The Virus of Surveillance: How the COVID-19 pandemic is fuelling technologies of control*

Félix Tréguer**

July 2021

Abstract

While it is too early to provide a definitive analysis of the impact that the COVID-19 health crisis will have on digital state surveillance, this article aims to provide a first assessment. It starts by situating states' response to the crisis in the longer history of epidemics and their connections to what philosopher Michel Foucault called "regimes of power." By surveying various surveillance discourses and practices in countries like France, Italy, the United Kingdom, the United States or Israel in the Spring of 2020, the article identifies three key trends magnified by the crisis, namely, the crystallisation of new public-private assemblages in the management of health data, a shift towards health-based justification regimes for legitimising controversial surveillance and urban policing technologies, as well as mounting human rights threats and oversight failures in a context marked by a "state of health emergency".

Keywords

COVID-19, crisis, governing, health, security, state, surveillance, technology

*Author manuscript, to be published in Political Anthropological Research on International Social Sciences (PARISS) 2 (1).

**Félix Tréguer is associate researcher at the CNRS Center for Internet and Society and postdoctoral fellow at CERI-Sciences Po. His research blends political history and theory, law as well as media and technology studies to look at the political history of the Internet and computing, power practices like surveillance and censorship, the algorithmic governmentality of the public sphere, and more broadly the digital transformation of the state and of the security field. He is a founding member of La Quadrature du Net, a French advocacy group dedicated to the defence of civil rights in relation to digital technologies. Contact: felix.treguer@sciencespo.fr – CERI 56 rue Jacob – 75006 Paris FRANCE. Acknowledgement: This research was supported by the French National Research Agency (ANR) through the GUARDINT project (Grant n°18-ORAR-0006-01).

Introduction

Some of the measures adopted by states in the Spring of 2020 to deal with the COVID-19 pandemic give a sense of the ratchet effect currently sweeping polities across the world. In Western Australia, the governor gained authority to put individuals suspected of being infected with the new coronavirus in isolation, and mandate that they wear electronic bracelet to monitor their every moves.[1] Through an application installed on their smartphones which embeds geolocation and facial recognition features, Polish residents placed in quarantine had to authenticate themselves by regularly sending the police a selfie taken from their home.[2] Meanwhile, in New Zealand, the police launched a digital platform, inviting citizens to denounce the violations of lock-down measures they might witness.[3]

For many of us, mobilising policing technologies as a way to manage a health crisis might have appeared somewhat archaic. Thanks to the development of medicine, we tended to take for granted a continuous decline in large-scale epidemics and the major political disorders they have sparked throughout history. By doing so however, we overlooked the role played by capitalism – through the destruction of natural habitats, industrial agriculture or the ever-increasing acceleration of international flows – in the spread of new pathogens.[4] Sure, since the 1990s, many experts had insisted on the resurgence of epidemic risks, which materialised with the SARS, H5N1 or the Ebola epidemics. But technology seemed able to mitigate that risk, as global health actors like the World Health Organisation or the Bill and Melinda Gates Foundation heralded the use of Big Data analytics to provide for the early detection of infectious diseases and prevent large-scale crisis.[5]

Alas, digital technologies have been of little help in preventing the COVID-19 pandemic disaster. Instead, they have largely been used to scale-up

[1] Simon Sharwood, 'Australian State Will Install Home Surveillance Hardware to Make Sure If You're in Virus Isolation, You Stay There', The Register, 1 April 2020, https://www.theregister.co.uk/2020/04/01/west_australia_isolation/.

[2] Anna Koper and Douglas Busvine, 'In Europe, Tech Battle against Coronavirus Clashes with Privacy Culture', *Reuters*, 26 March 2020, https://www.reuters.com/article/us-health-coronavirus-europe-tech-poland-idUSKBN21D1CC.

[3] Eleanor Ainge Roy, 'New Zealand Site to Report Covid-19 Rule-Breakers Crashes amid Spike in Lockdown Anger', *The Guardian*, 30 March 2020, sec. World news, https://www.theguardian.com/world/2020/mar/30/new-zealand-site-to-report-covid-19-rule-breakers-crashes-amid-spike-in-lockdown-anger.

[4] Rob Wallace, *Big Farms Make Big Flu: Dispatches on Infectious Disease, Agribusiness, and the Nature of Science* (New York: Monthly Review Press, U.S., 2016); Sonia Shah, 'The Microbes, the Animals and Us', Le Monde diplomatique, 1 March 2020, https://mondediplo.com/2020/03/05coronavirus; Anonymous, 'Social Contagion: Microbiological Class War in China', *Chuang*, 1 March 2020, http://chuangcn.org/2020/02/social-contagion/.

[5] Tim Eckmanns, Henning Füller, and Stephen L. Roberts, 'Digital Epidemiology and Global Health Security: An Interdisciplinary Conversation', *Life Sciences, Society and Policy* 15, n°1 (19 March 2019): 2.

surveillance and enforce new restrictions on rights and freedom. In this article, I take stock of the impact of the COVID-19 pandemic for digital state surveillance. After situating this latest health crisis in the longer history of epidemics and their connections to what philosopher Michel Foucault called "regimes of power," I survey three key trends magnified by this crisis, namely, the crystallisation of new public-private assemblages in the realm of surveillance and the management of health data, a shift towards health-based justification regimes for the roll-out of new surveillance technologies, and mounting human rights threats and oversight failures amidst the new global context of "state of health emergency." I conclude by noting that the crisis is fuelling an ongoing drift towards "authoritarian liberalism."

1. Health, Surveillance and Power in a Computerised Neo-Liberal Age

In February 2020, as the COVID-19 pandemic was in full swing in China, the world watched in amazement Chinese public authorities enforce drastic measures on their population to curb the spread of the epidemic. In parallel with the generalised containment measures implemented in Hubei province, Chinese authorities set up an impressive techno-policing apparatus designed in partnership with the country's major digital platforms such as Alibaba, Tencent and Baidu. "Monitoring [was] already everywhere" noted Chen Weiyu, a twenty-three year-old Shanghai resident. Now, "the epidemic has just made that monitoring, which we don't normally see during ordinary times, more obvious."[6] The surveillance of social media, drones, thermal cameras and so-called "backtracking" applications all formed part of technological spectacle aiming to prove China's resolve and mastery. Although experts doubted their actual effectiveness,[7] China's "hi-tech strategies" were framed as key cog in the authorities' fight against the virus.

Europe would be next in line to be hit by the pandemic. In framing their own response, ruling elites there often made a point of distinguishing itself from their Chinese counterparts. For instance, on 26 March 2020, as the French Minister of the Interior Christophe Castaner was asked about his view on using people's digital traces to help contain the virus, he replied that "this [was] not in the French culture," adding that he placed his "trust in the French so that we do not need to set up these systems which impact

[6] Lily Kuo, "'The New Normal": China's Excessive Coronavirus Public Monitoring Could Be Here to Stay', *The Guardian*, 9 March 2020, sec. World news, https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

[7] Robert Peckham, 'Coronavirus: The Low Tech of the High Tech', *Somatosphere* (blog), 6 March 2020, http://somatosphere.net/forumpost/coronavirus-low-tech-high-tech/.

the individual freedom of everyone."[8] A few days letter, Thierry Breton, the European Commissioner for the Internal Market and former CEO of the high-tech group Atos, similarly explained that China's authoritarian response "was not in our culture".[9]

Such distinction strategies aimed at distancing Europe's supposedly liberal regimes from that of China not only feed into a dangerous cultural relativism that ignores the forms of resistance opposed to state surveillance by Chinese citizens – for instance under the form artistic interventions[10] –, but they also obscure the reality of crisis management in liberal regimes. Indeed, in many European countries too, states' response largely lied in the accentuation of surveillance and social control. Whether we consider the tactics used to model the spread of the epidemic and the movements of the population, to locate individuals or to retrace their social interactions so as to detect new contagions, the differences between the techno-policing practices at play in liberal regimes and in their more illiberal counterparts are arguably much more a difference of degree than of nature.

