing economy driven by decentralised system that respects privacy and fits into local needs. Local data matters and Eva might have shed light on the way to follow. Local communities have more input, drivers are treated more fairly, and riding members maintain their privacy and are comforted by a locally supported app. Could this third generation of blockchain be a protocol from which to scale up a federated cooperative commonwealth based on structured data ecosystems by economic sectors (transport, healthcare, education, etc.)?

Probably, there are few policy aspects worth considering for scaling up data cooperatives: (i) First, there is a clear need to reactive civil societies for experimentation paying special attention to city-regional unique features as clear sources of community-driven sovereign data to foster the creation of locally-based data cooperatives. (ii) Second, it is probably very necessary still to provide enhanced training about the scope and functioning of cooperatives to enable the fertilisation of data cooperatives. (iii) Third, procurement and public incentives are required to push ahead, enhance, and reinforce platform and data cooperatives beyond marginal

experiments aligned with data donation and altruism. (iv) And finally, initiatives around data cooperatives need to find their own strategic pathways amidst the digital and social economy policy agenda in each regional context worldwide.

## 3 Conclusion

COVID-19 has been a trigger for increasing the impact of digital transformations on the daily lives of citizens and democracy. However, little is known or has been explored in relation to the direct effects of *big tech* surveillance capitalism and the cybercontrol push by nation-state governments during this crisis on citizens from stateless algorithmic nations. Paralleling this context, since the implementation of the GDPR in May 2018, the European Commission has been intensively promoting the idea of technological sovereignty without further specifics, but the emerging project in this field is Gaia-X (GaiaX, 2020), which in itself has been promoted by France and Germany, surfacing new democratic concerns about the role of citizens in this timely debate. The aim of Gaia-X is apparently to direct European companies towards domestic cloud providers. Paradoxically, China's Cybersecurity Law mandates that certain data be stored on local servers or undergo a security assessment before it is exported. China's data rules can be enforced anywhere in the world if the data at issue describes and affects Chinese citizens. This law will also create a blacklist prohibiting foreign entities from receiving personal data from China. It goes without saying that in this geopolitical competition, the USA is beginning to advance its own version of technological sovereignty by prohibiting Chinese cloud companies from storing and processing data on US citizens and businesses. Advocates of this approach argue that some degree of data sovereignty is inevitable. The global Internet still functions in the face of these rules, and companies continue to profit and innovate. Others argue that what is needed is for different nation-states to collaborate on common standards, agreeing to a set of core principles for the cloud and norms for government access to data stored there. Nonetheless, this chapter questions the remaining scope for subnational entities and, among them, for stateless algorithmic nations that present a strong will to bring their control of their citizens back through data devolution. This chapter claims that this debate has been absent for deepening democracy so far and requires further active positions to be taken by stakeholders in these territorial contexts by implementing the democratic toolkit consisting of four factors: algorithmic nations, data sovereignty, digital rights, and data cooperatives (Calzada, 2020g, h, i).

Alongside the debate on algorithmic nations, data sovereignty, digital rights, and data cooperatives, millions of companies now use cloud computing to store data and run applications and services remotely. Furthermore, the pandemic has exacerbated the way citizens telework by introducing a 24/7 remote pattern. The technological sovereignty term emerged to describe the many ways governments try to assert more control over the computing environments on which their nation-states rely. Thus, governments around the world are passing measures that require companies

to host data infrastructure and store certain kinds of data from citizens in local jurisdictions. Some also require companies that operate within their borders to provide the government with access to data and code stored in the cloud. This trend, especially when applied unilaterally, might erode the fundamental model of cloud computing that feeds, most importantly, non-European *big tech* firms—often without the public scrutiny of nation-states' governments—which relies on free movement of data across borders. A cloud user or provider should be able to deploy any application or data set to the cloud at any time or place. Thus, citizens should be able to select the data provider that can best meet their needs. To that end, the European Commission has established what are called "data ecosystems" without giving any clue about how local and regional authorities can self-govern and control their data power by relocating and devolving data ownership to their fellow citizens. Thus, in summary, this chapter suggests that stateless algorithmic nations need to start strategising in several policy areas without further ado: (i) to set up data strategies to have a say among pan-European agencies; (ii) to take the lead from the public sector on AI-intensive governance schemes; (iii) to explore the added value and the opportunity that blockchain may offer to better connect local administrations; (iv) to engage in collective actions through networks of cities, e.g. CCDR; (v) to implement data and platform cooperatives in stateless algorithmic nations as a way to reactivate socio-economic activity postpandemic; (vi) to further identify vulnerable groups in hyperconnected societies to avoid leaving them behind; and (vii) to put the digital rights of citizens at the forefront by prioritising actions in favour of protecting privacy and ensuring ownership.

