Pandemic Citizenship Amidst Stateless Algorithmic Nations:

Digital Rights and Technological Sovereignty at Stake

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 techno-political 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. In order to shed light on this debate, this article introduces the term 'pandemic citizenship' to better understand the extreme circumstances in which citizens have been surviving. Particularly, this article attempts to provide an overview by focussing on stateless nations and the need to conduct further research and gather policy evidence to articulate counter political strategies as 'algorithmic nations'. The COVID-19 pandemic has inevitably raised the need to resiliently and techno-politically respond to threats that hyper-connected and highly virialised societies produce. Amidst the increasingly artificial intelligence (AI)-driven governance systems in several nation-states in Europe, this article spotted the need to devolve data power to citizens through data ecosystems in European stateless algorithmic nations. This article argues that in the absence of a coordinated and inter-dependent strategy to claim digital rights and technological sovereignty by a set of stateless algorithmic nations in Europe, on the one hand, Big Tech *data-opolies,* and on the other hand, the General Data Protection Regulation (GDPR) led by the European Commission, might bound and expand, respectively, stateless nations' capacity to mitigate the negative side effects of algorithmic disruption. Individually, we already observed subtle reactions in several nations, including Catalonia and Scotland, that are unlikely to be consistent unless a joint strategy takes place at the European level by stakeholders operating in these nations' techno-political spheres.

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

1. Introduction: Pandemic Citizenship

Citizens in Europe have likely been pervasively surveilled during and probably as a result of the COVID-19 crisis (Aho & Duffield, 2020; Csernatoni, 2020; Hintz, Dencik, & Wahl-Jorgensen, 2017; Kitchin, 2020; Zuboff, 2019). Despite the fact that the homologation of the vaccine has 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 sovereignty (Calzada, 2020b). But how can e-democracy be ensured for all citizens while also creating further

This crisis has accelerated the need to increase the human and social understanding of the potential and risk of 'techno-politics' for 'pandemic citizens'.

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, Aditi, Ghoshal, Thomas, & Mishra, 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 (Delacroix & Lawrence, 2019) to claim digital rights and technological/digital/data sovereignty (Calzada, 2019a)? What does sovereignty mean for stateless citizens (Calzada, 2019b) amidst the pandemic crisis wrapped in an algorithmic global disruption (Dixson-Declève, 2020)?

The COVID-19 pandemic has stressed the growing impact of digital technologies in political and social life (Cheney-Lippold, 2011; Datta, 2020). Contact-tracing applications on mobile phones have raised 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, 2020e; 2021) —f or '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 AI (AI; Berditchevskaia & Baeck, 2020; Delipetrev, Tsinaraki, & Kostic, 2020; Dyer-Witheford, Kjosen, & Steinhoff, 2019; Lutz, 2019; Misuraca, 2020). The Cambridge Analytica scandal in the United Kingdom (UK), 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 (Lupton & Michael, 2017; Smuha, 2020; van Dijck, 2014; Wong, 2020).

Against this backdrop, the European Union (EU)'s 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 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, digital/data/technological sovereignty, and so on (Calzada & Almirall, 2020). This article aims to provide a substantial and original 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 challenges raised by the spread of claims towards technological sovereignty in stateless 'algorithmic nations' (Calzada, 2018a).

This era has slowed down several mundane routines for citizens and increased professional pressures, emotional fears, algorithmic exposure.

Nominally, over the last few decades, globalisation has led to a new class of global citizenship (Calzada, 2020f; Nguyen, 2017). While 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 post-COVID-19 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.

Actually, the 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 co-operatives and reinforcing social capital. 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 techno-political vulnerabilities among pandemic citizens (Bigo, Isin, & Ruppert, 2019). A particular collective intelligence response emerging in Europe has been the creation of digital co-operatives (Borkin, 2019; Cherry, 2016; McCann & Yazici, 2018), also known as *platform co-operatives* (Scholz, 2016) and *data co-operatives* (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, Fischer, Kayser-Bril, & Spielkamp, 2020): not only fixing market failure 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 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 article refers to it as fostering social innovation among stakeholders in civil societies (Moulaert & MacCallum, 2019) in stateless nations (Calzada, 2018b). The COVID-19 crisis has clearly shown that citizens in stateless nations are not only highly dependent on data and

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

Citizens in stateless nations are highly dependent on data and its economic value but also influenced by the techno-political biosurveillance it generates.

the economic value it creates but also directly influenced by the techno-political biosurveillance it generates. 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, 2017b; Loukissas, 2019). In doing so, this article introduces and contextualises the term 'stateless algorithmic nations' (Calzada, 2018a).

2. Debate on cybercontrol vs. civil liberties: evidence on digital rights post-COVID-19

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. Contact-tracing apps have shown profound implications for privacy, governmentality, control creep and citizenship, and they reinforce the logic of 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 socio-technical 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 concerns have produced a debate not just about the bounce-back to pre-COVID-19 normality but the bounce-forward to a more resilient and fair citizenship through foundational economic principles (Foundational Economy Collective, 2020).

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.

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 modeling 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

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

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 with a sense of control over their bodies via a playful mode of self-surveillance. Such a perspective relates to this article's interest in pandemic citizens' digital rights concerning technological sovereignty (Hobbs, 2020). Data sovereignty through well-informed, transparent public action and active social engagement therefore emerges as a crucial issue related to the digital rights of citizens.

Data sovereignty through well-informed, transparent public action and active social engagement emerges as a crucial issue.

As an amplifier of pre-existing concerns about digital rights, the COVID-19 crisis has underlined the absolute critical role of digital data governance 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 re-used have become central questions during the COVID-19 crisis in relation to citizens' digital rights.

Another critical aspect of technological 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, Entsminger, & Kattel, 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 AI and 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 socially or economically disadvantaged groups in stateless city-regional nations such as Catalonia or Scotland.

In the backdrop of these subtle reactions of stateless nations, a wide range of stakeholders in cities and regions are debating citizens' digital rights through accountable data ethics. This article 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, Hartog, Matheus, Yi Ding, & Kuk, 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.

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

Privacy is one inalienable and non-negotiable human right in a democracy and any decisions citizens make now will resonate for far longer than the virus will.

In order to provide evidence of such examples of digital rights in cities and regions in times of COVID-19, the Coalition of Cities for Digital Rights (CCDR), encompassing more than 50 global cities (www.citiesfordigitalrights.org), is worth mentioning. It is 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.

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. But 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 impacts on digital rights (Goggin, Wromen, Weatherall, Martin, & Sunman, 2019). How do we adequately balance the values of privacy and autonomy with those 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 inalienable and non-negotiable human rights 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, geo-location 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 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 center of their design and application? In order to shed some light on this issue, this article has hereby collected the following evidence produced during the outbreak of COVID-19 in 2020:

(i)   Action Plan for Digital Rights for COVID-19 by the City of Amsterdam, Netherlands. Some of the measures by the city aimed to explore how to support the move of the arts and creative industry online, to monitor the impact of cyber activity on our digital safety and to monitor the stability and resilience of the Internet in Amsterdam. Risks in supply chains for public safety were mapped. The COVID-19 data exchange was started to support the crisis team with data-gathering and analysis to measure the impact of measures, for example on mobility. Research and development on which tech could be used to ease the lockdown process has started to 'Unlock Amsterdam' (www.amsterdam.nl/digitalesta and https://www.amsterdam.nl/en/coronavirus/overview/).

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

(ii)   COVID-19 Extension of Telecare Service and VinclesBCN App - City of Barcelona, Catalonia. The City Hall of Barcelona opted for the extension of Telecare, which had almost 90,000 users and the Radars programme (1,600 users) that monitors people living alone with the collaboration of the neighbourhood network, as well as an extension of the VinclesBCN App service (2,400 users) that monitors elderly people. They also created a health channel to address the doubts that these people have (https://ajuntament.barcelona.cat/ personesgrans/es/canal/teleassistencia and https://ajuntament.barcelona.cat/vinclesbcn/ es/conoce-las-aplicaciones-0).

(iii)   Human Communication and Transparency vs. COVID-19 - City of Bratislava, Slovakia. The City of Bratislava identified transparency and human communication as success factors to navigate these challenging times. Consequently, the Mayor of Bratislava commissioned a famous local cartoonist to draw posters to inform citizens about the necessary measures to fight the coronavirus outbreak in a clear and simple fashion. These posters, made available both online and throughout the city, have been translated to English and the City Hall is enthusiastic about sharing an adaptable version with interested municipalities. Moreover, Slovakian IT communities collaborated with information dissemination and emotion curbing, with initiatives like 'covid.chat' a free chatbot (https://www.ktopomozeslovensku.sk/).

(iv)   Data-Driven Prediction and Citizen Engagement Techniques - City of Helsinki, Finland. Mikko Russama, Chief Digital Officer (CDO) at the City of Helsinki, provided a video intervention focussed on the three dimensions of the crisis: health, social life and the economy. He stressed the value of effective preparation, data-driven tracking and citizen engagement techniques. Helsinki's crisis management model included a taskforce divided into different areas and making predictive analysis. The need to have the right data was emphasised (https://www.intelligentcitieschallenge.eu/sites/default/files/2020-04/ICC_COVID-19_ Webinar_3_April_2020.pdf).

(v)   Connecting the Elderly: Digital Helpline and Prepopulated Tablets - City of New York, United States (US). The Mayor of NYC announced a new programme that entails the distribution of tablets to vulnerable and disconnected communities, such as seniors, in specific underserved areas of the city. The city partnered with T-Mobile to provide pre-populated tablets with apps that might be useful for them and a service telephone line for assistance and usage guidance. Seniors get to keep the tablet afterwards (http://bronx.news12.com/story/42035900/watch-live-mayor-gives-update-on-covid19-in-nyc).

(vi)   PEPP-PT & DP-3T: COVID-19-Related Technologies - Pan-European Initiatives. Europe developed its own technology, such as Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) and the DP-3T, which in the event of infection allowed citizens to keep track of the contacts they had had in recent days, while respecting the privacy of both those who tested positive and their contacts. The European Commission launched a set of guidelines and recommendations about the use of these contact-tracing apps (https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf).

(vii)   COVID-19 Open Data Hub & Digital Inclusion Partnerships - City of San Antonio, US. The City of San Antonio (Texas) developed an open data hub for citizens and interested stakeholders to access updated statistical information on COVID-19 on a daily basis. The hub site enabled citizens to download these data sets and application programming interfaces (APIs) while exploring useful links and maps about COVID-19 application. These applications and dashboards provided Health Insurance Portability and Accountability Act (HIPAA)-compliant, county-

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

wide information about testing, hospital capacity and case data, in addition to key health and capacity metrics the city and local health authority were tracking as Texas began to reopen. In one week, over three million hits were recorded on the public COVID-19 dashboards, with an average number of 450,920.86 visits per day. The Open Data Hub Site received nearly 20,000 visits two weeks after deployment, averaging over 1.5 thousand visits daily. A digital inclusion taskforce with over 100 members, including 50 agencies and organisations, as well as local school districts, was formed to coordinate digital inclusion efforts during the pandemic. The taskforce created a digital inclusion resources and needs tool and a list of service providers for connectivity and literacy. San Antonio's geographic digital divide was made particularly evident when the city mapped participation rates of an online self-screening COVID-19 tool. The tool made recommendations to residents for testing based on a series of questions regarding their symptoms. To address participation rates that were lower in areas that lacked Internet connectivity, the city responded with a taskforce that provided critical health information to disconnected residents on a door-to-door basis. To further address the digital divide, San Antonio also partnered with local transportation authority VIA on the program VIACares, which provides free Wi-Fi to underserved areas with otherwise underutilised vans during the pandemic (https://cosacovid-cosagis.hub.arcgis. com/ ; https://www.viainfo.net/cares/ ; https://cosagis.maps.arcgis.com/apps/MapSeries/ index.html?appid=9cdb2a0222ff4b4fb81b1452fd9d15fa).