Such similarity is no accident, but speaks to the fact that, fundamentally, the current pandemic is but a new illustration of the close relationship that has developed throughout history between medical rationality and surveillance practices rooted in the raison d'État. As Alison Howell points out,[11] rather than a recent "securitisation of health" as argued by some constructivist scholars in International Relations, it seems historically and epistemologically more fecund to insist on the "historical symbiosis of both modern warfare and modern medicine".[12] According to Howell, both are imbricated in that they "grew together as means for securing the population," and both wars and epidemics have played a central role in the building of the modern state.

[8] 'Christophe Castaner: le traçage numérique, contraire à la "culture française"', Yahoo News, 27 March 2020, https://fr.news.yahoo.com/christophe-castaner-tra%C3%A7age-num%C3%A9rique-contraire-102732161.html.

[9] 'Thierry Breton : "Aucun pays n'a prévu cette crise, aucun pays n'y était préparé"', France Inter, 2 April 2020, https://www.franceinter.fr/emissions/l-invite-de-8h20-le-grand-entretien/l-invite-de-8h20-le-grand-entretien-02-avril-2020.

[10] Charlotte Gao, 'One Man, One Road: A Funny Tale of Civic Protest in China', The Diplomat, August 2017, https://thediplomat.com/2017/08/one-man-one-road-a-funny-tale-of-civic-protest-in-china/; Lu Mingjun, 'Panorama: Visual Theater and the Politics of Surveillance', ARTLINKART, 2018, http://cloudliste.artlinkart.com/en/article/overview/7cdesxuk; Qianer Liu et al., 'China, Coronavirus and Surveillance: The Messy Reality of Personal Data', 2 April 2020, https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca; Jian Xiao and Shuwen Qu, "'Everybody's Donghu": Artistic Resistance and the Reclaiming of Public Space in China', *Space and Culture*, 6 February 2020.

[11] Alison Howell, 'The Global Politics of Medicine: Beyond Global Health, against Securitisation Theory', *Review of International Studies* 40, n°5 (December 2014): 961–87.

[12] Howell.

1.1. Health crisis and regimes of power

Observing the enforcement of mandatory lock-downs and quarantines that affected much of the world population in 2020,[13] one was of course drawn to the paragraphs that French philosopher Michel Foucault devoted to the 17th century plague epidemics in *Discipline and Punish.*[14] In this book, Foucault contrasted the power strategies experimented to manage plague epidemics to those used earlier against the leper. The latter were marked by the "great Closing," which Foucault tied to the *feudal regime of power*, one based on ostentatious violence and binary divisions. Leprous persons would be banned from civil life and forced to live beyond the city's gate, a form of exclusion aiming at maintaining the community's purity.

Later on, in the fight against the plague epidemics of the late 17th century, Foucault noticed a change in strategy: this time, public authorities chose to enact multiple levels of "spatial partitioning" and surveillance: within the confines of the city, "each individual [was] constantly located, examined and distributed among the living beings, the sick and the dead." According to the philosopher, these new strategies offered an ideal-typical version *disciplinary regime of power* that would take off in the 19th century in connection with the development of industrial capitalism and large state bureaucracies. In the wake of plague epidemics, Western societies saw the expansion, systematisation, and normalisation of new policing measures. For instance, as the plague virus ravaged the city of Marseilles from 1720 on, people who needed to get out of the city had to provide "*bullettes de santé*" – papers that would attest of their healthy condition to the authorities. Meanwhile, as the army enforced a "*cordon sanitaire*" (sanitary cordon) to fence off the Southern part of the kingdom and contain the epidemic, central authorities experimented with identity papers to track mobile populations across the country and detect potential fugitives, beggars, or plagued persons.[15]

In the mid-19th century, public health crises would once again lead to innovations in the government of mass societies, as their management evolved to prefigure a *"securitarian" regime of power*, which Foucault analysed in his 1977-1978 lecture series.[16] At the time, quarantines came to be seen as authoritarian and archaic, and public authorities in liberal-industrial regimes

[13] Alasdair Sandford, 'Coronavirus: Half of Humanity on Lockdown in 90 Countries', Euronews, 2 April 2020, https://www.euronews.com/2020/04/02/coronavirus-in-europe-spain-s-death-toll-hits-10-000-after-record-950-new-deaths-in-24-hou.

[14] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, New York: Vintage, 1995 [1975]).

[15] Vincent Denis and Vincent Milliot. 2004. 'Police et identification dans la France des Lumières'. *Geneses* 54 (1): 4–27.

[16] Michel Foucault, *Security, Territory, Population: Lectures at the Collège de France (1977-1978)*, ed. Arnold I. Davidson, trans. Graham Burchell , Basingstoke: Palgrave Macmillan, 2007).

started moving towards a more fine-grained, individualising and more liberal regulation of population flows, while more coercive measures were maintained along trade routes or in the colonies. As historian Patrice Bourdelais explains:

> "Liberal England established a new protection regime, based on the medical examination of passengers arriving in ships, the hospitalisation of the sick in dedicated hospitals and the follow-up of passengers who appeared to be well for a few weeks. It was at this time that the individual responsibility of the patient who visited public places or public transport was engaged; it could lead to him having to pay a fine or to be imprisoned for a few days."[17]

Since then, as Foucault and others thinkers of the 1970s noted in their respective works on power,[18] securitarian mechanisms have become predominant in a time marked by neo-liberalism and the intensification of mobilities. Contrary to disciplinary *dispositifs*, the space of securitarian power is not closed up but open, and its subjects are not so much the population located in circumscribed environment but fast-moving flows (of people, goods, money, data, etc.). To govern flows and their individual components, a securitarian *dispositif* does not assume that a desired norm can be imposed over well-disciplined subjects obeying the rule. Rather, it aims to manage them according to their natural qualities and their statistical average, which are to be measured in real-time and, when needs be, marginally tinkered with so as to reach the objective at hand. According to Foucault, securitarian *dispositifs* are "at once an analysis of what happens and a program for what should happen" (e.g. let in/out a given item in a flow – "*laisser faire, passer et aller*").[19]

Now, following Foucault – who had remained quite vague on this particular issue –, it is Gilles Deleuze who rightly identified the fundamental role played by new technologies, and in particular computers, in enabling this securitarian regime of power. According to Deleuze:

> Types of machines are easily matched with each type of society – not that machines are determining, but because they

[17]Patrice Bourdelais, 'Le retour des dispositifs de protection anciens dans la gestion politique des épidémies', Extrême-Orient Extrême-Occident, n° 37 (1 September 2014): 241–46, see also: Patrice Bourdelais, *Epidemics Laid Low: A History of What Happened in Rich Countries* (John Hopkins University Press, 2006).

[18]See e.g. Gilles Deleuze, 'Postscript on the Societies of Control', *October* 59 (1992): 3–7; Michel de Certeau, *The Practice of Everyday Life* (University of California Press, 1984).

[19]Foucault, *Security, Territory, Population: Lectures at the Collège de France (1977-1978)*, 40; On securitarian *dispositifs*, see also: Olivier Razac, *Avec Foucault, après Foucault : Disséquer la société de contrôle* (Paris: Editions L'Harmattan, 2008).

> express those social forms capable of generating them and using them. The old societies of sovereignty made use of simple machines –levers, pulleys, clocks; but the recent disciplinary societies equipped themselves with machines involving energy, with the passive danger of entropy and the active danger of sabotage; the societies of control operate with machines of a third type, computers (...). The conception of a control mechanism, giving the position of any element within an open environment at any given instant (whether animal in a reserve or human in a corporation, as with an electronic collar), is not necessarily one of science fiction.[20]

1.2. When a virus gone global meets ubiquitous digital surveillance

As Deleuze noted, computer technologies have supported the spread of securitarian dispositifs for the past half-century. In that regard, what has been remarkable in the response to the COVID-19 pandemic is not so much the strong resurgence of containment tactics, the closing of borders and the restrictions of flows. After all, as Foucault writes, different logics – sovereign, disciplinary, securitarian – always co-exist at any given time,[21] and it is to be expected that, when exposed to such an exceptional event, the state would tactically restrict flows and bring disciplinary logics to the fore.[22]

Rather, what is striking is how state actors were able to leverage the pervasive digital infrastructure of "liquid surveillance"[23] to enact both the enclosing but distributed tactics of containment as well as the securitarian management of flows. For instance, we have already mentioned how new digital technologies like smartphone apps were used in Poland to enforce confinement orders, enabling a low-cost and distributed panopticon. Computers have also been central to the security approach aimed at regulating

[20] Deleuze, 'Postscript on the Societies of Control'.

[21] "What above all changes is the dominant characteristic, or more exactly, the system of correlation between juridico-legal mechanisms, disciplinary mechanisms, and mechanisms of security (...). A technology of security, for example, will be set up, taking up again and sometimes even multiplying juridical and disciplinary elements and redeploying them within its specific tactic." Foucault, *Security, Territory, Population: Lectures at the Collège de France (1977-1978)*, 8.

[22] As Didier Bigo writes (commenting on Foucault): "When the state declares a state of exception or emergency, it is not the enactment of a security claim or practice, but its end." For, as he points out, securitarian governmentality presupposes freedom of movement, and in that respect mandatory lock-downs and confinements reflect the inherent fragility of a securitarian order, always exposed to contingency. Bigo, Didier, 'Security: A Field Left Fallow'. In *Foucault on Politics, Security and War*, edited by Michael Dillon and Andrew W. Neal, (London: Palgrave Macmillan UK, 2008), 107.

[23] Bauman, Zygmunt, and David Lyon, *Liquid Surveillance: A Conversation*, (Malden, MA: Polity Press, 2013).

flows: at the state's borders or within cities, they have been used to monitor the population on the move in order to detect deviations from the norm, for instance by measuring body heat or spatial proximity between individuals.

As the next section will make clear, the reliance on digital surveillance not only fuelled disciplinary and securitarian power strategies. It also provided state actors with the ability to enforce drastic restrictions on the population while minimising their political and economic costs. Not unlike other epidemics throughout history, the fast-rising tide of surveillance and control unleashed by the COVID-19 pandemic has largely be leigitimised by securitisation discourses and warfare analogies. French president Emmanuel Macron for instance talked repeatedly about being "at war against the virus" in his address of 16 March 2020, when he announced the first national lock-down.[24] Surely it was a tactical move, aimed at instigating fear and garnering support – or at least a resigned acceptance – for the extremely severe restrictions to the freedoms of movement and assembly he announced that night. But precisely, the war analogy also served to legitimise war-like practices. It marked the opening of yet another crisis, one that would lead to profound disruptions of social life.

In many countries, years of austerity policies had come to undermine the ability of national health systems to cope with such a surge in hospital patients. However, political and administrative elites had to manage this exceptional event while showcasing concern for the life of the majority, due to the supreme value attached to the preservation of life – or what Didier Fassin has termed *biolegitimacy*.[25] That and the lingering uncertainties about the disease left them with few options but engaging in an all-out show of coercive strength – or, in the language of Michael Mann, of *despotic powers*.[26] Except for a range of "essential workers," strict containment was thus enforced. "Regardless of the costs" once again became a leading motto, as actors across the administrative field – and especially those attached to what Pierre Bourdieu called the "right hand of the state"[27]–, were called upon to keep the economy afloat and the population in check.

Of course, at that stage, public officials could equate lock-downs with a kind of pastoral protection, downplaying both their long-term health im-

[24]Emmanuel Macron, Adresse Aux Français du Président de la République Emmanuel Macron', *Élysée*, 16 March 2020, https://www.elysee.fr/emmanuel-macron/2020/03/16/adresse-aux-francais-covid19.

[25]Fassin, Didier, 'Another Politics of Life Is Possible', *Theory, Culture & Society* 26 (5): 44–60.

[26]For a discussion of Mann's concepts, see Tarrow, Sidney, 'Mann, War, and Cyberspace: Dualities of Infrastructural Power in America', *Theory and Society* 47 (1): 61–85 (2018).

[27]See the work of Loïc Wacquant, which "fills in a gap in Bourdieu's model by inserting the police, the courts, and the prison as core constituents of the 'Right hand' of the state, alongside the ministries of the economy and the budget." Wacquant, Loïc, 'Bourdieu, Foucault, and the Penal State in the Neoliberal Era', In *Foucault and Neoliberalism*, edited by Daniel Zamora and Michael C. Behrant, (Malden, MA: Polity Press, 2016), 116.

pacts (e.g. on mental health) as well as their likely normalising effects (e.g. people's acceptance of an increasingly digitally-mediated and monitored interactions, the emptying and increased policing of public spaces, etc.). Drones and other forms of digital surveillance were used in that context. But after an initial phase where state actors primarily relied on forms of despotic powers to manage the crisis, they quickly moved to tap into the vast resources afforded by collaborative non-state actors to keep the economy running, manage medical resources and nudge the population. Next to medical supplies or supply chains managed by private actors, the digital sector also represented a key asset of what Mann called *infrastructural power*, providing state actors with "ideologically sustained" "soft tools" to reach their goals through "diffuse and non-coercive" means.[28]

"Backtracking applications" installed on people's smartphone to automate and scale-up the kind of contact-tracing traditionally carried out by health professionals or volunteers so as to identify chains of contamination provide a good illustration of the impact of the health crisis on infrastructural surveillance power. As we will see, their promoters within state administrations could benefit from the proactive collaboration of various non-state actors keen on helping develop these tools, while relying on the growing acculturation to self-tracking among the population to boast a "voluntary" approach that they hope would normalise people's conduct. By encouraging individuals to adopt the "right behaviours" through programmed suggestions embedded in these apps' interfaces, this form of distributed and automated contact-tracing is fully in line with behaviourist "nudge" theories advocated by thinkers like Richard Thaler and Cass Sunstein[29] – a new neoliberal "art of governing" which multinationals like Google have been experimenting and pioneering through the digital architectures they design.[30]

Beyond infrastructural power and the ability of state actors to leverage their connection with non-state actors to govern the population, backtracking applications also illustrate the extent to which digital surveillance is in fact co-constitutive of our neo-liberal modernity, reflecting and reinforcing some of its core tenets. First is the emphasis on the "reponsabilised subject": since they are spread throughout the population, computer devices can be used to "augment" and discipline individuals, making them more "responsible," "autonomous" and adaptable in the face of health hazards. Secondly, digital technologies are enmeshed with both bureaucratic rationalisation and fiscal austerity: through a qualitative leap in automation, computers hold the promise of multiplying and "scaling up" the surveil-

[28]Tarrow, 'Mann, War, and Cyberspace'.

[29]Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness* (Penguin UK, 2012).

[30]Vlad Savov, 'Google's Selfish Ledger Is an Unsettling Vision of Silicon Valley Social Engineering', *The Verge*, 17 May 2018, https://www.theverge.com/2018/5/17/17344250/google-x-selfish-ledger-video-data-privacy.

lance activities of bureaucratic organisations – e.g. health authorities or law enforcement agencies – while keeping costs at an acceptable level.

2. "Never Waste a Crisis": Amplifying Surveillance

As it should be clear by now, and despite their extraordinary intensity, the surveillance practices central to the management of the COVID-19 pandemic are not so much a prefiguration of a new regime of power as an amplification of pre-existing logics. As Sara Angeli Aguiton, Lydie Cabane and Lise Cornilleau warn, we should be cautious of the now banal critique of the "state of exception" which tends to consider crises as "laboratories for brutal political reforms."[31] According to the authors, "while these approaches have the advantage of drawing attention to the instrumentation (and instrumentalisation) of crises in order to carry out reforms in a context of shock and exceptional measures, they tend to recycle the discourse of institutions that often claim the image of a laboratory to frame their intervention."

The rhetoric of exception and the semantic field attached to the "war on the virus" has paradoxically normalised routines that were already in the making. It has contributed to instituting and trivialising an "already there" that hitherto remained marginal and contentious. This health crisis is therefore not so much a laboratory for innovation as a revealer and a sounding board, where the actors involved amplify and recompose existing practices through various forms of "tinkering." In this respect, the current pandemic is reminiscent of other recent crises, particularly the anti-terrorist crises that have occurred since 11 September 2001. It entrenches what Linda Weiss has called a "governed interdependence" between state actors and non-state actors – chiefly corporations –,[32] expanding the former's infrastructural reach and capabilities while furthering the business goals of the latter, thereby offering a new illustration of the elusiveness of the "limits of the state."[33] In this section, I survey some key trends in digital state surveillance that the COVID-19 pandemic has amplified.

[31]Sara Angeli Aguiton, Lydie Cabane, and Lise Cornilleau, 'Politiques de la « mise en crise »', *Critique internationale* n°4 (1 December 2019): 9–21.

[32]Weiss, Linda, *America Inc.?: Innovation and Enterprise in the National Security State*. Ithaca, (NY: Cornell University Press, 2014). See also Tarrow, "Mann, war, and cyberspace".

[33]Timothy Mitchell, 'The Limits of the State: Beyond Statist Approaches and Their Critics', *The American Political Science Review* 85, n°1 (March 1991): 77.

2.1. Fostering public-private assemblages focused on surveillance

First, the COVID-19 pandemic is leading to a fast-paced consolidation of the ties forged between public and private professionals from the security, health and, crucially, high tech fields.[34] At the beginning of the crisis, it first seemed like European's legacy telecom companies would make the most of their proximity with political and administrative elite to take advantage from the pandemic. Mid-March 2020, in Italy, telecom operators like Vodafone partnered with the Lombardy region to announce that they had analysed the population's geolocation data on a three-week period starting on 21 February. By isolating the cohort of cellphones whose movements were limited to five hundred meters around the place of residence, they estimated that only 60 per cent of the population had respected lock-down orders. Telecom operators in other European countries followed suit and, at the end of March, EU Commissioner Thierry Breton announced a partnership between the European Commission and the major European operators to generalise these aggregate analysis of the population's movements.[35]

But despite Europe's attempt to promote its home-grown and legacy "digital champions," US tech companies have often reaped the most out of these new public-private partnerships. Their unrivalled market dominance on different sectors of the digital economy make them inescapable partners. As Big Tech's technical, economic and organisational forms of capital gain the upper hand across the administrative field under the new paradigm of "data governance,"[36] and as new cross-socialisation spaces are being created with administrative elites, these companies have been able to use the crisis as an opportunity for legitimising their privacy-invasive economic models while forging new partnerships with health authorities – for instance to optimise the resource allocation of medical supplies, strained by dint of budget cuts.

A good example is the announcement made on 28 March 2020 by the British National Health Service (NHS) of a new, Big-Data powered dashboard. As the NHS explained at the time, "in this time of crisis, we need the private sector to play its part to tackle these unprecedented challenges. We have therefore enlisted the help of some of the most cutting edge and experienced firms from across Britain's technology sector."[37] NHS contracted

[34]Stephen L. Roberts, 'Big Data, Algorithmic Governmentality and the Regulation of Pandemic Risk', *European Journal of Risk Regulation* 10, n°1 (March 2019): 94–115; Félix Tréguer, 'Seeing Like Big Tech: Security Assemblages, Technology, and the Future of State Bureaucracy', in *Data Politics: Worlds, Subjects, Rights*, ed. Didier Bigo, Engin Isin, and Evelyn Ruppert, Routledge Studies in International Political Sociology (London: Routledge, 2019):144–65.

[35]Samuel Stolton, 'EU's Breton Defends COVID-19 Telecoms Data Acquisition Plans', *Wractiv.C*26 March 2020, https://www.euractiv.com/section/data-protection/news/eus-breton-defends-covid-19-telecoms-data-acquisition-plans/.

[36]Tréguer, 'Seeing Like Big Tech'.

[37]National Health Service, 'The Power of Data in a Pandemic - Tech-

a consortium comprised of tech multinationals like Google, Amazon, Microsoft or Palantir – a controversial Big Data analytics firm co-founded by venture-capitalist and Donald Trump supporter Peter Thiel.[38] In the US, a similar project involving Palantir was also established by the Federal Emergency Management Agency (FEMA).[39] As for the Australian government, it partnered with Amazon to host data tied to its controversial backtracking application.[40]

In France, the task force charged by the government with developing the "StopCovid" backtracking application included people from public agencies – such as the French Institute for Research in Computer Science and Automation (known by its French acronym INRIA), the National Agency for the Security of Information Systems (ANSSI) and the National Institute for Health and Medical Research (INSERM) – as well as companies like the global consultancy Capgemini, defence contractors like Thales and Dassault Systèmes, the telecommunications operator Orange but also smaller start-ups from the "Internet of Things" sector.[41] Ironically, the government claimed that this project would not rely on the backtracking features rolled-out by Apple and Google through the iOS and Android platforms, framing it as a commitment to "digital sovereignty"[42] – a term that as been central to the French and European debate on digital policy since at least 2013 and the disclosures of NSA whistle-blower Edward Snowden.[43] Still, Orange was eventually mandated by the government to negotiate with Apple and technical tweak to its iOS so as to improve the reliability of the StopCovid application.[44] And when the application was launched on 2 June 2020, it

nology in the NHS', 28 March 2020, https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/.

[38]Downey, Andrea, 'Private Data Contracts Risk "Undermining Core Values of NHS"', *Digital Health*, 25 November 2020. *https://www.digitalhealth.net/2020/11/data-contracts-with-palantir-risk-undermining-core-values-of-nhs/*.

[39]Spencer Ackerman, 'FEMA Tells States to Hand Public Health Data Over to Palantir', *The Daily Beast*, 21 May 2020, sec. politics, https://www.thedailybeast.com/fema-tells-states-to-hand-public-health-data-over-to-palantir.

[40]Linton Besser and Dylan Welch, 'Australians' Data from COVID-19 Tracing App to Be Held by US Cloud Giant Amazon', ABC News, 23 April 2020, https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682.

[41]Elsa Bembaron, 'Mobilisation générale pour développer l'application StopCovid', Le Figaro.fr, 26 April 2020, https://www.lefigaro.fr/secteur/high-tech/mobilisation-generale-pour-developper-l-application-stopcovid-20200426.

[42]Julien Cadot, 'StopCovid : Apple refuse de céder à la France, Cédric O feint l'étonnement', Numerama, 5 May 2020, https://www.numerama.com/tech/622279-stopcovid-apple-refuse-de-ceder-a-la-france-cedric-o-feint-letonnement.html.

[43]Félix Tréguer, 'From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France', 2016, https://halshs.archives-ouvertes.fr/halshs-01306332/document; Martin Untersinger, 'L'incertaine mais nécessaire « souveraineté numérique »', *Le Monde.fr*, 20 November 2019, https://www.lemonde.fr/idees/article/2019/11/20/l-incertaine-mais-necessaire-souverainete-numerique_6019810_3232.html.

[44]Elsa Bembaron, 'StopCovid: Orange en charge des discussions avec Ap-

used Google's captcha code to authenticate users, thereby sending the IP address of StopCovid users to Google's servers. Meanwhile, the COVID-19 crisis was also giving the French government new-found justifications to speed-up the roll-out of a controversial project called "Health Data Hub." The project will centralise health data collected through various actors of the "social security" system on Microsoft's servers.[45]

After years of new partnerships between law enforcement and large online platforms to bolster the surveillance of the online public sphere and take down litigious content – in particular content deemed to promote or glorify acts of terrorism or also so-called "fake news" –, companies like Facebook, Google or Twitter quickly responded to government calls to take down misleading information on the epidemic. All the more in a context of health emergency, the adverse impact of such extralegal censorship for freedom of expression seemed to go unnoticed. In France, after a meeting held on 28 February, government officials and representatives of Facebook, Google, Microsoft or Tik Tok announced new collaborations to fight disinformation related to the new coronavirus and instead promote official sources.[46] A few days later, on 3 March, Facebook's CEO Mark Zuckerberg published a statement in which he summed up his company's approach on the issue:

> We're also focused on stopping hoaxes and harmful misinformation. It's important that everyone has a place to share their experiences and talk about the outbreak, but as our community standards make clear, it's not okay to share something that puts people in danger. So we're removing false claims and conspiracy theories that have been flagged by leading global health organisations. We're also blocking people from running ads that try to exploit the situation (...).[47]

Google's Sundar Pichai followed suit on 6 March.[48] "On YouTube," Pichai explained, "we are working to quickly – and often automatically[49]

ple', Le Figaro.fr, 30 April 2020, https://www.lefigaro.fr/secteur/high-tech/stopcovid-orange-en-charge-des-discussions-avec-apple-20200430.

[45]Jérôme Hourdeaux, 'Le Health Data Hub attaqué devant le Conseil d'Etat', Mediapart, 9 June 2020, https://framatalk.org/dysmachinehttps://www.mediapart.fr/journal/france/090620/le-health-data-hub-attaque-devant-le-conseil-d-etat.

[46]Le Point AFP, 'Coronavirus: gouvernement et réseaux sociaux se préparent aux fausses nouvelles', Le Point, 28 February 2020, https://www.lepoint.fr/politique/coronavirus-gouvernement-et-reseaux-sociaux-se-preparent-aux-fausses-nouvelles-28-02-2020-2364966_20.php.

[47]Mark Zuckerberg, 'Update on the steps we're taking to respond to the coronavirus', Facebook, 3 March 2020, https://www.facebook.com/zuck/posts/10111615249124441.

[48]Sundar Pichai, 'Coronavirus: How We're Helping', Google, 6 March 2020, https://blog.google/inside-google/company-announcements/coronavirus-covid19-response/.

[49]Casey Newton, 'The Coronavirus Is Forcing Tech Giants to Make a Risky Bet on AI', *The Verge*, 18 March 2020, https://www.theverge.com/interface/2020/3/18/21183549/coronavirus-content-moderators-facebook-google-twitter.

– remove any content that claims to prevent the coronavirus in place of seeking medical treatment." In the US, a meeting between tech companies and government officials took place at the White House on 11 March.[50] In a similar fashion, the British NHS worked with Twitter, Facebook and Instagram to authenticate the social media accounts of nearly eight hundred healthcare organisations.[51]

Besides misinformation, at the core of these discussions was also the issue of using these companies' vast troves of data in the fight against the coronavirus. On that front, after months of heated debates on both sides of the Atlantic regarding the economic dominance of these multinationals and the privacy impact of their business models, calls for cooperation came from unexpected corners. In Italy for instance, a group of journalists published an open letter in the left-wing daily newspaper *Il Manifesto*, urging Big Tech to collaborate with the authorities: "Large service providers like Google, Facebook, Amazon or Twitter know a lot, if not all, of our social relations, the whereabouts, the state of mind and the physical condition of tens of millions of Italians," they wrote.[52] According to the journalists, "only the databases of these profiling giants" could provide the information necessary "to wage this war," to "delimit the zones of transmission" and "identify the most dangerous groups" at risk of spreading the epidemic.

US tech companies reacted to these calls with caution – probably out of fear of unleashing a new round of privacy concerns – and only aggregate statistics were released. By analysing the browsing history of the billion users of its mapping platform, Google was able to estimate the evolution of attendance of certain types of areas or facilities, for example cafes or restaurants, in nearly 130 countries.[53] But all of a sudden, their toxic business-models based on the large-scale collection of people's digital traces for the purpose of selling targeted advertising – what John Bellamy Foster and others have called "surveillance capitalism"[54] – seemed retrospectively

[50]Tony Romm, 'White House Asks Silicon Valley for Help to Combat Coronavirus, Track Its Spread and Stop Misinformation', *Washington Post*, 3 November 2020, https://www.washingtonpost.com/technology/2020/03/11/white-house-tech-meeting-coronavirus/.

[51]Alex Hern and Dan Sabbagh, 'NHS Announces Plan to Combat Coronavirus Fake News', *The Guardian*, 10 March 2020, sec. World news, https://www.theguardian.com/world/2020/mar/10/nhs-plan-combat-coronavirus-fake-news.

[52]Michele Mezza et al., 'Facciamoci dare i dati della rete', *Il Manifesto*, 24 March 2020, sec. Editoriale, https://ilmanifesto.it/facciamoci-dare-i-dati-della-rete/.

[53]Sarah Elzas, 'Google Publishes Location Data for Governments to See Effect of Covid-19 Confinement Measures', RFI, 3 April 2020, https://www.rfi.fr/en/science-and-technology/20200403-google-publishes-location-data-for-governments-to-see-effect-of-covid-19-confinement-measures.

[54]John Bellamy Foster and Robert W. McChesney, 'Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age', *Monthly Review* 66, n°3 (July 2014), http://monthlyreview.org/2014/07/01/surveillance-capitalism; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 1 edition (New York: PublicAffairs, 2019).

legitimised.

2.2. A shift in legitimation discourse

These initiatives signalled Big Tech's readiness to frame itself as a public utility. In the United States, Eric Schmidt, former CEO of Google and who still holds more than $5.3 billion worth of shares in Google's parent company Alphabet,[55] has been at the forefront of this broader push. As a representative of the tech industry in Washington, and as chair of both the Pentagon's Defense Innovation Advisory Board and of the National Security Commission on Artificial Intelligence, Schmidt made many public interventions in which he was adamant about the importance of digital technologies in the midst of the health crisis. He essentially argued that instead of the critical scrutiny Big Tech had received in recent months and years, it actually deserved some praise. According to him, "the benefit of these corporations, which we love to malign, in terms of the ability to communicate, the ability to deal with health, the ability to get information, is profound. Think about what your life would be like in America without Amazon."[56] For this, he said, we all should "be a little bit grateful that these companies got the capital, did the investment, built the tools that we're using now, and have really helped us out."

Through such statements, Schmidt's goal was not only to re-legitimise Big Tech, but also to stress that their infrastructures had proved crucial in absorbing the shock of the pandemic, for instance by providing telework solutions to confined workers across the world.[57] His subtext was that Big Tech's mightiness should not to be viewed as problem, but instead duly appreciated given how much it helped everyone cope with the crisis, including the public officials in charge of managing it. In sum, the health crisis had provided a new illustration of the fact that large technology companies form a core component of the state's infrastructural power – one to be reinforced rather than dismantled through the kind of legislative reforms contemplated

[55] Kate Conger and Cade Metz, "'I Could Solve Most of Your Problems": Eric Schmidt's Pentagon Offensive', *The New York Times*, 2 May 2020, sec. Technology, https://archive.vn/xhMAQ, https://www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html.

[56] *The Technological Response to COVID-19*, The Economic Club of New York, 2020, https://www.youtube.com/watch?v=XtAyGVuRQME.

[57] Jason Aten, '5 Big Tech Companies Making Remote-Work Tools Free during the Coronavirus Outbreak, Including Google and Microsoft', *Business Insider*, 10 March 2020. *https://www.businessinsider.com/tech-companies-making-remote-work-tools-free-during-coronavirus-outbreak-2020-3*; on telework and surveillance in the wake of the pandemic, see also Ivan Manokha, 'Covid-19: Teleworking, Surveillance and 24/7 Work. Some Reflexions on the Expected Growth of Remote Work After the Pandemic', *Political Anthropological Research on International Social Sciences (PARISS)* 1 (2) (December 2020): 273–87.

by the U.S. Congress.[58] But as an experienced tactician, Schmidt also understood he take advantage of the crisis to play offence. In Op-Ed published in the Wall Street Journal in late March 2020, he not only celebrated the "entrepreneurial, results-driven ethos of today's tech sector" but also asked Americans to think hard about "how could the emerging technologies being deployed in the current crisis propel us into a better future."[59] Of course, he had his own ideas: "If we are to build a future economy and education system based on tele-everything, we need a fully connected population and ultrafast infrastructure. The government must make a massive investment—perhaps as part of a stimulus package—to convert the nation's digital infrastructure to cloud-based platforms and link them with a 5G network."

Now the "tele-everything society" promoted by Eric Schmidt and others is highly profitable for the tech sector. As a matter of fact, social distancing has been a boon for Big Tech. As the global economy faced a huge recession and as financial market contracted, the stocks of Apple, Amazon, Alphabet, Microsoft and Facebook rose by thirty-seven per cent during the first seven months of 2020. Their combined stocks now represent about twenty per cent of the US stock market's total worth, a level that is unrivalled for a single industry in at least seventy years.[60] On 1 September 2020, Apple's stock market value passed the two trillion dollars mark, or roughly the double of what is was before the pandemic began.

According to Naomi Klein, the Canadian journalist and writer, what these public-private initiatives suggest is that "something resembling a coherent Pandemic Shock Doctrine is beginning to emerge."[61] She sums up the essence of what she calls a "Screen New Deal" in this way: "Far more high-tech than anything we have seen during previous disasters, the future that is being rushed into being as the bodies still pile up treats our past weeks of physical isolation not as a painful necessity to save lives, but as a living laboratory for a permanent – and highly profitable – no-touch future." With health quickly becoming an ultimate motive for policy makers, and with record-setting stimulus packages underway, the hope is also to see an avalanche of public money supporting home-grown tech firms to help

[58]See, e.g., Kang, Cecilia, and David McCabe, 'House Lawmakers Condemn Big Tech's "Monopoly Power" and Urge Their Breakups', *The New York Times*, 6 October 2020, sec. Technology. f*https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html*.

[59]Eric Schmidt, 'A Real Digital Infrastructure at Last', *Wall Street Journal*, 27 March 2020, sec. Life, https://www.wsj.com/articles/a-real-digital-infrastructure-at-last-11585313825.

[60]Peter Eavis and Steve Lohr, 'Big Tech's Domination of Business Reaches New Heights', *The New York Times*, 19 August 2020, sec. Technology, https://www.nytimes.com/2020/08/19/technology/big-tech-business-domination.html.

[61]Naomi Klein, 'Screen New Deal: Under Cover of Mass Death, Andrew Cuomo Calls in the Billionaires to Build a High-Tech Dystopia', *The Intercept* (blog), 8 May 2020, https://theintercept.com/2020/05/08/andrew-cuomo-eric-schmidt-coronavirus-tech-shock-doctrine/.

them overcome their global competitors.

As Klein notes, before the crisis Schmidt was already vocal about the need for large-scale investment in the technology sector, in particular artificial intelligence and quantum computing. And just like Russia in the 1960s or Japan in the 1980s, the ultimate call of alarm is that the US technological dominance is being threatened by China. This "techno-nationalist" vibe – somewhat toned down during the first phase of the pandemic – was evident in another Op-Ed published by Schmidt in a February 2020 issue of the New York Times. The piece's title warned that "Silicon Valley could lose to China," conveying that simple message: "We can't win the technology wars without the federal government's help."[62]

But Big Tech is not alone in taking advantage of the health crisis to promote its business interests. Smaller start-ups too are riding the wave. Such is the case of Small and Medium-sized Enterprises (SMEs) operating in the gigantic market of personal data, many of which also seized the occasion to advertise their population tracking capabilities. A case in point is the French startup Geo4Cast. Its business model is based on trading geolocation data collected through the myriad of smartphone applications embedding its software packages, which provide third-party developers with targeted advertising features.[63] In early April, Geo4Cast published maps showing aggregate data about population movements between 26 March and 2 April. During a whole weekend, its CEO Antoine Couret intervened in the media while headlines pointed at the "relaxation" of the French in respecting blanket confinement.

Indirectly, many of these crisis discourses and measurements helped instill the idea of irresponsible "black sheep" among the population, who jeopardised the collective effort at slowing the epidemic. In doing so, they comforted the framing pushed by state officials who mobilised the semantic field of war in order to normalise recent trends in law enforcement tactics. After only five weeks of near-total lock-down, the French police had carried 15,5 million checks and issued close to a million fines for violating the restrictions – out of a population of 66 million residents .[64]

This massive deployment, punctuated by numerous cases of police violence, was accompanied the use of new surveillance technologies like drones. Until the pandemic, these remotely piloted aircraft, often equipped with

[62]Eric Schmidt, 'Eric Schmidt: I Used to Run Google. Silicon Valley Could Lose to China.', *The New York Times*, 27 February 2020, sec. Opinion, https://www.nytimes.com/2020/02/27/opinion/eric-schmidt-ai-china.html.

[63]Olivier Tesquet, 'Post-scriptum sur le déconfinement : demain, tous auxiliaires de police ?', Télérama, 9 April 2020, https://www.telerama.fr/medias/post-scriptum-sur-le-deconfinement-demain,-tous-auxiliaires-de-police,n6625533.php.

[64]Anonymous, 'Confinement : "915 000 PV, 15,5 millions de contrôles" annonce Christophe Castaner', ladepeche.fr, 23 April 2020, https://www.ladepeche.fr/2020/04/23/confinement-915-000-pv-155-millions-de-controles-annonce-christophe-castaner,8859044.php.

cameras or loudspeakers, were used very sparingly, mainly to monitor protests. Like other countries, the French police took advantage of the crisis to generalise their use despite the lack of any detailed legal framework to regulate their use. It rented these devices from private companies to broadcast preventive messages or monitor streets and natural areas to as to identify people in breach of lock-down orders and help ground patrols apprehend them. In mid-April, the ministry of the Interior published a call for tender to equip its police forces with more than 600 drones capable of flying high enough so as to be almost invisible, and embarking powerful cameras and data transmission capabilities.[65] Parts of that four million budget come from a program of the European Union, the Internal Security Fund (ISF), dedicated to "law enforcement cooperation" and "the management of the Union's external borders."[66]

Other technologies of urban policing are also gaining new momentum with the health crisis, such as so-called "smart video-surveillance." These systems, which use algorithms that are trained through "machine learning" techniques to automatically detect certain events in video-surveillance streams, are now being promoted by their designers for their ability to enforce "social distancing." In France, in the midst of the crisis, a start-up called Two-I – one of the country's leading actors in this fast-developing market – launched a promotional video and offered free trials for law enforcement agencies willing to test its video analytics services. Two-I algorithms can parse in real-time the huge data flows coming from video-surveillance cameras to detect "abnormal events." "Our technology is capable of detecting gatherings, which then enables the police to implement prevention measures," explained Two-I's co-founder Guillaume Cazenave.[67]

Facial recognition is of course one of the leading applications of automated video-surveillance. And here again, the health crisis is helping legitimise its growing use. At the beginning of the epidemic, the French Secretary of State for Digital Technology, Cédric O, stated that "facial recognition could bring a certain number of benefits, both in terms of public order and disease management."[68] In Moscow, the authorities mobilised their recently-

[65]Fabien Leboucq, 'Pourquoi le ministère de l'Intérieur vient-il de commander des drones ?', Libération.fr, 15 April 2020, https://www.liberation.fr/checknews/2020/04/15/pourquoi-le-ministere-de-l-interieur-vient-il-de-commander-des-drones_1785166.

[66]European Commission, 'Internal Security Fund - Police', Text, Migration and Home Affairs - European Commission, 6 December 2016, https://ec.europa.eu/home-affairs/financing/fundings/security-and-safeguarding-liberties/internal-security-fund-police_en.

[67]Anonymous, 'Coronavirus : Two-i met sa technologie à disposition des acteurs étatiques', Le Journal des Entreprises, Le Journal des Entreprises, 25 March 2020, https://www.lejournaldesentreprises.com/lorraine/breve/coronavirus-two-i-met-sa-technologie-disposition-des-acteurs-etatiques-489722.

[68]'Cédric O estime que la reconnaissance faciale peut avoir des « bénéfices» dans la «gestion de maladies »', Libération.fr, 12 March 2020, https://www.liberation.fr/direct/element/reconnaissance-faciale-la-bonne-idee-du-gouvernement-contre-le-coronavirus_110386/.

installed facial recognition system – plugged to about a hundred thousand CCTV cameras across the city – to detect people in breach of their quarantine orders.[69] As for the U.S. Customs and Border Protection, their representatives touted facial recognition technology as "touch-free" and therefore a more "hygienic way to validate your identity" than traditional passports during airport check-ins.[70] In the coming months and years, we can expect the proliferation of biometric surveillance to be fuelled by health concerns.

2.3. Health emergency and rule by law

Unsurprisingly, like other crises, the "war on the virus" has also accelerated the circumvention of the rule of law, either because new surveillance programs are rolled-out in the absence of any appropriate legal framework or because "exceptional" norms are adopted under the guise of a "state of health emergency."[71] Israel provides a good illustration of this later case. As early as March 14th, Israeli Prime Minister Benyamin Netanyahu authorised the Shin Bet, the domestic intelligence service, to use a hitherto clandestine tool for fighting suicide attacks in order to counter the epidemic. "Up until now," Netanyahu explained, "I have avoided using these measures against the civilian population, but we no longer have a choice."[72] NSO Group – an Israeli company specialising in cyber espionage and involved in several surveillance scandals against human rights activists and journalists[73] – is providing this new monitoring tool capable of analysing cellphone metadata and communication content siphoned off telecom networks. By cross-referencing all of this data, NSO is able to assign each user a "contagiousness score" ranging from 1 to 10. "The system would be updated in real time" wrote Israeli Defence Minister Naftali Bennett in an official document detailing the scheme.[74] "It could be that yesterday, my 'grade'

[69]Sam Ball, '100,000 Cameras: Moscow Uses Facial Recognition to Enforce Quarantine', France 24, 24 March 2020, https://www.france24.com/en/20200324-100-000-cameras-moscow-uses-facial-recognition-to-enforce-quarantine.

[70]Diane J. Sabatino, 'Facial Recognition is a touch-free, hygienic way to validate your identity, as well as protect from exposure to COVID-19 and other germs at the airport.', Twitter, 14 March 2020, https://twitter.com/OFODEAC/status/1238866399524724736.

[71]Fionnuala Ní Aoláin, 'The Contemporary Exercise of Emergency Powers: Reflections on Permanence, Impermanence and Challenging Times', *Political Anthropological Research on International Social Sciences (PARISS)* 1 (2) (December 2020): 197–215.

[72]Guillaume Gendron, 'Coronavirus : en Israël, l'antiterrorisme pour détecter les malades', Libération.fr, 3 April 2020, https://www.liberation.fr/planete/2020/04/03/en-israel-l-antiterrorisme-pour-detecter-les-malades_1784172.

[73]Nick Hopkins and Stephanie Kirchgaessner, 'WhatsApp Sues Israeli Firm, Accusing It of Hacking Activists' Phones', *The Guardian*, 29 October 2019, sec. Technology, https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-accusing-it-of-hacking-activists-phones.

[74]Refaella Goichman, 'Israeli Defense Ministry Teaming Up With Spyware Firm NSO to Fight Coronavirus', *Haaretz*, 29 March 2020, https://www.haaretz.com/israel-news/.premium-israeli-defense-chief-plans-to-employ-spyware-firm-nso-in-fight-against-coronavirus-1.

was 5.6, but now it has jumped to 9, because I visited a grocery store that two other carriers had visited in recent days," he explained. A dozen other countries have reportedly tested the system.[75]

From this point of view, the epidemic offers a new illustration of the shift from the rule *of* law to the rule *by* law, that is the strengthening of the state's executive powers through legal norms.[76] The rhetoric of the health crisis does not necessarily undermine the formal prerogatives of oversight bodies in charge of keeping state surveillance in check – such as the courts or personal data protection authorities – but it aggravates their structural weakness vis-à-vis the executive branch. Legal safeguards do not disappear altogether, but the crisis gives way to laxer interpretations of the law. The legal constraints weighing on state intervention are thus often pushed back, offering new leeway to the hypertrophy of surveillance and other practices of social control. Strictly speaking, as Didier Bigo points out in a commentary on Gorgio Agamben's theses, the crisis does not so much lead to a total "state of exception" as it extends the contradictions at the heart of the liberal state between state power and human rights – contradictions that are inscribed in state rationalities and practices and whose "logic is internal to liberalism but controlled by liberalism, in short that [are] 'contained' by liberalism in the double sense of the word."[77]

In the field of surveillance, Israel here again provides a case in point. In the Spring of 2020, the Supreme Court eventually issued a ruling against the government's plan to expand its antiterrorist surveillance program to the whole population. But the court essentially asked the government to back up the program with a detailed legal framework and bring special protections to journalists.[78] Soon enough, a new legislative provision was passed by the Knesset to address these procedural requirements.[79] Like in

8722464.