Above all, how do we foresee stateless algorithmic nations operating through technological sovereignty in the postpandemic and post-Brexit scenario? Data sovereignty is a political outlook in which information and communications infrastructure and technology are aligned to the laws, needs, and interests of the city, region, or country in which users are located. Thus, data location and data devolution unequivocally matter as we have witnessed during the COVID-19 crisis. In postpandemic societies, the major challenge for the EU and the United Kingdom is to establish their cyber-sovereignty policy to be aligned with data ecosystems on the city-regional scale. In this endeavour, the emerging generation of digital cooperatives—so-called data and platform cooperatives—can clearly contribute (Calzada, 2020c). The EU and the United Kingdom are at the moment living labs for creating data and platform cooperatives stemming from data altruism and data donation. How can citizens be governed and organise themselves in stateless algorithmic nations to establish new social capital that could overcome the postpandemic social distancing measures and consequently the loss of social capital? These challenges ultimately boil down to protecting citizens' digital rights while relying on the capacity of cities and regions to deal with self-governing and interdependent data policies as the only possible way to ensure fairer European and British democracies.

## References


Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data Europe and China. *Economy and Society, 49*(2), 187–212. https://doi.org/10.1080/03085147.2019.1690275

Allam, Z. (2020). *Cities and digital revolution: Aligning technology and humanity*. Springer.

Andersen, R. (2020). *The panopticon is already here*. Retrieved from https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/

Arendt, H. (1949). The rights of man: What are they? *Modern Review, 3*, 4–37.

Berditchevskaia, A., & Baeck, P. (2020). *The future of minds and machines: How artificial intelligence can enhance collective intelligence*. NESTA.

Bigo, D., Isin, E., & Ruppert, E. (2019). *Data politics*. Routledge.

Borkin, S. (2019). *Platform co-operatives – solving the capital conumdrum*. NESTA.

Bridle, J. (2016). Algorithmic citizenship, digital statelessness. *GeoHumanities, 2*(2), 377–381. https://doi.org/10.1080/2373566X.2016.1237858

Burki, T. (2021). Equitable distribution of COVID-19 vaccines. *The Lancet Infectious Diseases, 21*(1), 33–34. https://doi.org/10.1016/S1473-3099(20)30949-X

Calzada, I. (2017a). Data devolution in Europe. *ESADE MSc Speaker Series. Big Data and Smart Cities*. Retrieved from https://www.youtube.com/watch?v=iP8LVQWrdJ0

Calzada, I. (2017b). The techno-politics of data and smart devolution in city-regions: Comparing Glasgow, Bristol, Barcelona, and Bilbao. *Systems, 5*(1), 18. https://doi.org/10.3390/systems5010018

Calzada, I. (2017c). Metropolitan and city-regional politics in the urban age: Why does "(smart) devolution" matter? *Palgrave Communications, 3*(17094), 1–17. https://doi.org/10.1057/palcomms.2017.94

Calzada, I. (2018a). 'Algorithmic nations': Seeing like a city-regional and techno-political conceptual assemblage. *Regional Studies, Regional Science, 5*(1), 267–289. https://doi.org/10.1080/21681376.2018.1507754

Calzada, I. (2018b). Metropolitanising small European stateless city-regionalised nations. *Space and Polity, 22*(03), 341–360. https://doi.org/10.1080/13562576.2018.1555958

Calzada, I. (2018c). (Smart) citizens from data providers to decision-makers? The case study of Barcelona. *Sustainability, 10*(9), 3252. https://doi.org/10.3390/su10093252