(viii)   'Solidarity City Action' & CIL's COVID-19 App Extension: A Network of Public and Civil Solidarity - City of São Paulo, Brazil. The City Hall of São Paulo collaborated with several civil organisations to create the 'Solidarity City Action', a platform for donations to help the city's most vulnerable populations. The website provided citizens with information on where the eight drive-thru points were located and the type of expected donations (from staple food to hygiene products). The page also included an interactive map next to ongoing actions and figures. Additionally, the Sign Language Intermediation Center (CIL) launched a new service offering guidance on COVID-19. São Paulo City Hall's mobile app brought information about the coronavirus to people with hearing impairment. By accessing a specific icon and making a call, the interpreter would know that it was a request about COVID-19. In addition to the COVID-19 guidance option, the app offered other emergency, security and utility services. Besides meeting the demand from the deaf community, it also focussed on municipal public servants, who were able to download the app on their smartphones and use it when they had to assist a citizen who only communicated in sign language (https://www.spcidadesolidaria. org/; https://www.prefeitura.sp.gov.br/cidade/secretarias/pessoa_com_deficiencia/ central_de_libras/index.php?p=203752).

(ix)   Open & free courses on e-commerce for SMEs - City of Zaragoza, Spain. Zaragoza's City Hall and Chamber of Commerce made free online courses available for small and medium-sized entreprises (SMEs) to be able to offer their services and products digitally to citizens. These included digital marketing, advertising on the Internet, web analytics, and social networks in retail. All were aimed at empowering local commerce with the skills necessary for their digital transformation so that no SMEs were left behind (https://www.camarazaragoza.com/ empresa-en-marcha/; https://www.camarazaragoza.com/productos/curso-de-comercio- electronico-nuevas-oportunidades-para-el-comercio/).

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

3. Stateless algorithmic nations: digital rights and technological sovereignty at stake

The evidence presented in the previous section regarding the CCDR shows the importance of digital rights in several global cities worldwide, which locates the need for a debate on technological sovereignty in full consideration at the subnational level — namely, stateless nations. How are these digital rights related to claims for further data devolution of stateless nations? This article suggests a new term to refer to the way stateless nations need to approach the post-COVID-19 digital revolution: *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 techno-political 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).

Full democracy can only survive in stateless nations if citizens are able to make better choices than machines owned by big tech companies.

COVID-19 responses have shown the importance of the motto *small is beautiful* (Calzada, 2020d; Thorhallsson, 2006, 2016). Highly decentralised city-regions have demonstrated their ability to better cope with resilient pandemic responses in established small-state cases, such as New Zealand, Iceland, Ireland, Denmark, The 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 technological 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 digital sovereignty may impact young people in intermediary cities, denying them financing, employment, entrepreneurship, education and training opportunities offered on digital platforms and locking many young people and key stakeholders out from participating directly in the digital economy and governance.

Against this backdrop, in a 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 data control to citizens. Claims to technological sovereignty through data commons policy programmes are increasingly emerging in several locations. In a post-GDPR scenario, citizens' data privacy, security and ownership ultimately need to be protected by localising personal data via grassroots innovation and co-operative platforms as has been the case in Barcelona and Catalonia overall (Calzada, 2018c). How citizenship in small algorithmic stateless nations will be influenced and shaped by geopolital 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 can only survive in stateless nations if citizens are able to make better choices than machines owned by big tech companies that are becoming more powerful than 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

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

Stateless algorithmic nations should establish an alternative techno-political discourse on citizens' digital and data rights.

algorithmic nations. In this direction, new versions of the e-state in Estonia may already offer 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 techno-political 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 techno-political discourse on citizens' digital and data rights.