[75]Rory Cellan-Jones, 'Israeli Spyware Firm Pitches to Be Covid-19 Saviour', *BBC News*, 2 April 2020, sec. Technology, https://www.bbc.com/news/health-52134452.

[76]Sidney Tarrow, *War, States, and Contention: A Comparative Historical Study*, 1 edition (Ithaca ; London: Cornell University Press, 2015), 165–66.

[77]Didier Bigo, 'Exception et Ban : À Propos de l'« État d'exception »', *Erytheis, Revue Éléctronique d'études En Sciences de l'homme et de La Société*, n°2 (November 2007): 115–45.

[78]Noa Landau and Netael Bandel, 'Israel Secretly Sought to Expand Shin Bet Tracking of Coronavirus Patients before Court Ruling', Haaretz.com, 26 April 2020, https://www.haaretz.com/israel-news/.premium-israel-secretly-sought-to-expand-tracking-of-coronavirus-patients-before-ruling-1.8801167.

[79]Anonymous, 'Israel Allows Shin Bet to Continue Using Tracking App for Virus Carriers', Middle East Monitor, 5 May 2020, https://www.middleeastmonitor.com/20200505-israel-allows-shin-bet-to-continue-using-tracking-app-for-virus-carriers/;
Anonymous, 'Israel Approves Mobile Phone Tracking of COVID-19 Carriers for Rest of Year', Middle East Monitor, 21 July 2020, https://www.middleeastmonitor.com/20200721-israel-approves-mobile-phone-tracking-of-covid-19-carriers-for-rest-of-year/.

other recent case law around large-scale surveillance, the notion that a whole population could be put under surveillance was not in and of itself challenged by the judges. Such court decisions regarding privacy interference justified in the name of fighting the COVID-19 pandemic exemplify the inherent limitations of the law in countering an ever-expanding state surveillance, and generally speaking of the inadequacy of legal procedures in protecting some of the core values attached to democracy.[80] They speak to the fact that the expansion of state surveillance is only exceptionally hindered by the courts, but instead mostly constrained through forms of proceduralisations that are meant – but, one may argue, often fail – to safeguard human rights and other substantive values that the rule of law serves to protect.

Finally, the ongoing health crisis could also lead to another classic consequence of "warlike" crises in the relations between states and citizenship: the muzzling of political oppositions. In this respect, a brief from the research centre of the French "*gendarmerie*" (rural police) – which provides an "analysis of the [terrorist] threat in the context of a pandemic"[81] – offers a signal which could prove to be a harbinger. Among other things, its author gives an overview of activist publications critical of the techno-securitarian response of states to the pandemic, including the opposition to backtracking applications. Writing that these build on "the fantasised spectre of a Big Brother state taking advantage of the crisis to 'militarise the public space'," the author go as far as presenting such texts as a form of proto-terrorist propaganda fuelling the "ultra-left." Echoing other similar "you're either with us or against us" discourses by prominent politicians and other elites, such claims serve to create a symbolic space which could be leveraged to engage in the surveillance and repression of anti-surveillance activism.

Conclusion

At the time of writing, the COVID-19 pandemic is still underway and its consequences in the realm of state surveillance will continue to unfold in the coming months. But as I have shown in this article, it has so far led to to the amplification of ongoing trends in the realm of digital surveillance in at least three interrelated ways.

First, along with the growing resort to computing technologies aimed at enforcing at scale the restrictions attached to the health crisis, social distanc-

[80] Félix Tréguer, 'The Reason of State, Surveillance & Radical Democracy', GUARDINT Working Paper (Paris: CERI Sciences Po, November 2019), https://halshs.archives-ouvertes.fr/halshs-02864410.

[81] Alexandre Rodde, 'Covid-19 et terrorisme : analyse de la menace dans un contexte de pandémie', Note du CREOGN (Centre de recherche de l'école des officiers de la gendarmerie nationale, April 2020), https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Covid-19-et-terrorisme-analyse-de-la-menace-dans-un-contexte-de-pandemie.

ing and the ever-growing digitisation of social life are reinforcing surveillance assemblages that already dominate digital infrastructures and which are now proliferating in new policy fields such as health policy. Secondly, the goal of protecting the population's health is joining other prominent legitimation discourses – e.g. those related to crime and terrorism, or more mundanely to bureaucratic rationalisation and optimisation – in forming the symbolic space through which new and controversial surveillance technologies and practices can turn into a "new normal." Thirdly, I have argued that "health crisis discourses" also tend to weaken the position of oversight actors enacting "checks and balances," allowing the executive branch to enroll other state institutions in pushing back legal boundaries, thereby undermining human rights.

Of course, the power tactics deployed in the course of the pandemic have faced various and diverging forms of popular resistance, be they expressed through protest, rejection or disbelief. In the realm of surveillance, an interesting example are backtracking applications and their low rates of adoption across Europe.[82] Non-use of backtracking apps may be interpreted as a rebuttal of governments handling of the crisis, a form of "exit" that directly or indirectly indicate that people are not buying into the "technological solutionism" staged by ruling elites and allied experts.[83] Rather than an actual solution, many people saw backtracking apps as a form of distraction or manipulation aimed at concealing the mishaps of state actors in the handling of the crisis. In that sense, the rush towards techno-securitarian response to the COVID-19 pandemic may have reinforced the lack of trust between ruling elites and the wider population. While it is too early to tell, it may foreshadow future mobilisations opposing the broader push towards digitisation and surveillance

But in the meantime, while Big Tech and their "little sisters" of the start-up world push for the technocratic vision of a "tele-everything society" and partner with state actors to de-multiply data collection as well as surveillance and policing measures, as the rule of law gets supplanted by ever-growing executive powers in the name of protecting the population from the COVID-19, and as massive stimulus plans seem to focus first and foremost on preserving the industrial and financial sectors while schools, higher education and indeed public healthcare are plunged into chaos, we arrive at a rather chilling conclusion: after the 2007-2008 economic crash and a long series of anti-terrorist crises, the COVID-19 pandemic looks like yet another crisis

[82]Gabriel Geiger, 'Europeans Aren't Really Using COVID-19 Contact-Tracing Apps', Vice, 21 July 2020, https://www.vice.com/en_us/article/akzne5/europeans-arent-really-using-covid-19-contact-tracing-apps.

[83]Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (New York: PublicAffairs, U.S., 2013); see also: Sean McDonald, 'Technology Theatre', Centre for International Governance Innovation, 13 July 2020, https://www.cigionline.org/articles/technology-theatre.

deepening the drift towards "authoritarian liberalism": a regime which, time after time and "regardless of the costs," protects industrial capitalism while reinforcing social control and undermining the very institutions of civic life.[84]

[84]The expression "authoritarian liberalism" was proposed Herman Heller, a critic and adversary of the German jurist Carl Schmitt, in a comment on Schmitt's 1932 speech entitled "Strong State Healthy Economy." In this talk, Schmitt advocated a state working for interest of capitalists barons while sheltering them from the contingencies of economic crisis and democratic claims. Heller, Hermann. 2015. 'Authoritarian Liberalism'. *European Law Journal* 21: 295. See also Chamayou, Grégoire, *Du libéralisme autoritaire*, (Zones. Paris: La Découverte, 2020). On the role of the 2007-2008 economic crisis in fostering authoritarian forms of liberalism, see Jessop, Bob, 'Crises, Crisis-Management and State Restructuring: What Future for the State?' *Policy & Politics* 43 (4): 475–92 (2015); Lazzarato, Maurizio, 'Naissance de la biopolitique, à la lumière de la crise'. *Raisons politiques* n°52 (4): 51–61 (2013).