Calzada, I. (2019a). Technological sovereignty: Protecting citizens' digital rights in the AI-driven and post-GDPR algorithmic and city-regional European realm. *Regions eZine*, (4). https://doi.org/10.1080/13673882.2018.00001038

Calzada, I. (2019b). Catalonia rescaling Spain: Is it feasible to accommodate its "stateless citizenship"? *Regional Science Policy and Practice, 11*(5), 805–820. https://doi.org/10.1111/rsp3.12240

Calzada, I. (2020a). Democratising smart cities? Penta-helix multistakeholder social innovation framework. *Smart Cities, 3*(4), 1145–1172. https://doi.org/10.3390/smartcities3040057. Retrieved from https://www.mdpi.com/2624-6511/3/4/57

Calzada, I. (2020b). Emerging citizenship regimes and rescaling (European) nation-states: Algorithmic, liquid, metropolitan and stateless citizenship ideal types. In S. Moisio, N. Koch, A. E. Jonas, C. Lizotte, & J. Luukkonen (Eds.), *Handbook on the changing geographies of the state: New spaces of geopolitics*. Edward Elgar Publishing. https://doi.org/10.13140/RG.2.2.17301.6832/1

Calzada, I. (2020c). Platform and data co-operatives amidst European pandemic citizenship. *Sustainability, 12*(20), 8309. https://doi.org/10.3390/su12208309. Retrieved from https://www.mdpi.com/2071-1050/12/20/8309

Calzada, I. (2020d). *Tekno-Politika/Techno-Politics*. Retrieved from https://www.sarean.eus/tekno-politika/. https://doi.org/10.13140/RG.2.2.27126.22086/1

Calzada, I. (2020e). Will Covid-19 be the end of the global citizen? *Apolitical*. https://doi.org/10.13140/RG.2.2.11942.27208/1

Calzada, I. (2020f). Pandemic citizenship: Will COVID-19 reinforce nation-states' borders and liquify citizens? *Academia Letters*, 910. https://doi.org/10.20935/AL910
Calzada, I. (2020g). Gizarte mugimenduen rola gizarte berrikuntzan (GB): Euskaraldia, panoptiko digital gisa. *BAT, 115*(2), 85–114. https://doi.org/10.13140/RG.2.2.35980.05763/2
Calzada, I. (2020h). Herrigintza algoritmikoa eta adimen artifiziala post COVID-19 gizartean. *Galde*, 29. https://doi.org/10.13140/RG.2.2.33413.58081/1
Calzada, I. (2020i). *Euskal nazio algoritmikoa sortuz: Subirautza teknologikoa post-COVID-19 gizartean*. TMLab. https://doi.org/10.13140/RG.2.2.28853.01766/1
Calzada, I. (2021). *Smart city citizenship*. Elsevier Science Publishing Co.
Calzada, I., & Almirall, E. (2020). Data ecosystems for protecting European citizens' digital rights. *Transforming Government: People, Process and Policy, 14*(2), 133–147. https://doi.org/10.1108/TG-03-2020-0047
Cheney-Lippold, J. (2011). A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture and Society, 28*(6), 164–181. https://doi.org/10.1177/0263276411424420
Cherry, M. (2016). Beyond misclassification: The digital transformation of work. *Comparative Labor Law and Policy Journal, 37*(577), 1–27.
Chiusi, F., Fischer, S., Kayser-Bril, N., & Spielkamp, M. (2020). *Automating Society Report 2020*.
Christensen, B. (2019). Cyber state capacity: A model of authoritarian durability, ICTs, and emerging media. *Government Information Quarterly, 36*(3), 460–468. https://doi.org/10.1016/j.giq.2019.04.004
Christl, W. (2017). Corporate surveillance in everyday life. In *How companies collect, combine, analyze, trade, and use personal data on billions*. A Report by Cracked Labs. Retrieved from http://crackedlabs.org/en/corporate-surveillance/info
Christl, W., & Spiekermann, S. (2016). *Networks of control: Corporate surveillance, digital tracking, big data and privacy*. Retrieved from http://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf
Cities Coalition for Digital Rights. (2019). *Declaration of cities coalition for digital rights*. Retrieved from https://citiesfordigitalrights.org/
Csernatoni, R. (2020). New states of emergency: Normalizing techno-surveillance in the time of COVID-19. *Global Affairs, 6*, 301–310. https://doi.org/10.1080/23340460.2020.1825108
Datta, A. (2020). Self(ie)-governance: Technologies of intimate surveillance in India under COVID-19. *Dialogues in Human Geography, 10*, 234–237. https://doi.org/10.1177/2043820620929797
Datta, A., Aditi, A., Ghoshal, A., Thomas, A., & Mishra, Y. (2020). Apps, maps and war rooms: On the modes of existence of "COVtech" in India. *Urban Geography, 42*(3), 382–390. https://doi.org/10.1080/02723638.2020.1807165
Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance. *International Data Privacy Law, 9*(4), 236–252. https://doi.org/10.1093/idpl/ipz014
Delipetrev, B., Tsinaraki, C., & Kostic, U. (2020). *Historical evolution of artificial intelligence*.
Dixson-Declève, S. (2020). *Protect, prepare and transform Europe: Recovery and resilience post COVID-19*.
Dyer-Witheford, N., Kjosen, M., & Steinhoff, J. (2019). *Inhuman power artificial intelligence and the future of capitalism*. Pluto Press.
European Commission. (2020). *Data governance act*. https://wayback.archive-it.org/12090/20210728140407/https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767
Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy and Technology, 33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6
Foundational Economy Collective. (2020). *What comes after the pandemic? A ten-point platform for foundational renewal*. Retrieved from https://foundationaleconomy.com
GaiaX. (2020). *GaiaX*. Retrieved from https://www.politico.eu/article/germany-france-gaia-x-cloud-platform-eu-tech-sovereignty/