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

(i) Barcelona in Catalonia: Barcelona has been focussing 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 universities. A specific contextual aspect that has leveraged the relevance of digital rights in Barcelona has been a 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 and equal access to the Internet and digital literacy are seen as the main priorities alongside transparency, accountability and non-discrimination in 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 private companies, especially those providing public services. However, according to 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 co-operatives sharing health data to tackle COVID-19. Finally, citizens have so far reacted posivitively to the City Hall's adoption of AI that particularly focusses on social services, transport and mobility. The way in which the claim for digital rights could be scaled up towards further technological sovereignty at the regional level remains to be seen.

(ii) Glasgow in Scotland: Glasgow has been focussing 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 focussing on establishing its 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 within its citizens. Given that tackling social inequalities is the most pressing need for the city of Glasgow, local authorities have actively been implementing measures to achieve universal and equal access to the Internet and digital literacy. According to a 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

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

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

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 technological 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 co-operatives could assist the city in tackling COVID-19-driven economic and social vulnerabilities among pandemic citizens. Regarding existing data co-operative initiatives in the city, interestingly there are more general data-sharing agreements being established between public bodies that could provide the basis for data co-operatives. 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, in which Glasgow has an active role and a say in the technological sovereignty-driven strategy on AI, which essentially shows what this article is attempting to depict: an inter-dependent joint effort between Glasgow's claim on digital rights and a strategy on technological sovereignty by the stateless algorithmic nation of Scotland. Regarding how citizens would react to the adoption of AI for implementation 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.

4. Final Remarks

COVID-19 has been a trigger for increasing the impact of digital transformations on the daily lives of citizens.

COVID-19 has been a trigger for increasing the impact of digital transformations on the daily lives of citizens. 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 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 concerns about the role of citizens in this timely debate. The aim of Gaia-X is apparently to direct European companies toward domestic cloud providers. Paradoxically, China's Cybersecurity Law mandates that certain data be stored on local servers or undergo a security assessment before exportation. 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 article 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

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

back through data devolution. This article claims that this debate has been absent so far and requires further active positions to be taken by stakeholders in these territorial contexts, as has been shown in two cases in the previous section.

The challenge for the EU and UK is to establish cyber-sovereignty policies to be aligned with data ecosystems on the city-regional scale.

Alongside the debate on technological sovereignty, 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 term "technological sovereignty" 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 the 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 article 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 co-operatives in stateless algorithmic nations as a way to reactivate socio-economic activity post-pandemic; (vi) to further identify vulnerable groups in hyper-connected 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 post-COVID-19 and post-Brexit scenario? Technological 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 devolution unequivocally matter as we have witnessed during the COVID-19 crisis. In post-COVID-19 societies, the major challenge for the EU and the UK is to establish their cyber-sovereignty policies to be aligned with data ecosystems on the city-regional scale. In this endeavour, the emerging generation of digital co-operatives — so-called data and platform co-operatives — can clearly contribute (Calzada, 2020c). The EU and the UK are at the moment living labs for creating data and platform co-operatives stemming from data altruism and donation. How can citizens be governed and organise themselves in stateless algorithmic nations to establish new social capital that could overcome post-COVID-19 social distancing measures and consequently a 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 inter-dependent data policies as the only possible way to ensure fairer European and British democracies.

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

References

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

Allam, Z. (2020). *Cities and Digital Revolution: Aligning technology and humanity.* Cham: 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.* London: NESTA.

Bigo, D., Isin, E., & Ruppert, E. (2019). *Data Politics.* London: Routledge.

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

Bridle, J. (2016). Algorithmic Citizenship, Digital Statelessness. *GeoHumanities, 2*(2), 377-381. doi:10.1080/2373566X.2016.1237858

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

Calzada, I. (2017a). Data Devolution in Europe. *ESADE MSc Speaker Series: Big Data & 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. doi:10.3390/systems5010018

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

Calzada, I. (2018b). Metropolitanising Small European Stateless City-Regionalised Nations. *Space and Polity, 22*(03), 341-360. doi:10.1080/13562576.2018.1555958

Calzada, I. (2018). (Smart) Citizens from Data Providers to Decision-Makers? The Case Study of Barcelona. *Sustainability, 10*(9), 3252. doi:10.3390/su10093252

Calzada, I. (2019b). Catalonia Rescaling Spain: Is It Feasible to Accommodate Its "Stateless Citizenship"? *Regional Science Policy & Practice, 11*(5), 805-820. doi:10.1111/rsp3.12240

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). doi:10.1080/13673882.2018.00001038

Calzada, I. (2020a). Democratising Smart Cities? Penta-Helix Multistakeholder Social Innovation Framework. *Smart Cities, 3*(4), 1145-1172. doi:10.3390/smartcities3040057. Retrieved from https://www.mdpi.com/2624-6511/3/4/57

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

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*. Cheltenham, UK and Northampton, MA, USA: Edward Elgar Publishing. doi:10.13140/RG.2.2.17301.6832/1.

Calzada, I. (2020c). Platform and Data Co-Operatives amidst European Pandemic Citizenship. *Sustainability, 12*(20), 8309. doi:10.3390/su12208309. Retrieved from https://www.mdpi.com/2071-1050/12/20/8309

Calzada, I. (2020d). Setting up the Basque Algorithmic Nation: Technological Sovereignty Amidst the Post-COVID-19 Society / Euskal Nazio Algoritmikoa Sortuz: Subirautza Teknologikoa Post-COVID-19 Gizartean. In TMLab (ed), *Reflections on COVID-19*. Donostia: Elkar.

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

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

Calzada, I. (2021). *Smart City Citizenship.* Cambridge, Massachusetts: Elsevier Science Publishing Co Inc.

Calzada, I., & Almirall, E. (2020). Data Ecosystems for Protecting European Citizens' Digital Rights. *Transforming Government: People, Process and Policy, 14*(2), 133-147. doi:10.1108/TG-03-2020-0047

Cheney-Lippold, J. (2011). A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society, 28*(6), 164-181. doi:10.1177/0263276411424420

Cherry, M. (2016). Beyond Misclassification: The Digital Transformation of Work. *Comparative Labor Law & 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. doi:10.1016/j.giq.2019.04.004

Christl, W. (2017). Corporate Surveillance in Everyday Life. 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,* 1-10. doi:10.1080/23340460.2020.1825108

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

Datta, A. (2020). Self(ie)-governance: Technologies of intimate surveillance in India under COVID19. *Dialogues in Human Geography,* 2043820620929797. doi: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,* 1-9. doi: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.* doi: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*. London: Pluto Press.

European Commission (2020). *Data Governance Act*.

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology, 33*(3), 369-378. doi: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 & Society*, 1461444819879426. doi: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. doi:10.14763/2019.1.1390.

Hand, D. J. (2020). *Dark Data*. Princeton: 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.*

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,* 0894439320980118. doi: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,* 1-20. doi:10.1080/13562576.2020.1770587

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society, 21*(7), 1565-1593. doi: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. doi: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.* Massachusetts: 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 & 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. doi: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.*

Misuraca, G. (2020). Artificial Intelligence and public sector innovation in a data-driven society: Shaping Digital Europe 2040.

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.* Cheltenham: 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,* 1-8. doi: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. doi: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

Pandemic Citizenship Amidst Stateless Algorithmic Nations:
Digital Rights and Technological Sovereignty at Stake

POST-COVID EUROPE SERIES - 4

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 & Change,* 1024529420932418. doi:10.1177/1024529420932418

Scholz, T. (2016). *Platform Cooperativism: Challenging the Corporate Sharing Economy.* New York: Rosa Luxemburg Stiftung.

Smuha, N. A. (2020). Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea. *Philosophy & Technology.* doi:10.1007/s13347-020-00403-w

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

Taylor, A. (2020). *The People's Platform: Taking Back Power and Culture in the Digital Age.* NYC: 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.* Oxon: Routledge.

Tommaso, F. (2020). An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons. *Global Jurist*(0), 20200034. doi:10.1515/gj-2020-0034

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197-208. doi: 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 & Technology,* 1-11. doi:10.1007/s13347-020-00413-8

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* London: Profile.

Acknowledgements
Coppieters publications