Gekker, A., & Hind, S. (2019). Infrastructural surveillance. *New Media and Society, 22*, 1414–1436. https://doi.org/10.1177/1461444819879426

Goggin, G., Vromen, A., Weatherall, K., Martin, F., & Sunman, L. (2019). Data and digital rights: Recent Australian developments. *Internet Policy Review, 8*(1), 1–19. https://doi.org/10.14763/2019.1.1390

Hand, D. J. (2020). *Dark data*. Princeton University Press.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2017). Digital citizenship and surveillance society. *International Journal of Communications, 11*, 731–739. Retrieved from http://ijoc.org/index.php/ijoc/article/view/5521

Hobbs, C. (2020). *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data and Society, 8*(1), 1–17. https://doi.org/10.1177/2053951720982012

Janssen, M., Hartog, M., Matheus, R., Yi Ding, A., & Kuk, G. (2020). Will algorithms blind people? The effect of explainable AI and decision-makers' experience on AI-supported decision-making in government. *Social Science Computer Review, 40*(2), 478–493. https://doi.org/10.1177/0894439320980118

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, 24*, 362–381. https://doi.org/10.1080/13562576.2020.1770587

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media and Society, 21*(7), 1565–1593. https://doi.org/10.1177/1461444819826402

Levy, K., & Barocas, S. (2018). Refractive surveillance: Monitoring customers to manage workers. *International Journal of Communications, 12*, 1166–1188. Retrieved from http://ijoc.org/index.php/ijoc/article/view/7041

Lightfoot, G., & Wisniewski, T. P. (2014). Information asymmetry and power in a surveillance society. *Information and Organization, 24*(4), 214–235. https://doi.org/10.1016/j.infoandorg.2014.09.001

Loukissas, Y. A. (2019). *All data are local: Thinking critically in a data-driven society*. MIT Press.

Lucas, E. (2020). *Pandemic democracy*. Retrieved from https://www.cepa.org/pandemic-democracy

Lupton, D., & Michael, M. (2017). Depends on who's got the data: Public understandings of personal digital dataveillance. *Surveillance and Society, 15*(2), 254–268.

Lutz, C. (2019). Digital inequalities in the age of artificial intelligence and big data. *Human Behavior and Emerging Technologies, 1*(2), 141–148. https://doi.org/10.1002/hbe2.140

Maxmen, A. (2019). Surveillance science. *Nature, 569*, 614–617.

Mazzucato, M., Entsminger, J., & Kattel, R. (2020). *Public value and platform governance*.

McCann, D., & Yazici, E. (2018). *Disrupting together: The challenges (and opportunities) for platform co-operatives*.

Morozov, E. (2020). *The tech 'solutions' for coronavirus take the surveillance state to the next level*. Retrieved from https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveilance-state-digital-disrupt

Moulaert, F., & MacCallum, D. (2019). *Advanced introduction to social innovation*. Edward Elgar.

Muldoon, J., & Stronge, W. (2020). *Platforming equality: Policy challenges for the digital economy*.

Nguyen, J. (2017). Identity, rights and surveillance in an era of transforming citizenship. *Citizenship Studies, 22*, 86–93. https://doi.org/10.1080/13621025.2017.1406456

Nichols, T. P., & LeBlanc, R. J. (2020). Beyond apps: Digital literacies in a platform society. *The Reading Teacher, 74*(1), 103–109. https://doi.org/10.1002/trtr.1926

Pentland, A., Hardjono, T., Penn, J., Colclough, C., Ducharmee, B., & Mandel, L. (2019). *Data cooperatives: Digital empowerment of citizens and workers*.

Pilkington, E. (2019). *Digital dystopia: How algorithms punish the poor*. Retrieved from https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor

Prainsack, B. (2020). Solidarity in times of pandemics. *Democratic Theory, 4*(2), 124–133. Retrieved from https://www.berghahnjournals.com/view/journals/democratic-theory/7/2/democratictheory.7.issue-2.xml

Rikap, C. (2020). Amazon: A story of accumulation through intellectual rentiership and predation. *Competition and Change, 26*(3–4), 436–466. https://doi.org/10.1177/1024529420932418

Scholz, T. (2016). *Platform cooperativism: Challenging the corporate sharing economy*. Rosa Luxemburg Stiftung.

Scholz, T., & Calzada, I. (2021). Data cooperatives for pandemic times. *Public Seminar Journal*. Retrieved from https://publicseminar.org/essays/data-cooperatives-for-pandemic-times/; https://doi.org/10.13140/RG.2.2.12320.51200/1

Smuha, N. A. (2020). Beyond a human rights-based approach to AI governance: Promise, pitfalls, plea. *Philosophy and Technology, 34*(1), 91–104. https://doi.org/10.1007/s13347-020-00403-w

Stucke, E., & Grunes, A. P. (2017). *Data-Opolies*. Retrieved from https://ssrn.com/abstract=2927018 or https://doi.org/10.2139/ssrn.2927018

Taylor, A. (2020). *The People's platform: Taking back power and culture in the digital age*. Metropolitan Books.

Thorhallsson, B. (2006). The size of states in the European Union: Theoretical and conceptual pespectives. *European Integration, 28*(1), 7–31.

Thorhallsson, B. (2016). *The role of small states in the European Union*. Routledge.

Tommaso, F. (2020). An alternative to data ownership: Managing access to non-personal data through the commons. *Global Jurist, 21*, 181–210. https://doi.org/10.1515/gj-2020-0034

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance and Society, 12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Wong, P.-H. (2020). Cultural differences as excuses? Human rights and cultural values in global ethics and governance of AI. *Philosophy and Technology, 33*, 705–715. https://doi.org/10.1007/s13347-020-00413-8

Zabalo, J., & Iraola, I. (2020). Current discourses and attitudes in favour of the independence of the Basque Country. *Regional and Federal Studies, 32*(1), 73–93. https://doi.org/10.1080/13597566.2020.1831475

Zabalo, J., Larrinaga, A., Iraola, I., Saratxo, M., Amurrio, M., Mateos, T., Fullaondo, A., & Anduaga, U. (2016). *Imagining the Basque state: Opinions and attitudes with respect to a Basque state in Euskal Herria. A quantitative and qualitative study*. Parte Hartuz ikerketa taldea, Ipar Hegoa Fundazioa.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile.