Social Sciences & Humanities Open 2 (2020) 100096

Contents lists available at ScienceDirect

Social Sciences & Humanities Open

journal homepage: www.elsevier.com/locate/ssaho

The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance?

Antónia do Carmo Barriga [a,b,c,*], Ana Filipa Martins [d], Maria João Simões [e,f], Délcio Faustino [d]

[a] Departamento de Sociologia, FCSH, Universidade da Beira Interior (UBI), Estrada Do Sineiro, S/n, 6200, Covilhã, Portugal
[b] CIES-IUL, Sala 2W10, Edifício Sedas Nunes, Av. Das Forças Armadas, 1649-026, Lisboa, Portugal
[c] CICS.NOVA, Avenida de Berna, 26-C, 1069-061, Lisboa, Portugal
[d] Sociology Department, Universidade da Beira Interior, R. José Caetano Júnior 149, 6200-209, Covilhã, Portugal
[e] University of Beira Interior (UBI), Portugal
[f] Interdisciplinary Centre of Social Sciences (CICS.NOVA.UMinho) and LabCom, Portugal

ARTICLE INFO

Keywords:
COVID-19
Surveillance technologies
ICTs
Apps
Privacy and democracy

ABSTRACT

This commentary addresses the use of surveillance technologies in the context of the Covid-19 pandemic, using examples from the current geopolitical frame, and questioning the possible consequences of data collection for the individual and for society. In this regard, some questions emerge: in the fight against the pandemic, what measures and tools of surveillance are being adopted by the different states? Will the extraordinary measures, that are now being implemented, become permanent? And if so, what will the consequences be for privacy and democracy?

1. Introduction

The technological advances that occurred in recent years have made the COVID-19 pandemic context an absolutely new experience for contemporary societies. Today we behold the existence of a variety of technological applications that are being used to minimize certain constraints, which would not be possible otherwise. The people who faced the Spanish Influenza in 1918, did not have the opportunity to talk and see their distant relatives during the period of isolation, did not know in real-time what was happening in the rest of the world, and did not have the opportunity to work from home, or to attend concerts of their favourite artists without leaving their sofa.

It is undeniable that without the technologies that exist today, maintaining the communication with work, friends, and family would be even more difficult. Information and communication technologies (ICTs), essential for communication in times of confinement due to COVID-19, have been crucial in preserving interactions between people and groups, allowing universal connectivity, and keeping individuals connected and collaborating actively (Nunes, 2020). With the intensification of communication through technological resources, data sharing is also intensified, which is fundamental for the effectiveness of artificial intelligence (AI) applications. Additionally, the great investment in the development of AI technologies makes this an area that continually presents us with new concepts and solutions for increasingly complex challenges (Hamet & Tremblay, 2017). Health is one of the areas that could benefit most from advances in this technological area, for example, by contributing to an accrued accuracy in diagnoses and efficiency in treatments, or by assisting in patient surveillance (Ribeiro, 2019). AI and its algorithms, through the manipulation of the data they are programmed to access, exhibit the capacity to make predictions and provide the ideal approach to solve problems associated with the pandemic control (Steiner, 2012).

But there are not only benefits, one of the greatest risks may lie in the combined use of AI and ICTs which further augments the potential for mass surveillance. Through the access to the vastness of data that most individuals make available online, the entities using algorithms are able to perceive aspects about the life of each one of us much more effectively than the individuals themselves (Bartlett, 2018). AI works through these algorithms and, as Nemitz states, "the capabilities of AI, based on big data and combined with the pervasiveness of devices and sensors of the Internet of things, will eventually govern core functions of society" (NemitzPaul, 2018).

The advent of the Internet of Things (IoT) is also crucial to this central role of AI in society. Essentially, the IoT is the interconnectivity between

[*] Corresponding author. Departamento de Sociologia, FCSH, Universidade da Beira Interior (UBI), Estrada do Sineiro, s/n, 6200, Covilhã, Portugal.
E-mail addresses: acab@ubi.pt (A.C. Barriga), ana.filipa.martins@ubi.pt (A.F. Martins), mariajoaosimoes@sapo.pt (M.J. Simões), delcio_faustino@ubi.pt (D. Faustino).

https://doi.org/10.1016/j.ssaho.2020.100096
Received 30 April 2020; Received in revised form 28 November 2020; Accepted 30 November 2020

the various “things” that are used in everyday life and that are linked to each other through the internet, being the main function the communication between all these “things’’ and other entities, such as people or applications (Ciobanuet al. et al., 2014). In fact, we are increasingly surrounded by these smart objects, which make our life easier in many aspects, wherefore we grant them access to our most personal data and multiple activities of our daily lives. In this way, the IoT becomes a fundamental form of data collection that will allow greater efficiency in the performance of AI technologies (Bartlett, 2018) (Broad, 2018).

There are multiple risks associated with certain technological applications, since all technologies used by governments in the control and fight of the pandemic can be used for surveillance and pose undeniable threats to privacy, individual freedoms, and democracy. Taking into account the above, this piece aims to discuss and highlight these threats. This piece is structured into two sections. The first one approaches several theoretical aspects of surveillance, namely its ambivalent nature often associated with the privacy-security trade-off, and the concept of surveillance creep. On the second one, we try to summarize the adopted surveillance measures and technologies highlighting some specific and relevant cases in the fight against the current COVID-19 pandemic.

2. The ambivalent nature of surveillance

Lyon (Lyon, 2001), Finn et al. (Finn et al., 2018) point out the Janus-faced nature of surveillance which acts both as an enabler and constrainer to our action. This ambivalent process can be found in the way how surveillance is oriented towards both care and control, for instance when considering governmental surveillance, the same surveillance systems that can be used to serve positive aspects such as protection, optimization of administration, and rule compliance can also enable negative aspects such as manipulation, discrimination and social control (Marx and Staples, 2007). As Lyon (Lyon, 2001) asserts, negative and/or positive dimensions of surveillance can be enhanced more in one direction than in the other, depending on several aspects such as interests, and the purposes surveillance devices are designed, created, and used for. Other aspects to consider are the social and historical context as well as the ideologies of people and organisations.

The belief that collecting more data will lead to a more timely and efficient response to a crisis, makes it difficult to resist the urge for more data collection, as Boersma and Fonio (Boersma et al., 2018) address in such contexts the negative dimension of control “is often overlooked in the literature of crisis management due to the positive connotation of control for assessing needs, helping people, and counting human and economic losses”. Such data collection, processing, and analysis have reinforced concerns regarding the trade-off of security versus privacy and liberty (Büscher et al., 2015). Additionally, even if improvements on security and safety are achieved through the new reinforced surveillance measures, it is hard to guarantee that once the crisis is over, these technologies will not be redirected for control-oriented surveillance. Moreover, totalitarian governments can take advantage of the fight against a crisis to install technologies to reinforce the political surveillance of citizens.

In fact, the adoption of more surveillance technologies is always a risk, the expression ‘when one door opens, it hardly closes again’ can easily be applied to the adoption of new surveillance technologies. As Edward Snowden argued in his recent interview for Vice, once we abdicate certain civil liberties due to an emergency, it might be hard to get them back or a least fully back. Snowden presents the example of the Bush-era warrantless wiretapping, claiming that it came as a response to the events of 9/11 but that only part of it was shutdown (Dowd, 2020). This is just an example among many that can be described as *surveillance creep* since a “tool introduced for a specific purpose comes to be used for other purposes” (Marx, 2005). Other authors such as Pisa (Pisa, 2020) and Harari (Harari, 2020) also address the potential post-COVID-19 pandemic long-term effects on surveillance after the end of the crisis. Harari (Harari, 2020) clearly expresses his concern about the possibility of COVID-19 temporary measures outlasting the pandemic, becoming entrenched in our lives. Pisa (Pisa, 2020) adds that there is a need for mechanisms to unwind surveillant measures that were implemented and legitimised during the crisis, such as ‘sunset clauses’ where an emergency surveillance measure is automatically terminated once the triggering event is over.

In this sense, the crucial question that needs to be addressed is what happens once the pandemic is over? Many are concerned that the extraordinary measures being implemented will become permanent or also used for other purposes, further aggravating the threats to privacy, political and civil rights.

Until now, in the Western world, the public debate on the reinforcement of surveillance was focused on how each citizen was willing to sacrifice their privacy in the name of security, that is, to make society safer, particularly from terrorist attacks (which was greatly increased after the 9/11 events). With the COVID-19 outbreak, the question that many have started to ask is how far is one willing to sacrifice their privacy to help in the fight against the pandemic. In this context, one needs to consider the impacts of the use of technologies such as tracking apps or other invasive technologies that include facial recognition or body temperature measurement. It should be noted that, already in 1890, Warren and Brandeis were advocating for privacy to be a right that should be protected by the State, indicating their concerns towards the emergence of cameras and the seemingly unlimited development of the media (Brandeis & Warren, 1890). Today the fear of privacy invasion – where one is, with whom has one been, what diseases does one have – comes mainly from digital media (see, for example, the Facebook-Cambridge Analytica scandal where millions of Facebook users’ personal data was acquired without consent). Yet, privacy is more than an individual concern, it is a functional prerequisite for free democratic societies (Büscher et al., 2015), for instance, one can certainly wonder if citizens can politically participate when they are aware that they are under surveillance? (Simões et al., 2018).

3. Surveillance measures and technologies used for pandemic control

In the fight against the contagion from the new coronavirus and the control of the COVID-19 pandemic, several states have been adopting measures and tools of surveillance very diverse in the degree of invasion of citizens’ privacy and the violation (or not) of their fundamental rights and guarantees. During April, the Organisation for Economic Cooperation and Development (OECD) warned about the risks for privacy arising from the adoption of tracking technologies in the control of COVID-19, such as contact tracing and facial recognition systems. The European Commission has published a set of rules for applications that collect data from users, deeming unnecessary the creation of highly invasive applications that collect the exact location of the user through GPS. While safeguarding that European countries cannot force people to install applications either, the European Commission has mentioned the need for the anonymity of collected data and has defined that applications must be suspended when they are no longer needed (Pequenino, 2020a).

Technology using facial recognition, biometrics, AI, and big data analysis has been applied before, but now several organisations are striving to develop applications that specifically can help contain the COVID-19 pandemic. Under the excuse of disease control, technologies can be used to monitor all steps, activities, and contacts of citizens through the use of big data. Hence, government entities will be able to know, for example, who broke the confinement, or who is more likely to be infected (Marr, 2020). This is certainly something that greatly eases the efforts being made in the fight against COVID-19, but in any case, there will be, although to different degrees, threats to both civil rights and liberties, and even to democracy itself.

In Europe, as in the USA, there has been a search for an app that is both efficient at epidemiological control, and that guarantees the privacy of its users. The debate revolves around two major questions: on the one hand, whether the most adequate technique used for the screening is Bluetooth or geolocalisation, and on the other hand, the choice of data storage procedure – a centralised model in which data is gathered in the cloud or server of the responsible institution, or a decentralised one where data is stored in the users' phones (Marr, 2020).

In order to be efficient, Bluetooth needs a massive adherence, although, it is less intrusive because it can analyse the information without collecting personal data. On the other hand, geolocalisation requires that the user grants access to their location. Yet, many other variables determine the success or feasibility of an app created for this purpose. First of all, its success depends on the number of citizens who decide to install it. At the moment (November 2020), there are more than 50 digital applications worldwide to help the fight against COVID-19, however, the download percentage is often situated in around 20%. The most used applications are those in Singapore with more than 2.4 million people using Trace Together, which is equivalent to 42% of the population; Ireland's COVID Tracker-App, which follows the most popular European model (uses technology developed by Google and Apple to register anonymous contacts between mobile phones), was already installed by more than two million people (40% of the country's population). However, without mass acceptance by the population, experts warn that apps alone are of little use in combating the pandemic. Secondly, the success of an application depends on whether the population has compatible smartphones. Thirdly it also depends on the willingness of the medical class to be collaborative in providing the codes to be introduced by the infected people. Fourthly, the collaboration of the people is crucial, only installing the app is not enough, they need to indicate the correct test results and insert them on the apps. Lastly, the correct functioning of the app is necessary, it should be noted that in late October, the United Kingdom's app version, the NHS COVID-19, sent "false alarms" to several users of the app, indicating that they had been close to someone diagnosed with COVID-19. The error was amended later on, but the information had already been sent to more than 19,000 people (Pequenino, 2020b).

All things considered, governmental representatives of 5 European countries (Germany, France, Italy, Spain, and Portugal) argued in a collective statement that tracking apps would be a "useful tool" in the fight against the spread of COVID-19 in Europe, since they can "play an important role" in bringing this health crisis to an end. The development of efficient technical solutions that can be used beyond the borders of member states is seen as the current challenge (Lusa, 2020a).

Regarding the choice of data storage procedure, Apple and Google, in an unprecedented partnership, joined efforts in a contact tracking technology project, based on Bluetooth technology, which allows the reduction of the virus spread while setting limits on the type of data that can be sent to public authorities (Google and Apple and Google, 2020).

On the 20th of May, they provided an Application Programming Interface (API) to the 22 countries that requested access to it. But only one application per country can have access to the API and it must be developed by the government or the public health entities. Apple and Google's approach is "decentralised" and presented as offering more privacy. This model has been the one gathering more consensus in Europe. Additionally, it has been supported by scientists and has the adhesion of Germany (Pequenino, 2020c). In early August, using Apple and Google's API, European countries such as Austria, Croatia, Denmark, Germany, Italy, Ireland, Latvia, and Poland, released their apps. Additionally, Switzerland, Northern Ireland, and Gibraltar have adopted similar apps (StaffExplainer, 2020). The StayAway COVID app, released by the Portuguese Government on the 1st of September, also follows the technological module that has been presented as Google Apple Exposure Notification (GAEN) (Moreira, 2020).

OneZero magazine indicates 28 countries where surveillance to fight the coronavirus has increased significantly (Gershgorn, 2020). The most common form of surveillance implemented to fight the pandemic is the use of smartphone location data, which can track the movement of the population and the quarantines when these are imposed. But it can be intrusive in different ways and to different degrees, there are numerous disturbing examples of surveillance and rights violations, which can be aggravated in the post-pandemic context due to the possibility of surveillance creep. Not having the pretension of exhaustiveness, here we refer a few examples below, despite the need for constant updates.

In the United States, state agencies are reportedly in discussions with Clearview A.I. Inc. and Palantir about ways to use facial recognition and data mining technology to track infected patients, while the Federal Government is exploring the use of geolocational data provided by Google and Facebook and other tech companies to monitor the spread of the virus (Grind et al., 2020) (Romm et al., 2020).

In Europe, there are diverse uses of technology somewhat dissimilar in terms of the degree of invasion of privacy. Thus, some countries are developing applications that use Bluetooth technology: Germany, Italy, Ireland, Austria, and the Czech Republic. But in this last country, the app eRouška uses location data from telecommunication operators to build "memory maps" which can be summarised to a graphical view of where a user has spent significant time over the past five days. Still in Europe, the UK is also developing a system similar to the one used in China: users who have been close to COVID-19 patients receive a yellow alert and infected users receive a red alert and instructions to enter quarantine. Documents released by the Guardian newspaper report technology companies using the information to create 'COVID-19 data storage' and the use of confidential patient data by the government in response to the coronavirus (Marr, 2020). In Poland, the government has created an application that randomly asks citizens, that have to quarantine, for mandatory selfies; the user has 20 min to post a selfie on the spot, or is otherwise visited by the police at home (Hamilton, 2020).

Asian countries have gone further in their contact tracing efforts, building upon systems and tools developed in the aftermath of SARS and MERS, that rely on a combination of on-the-ground detective work and the use of invasive digital tools to track people's movements (Pisa, 2020).

Thus, China has used the impressive tracking innovations of the country's technology companies: AI helmets to measure temperature, drones capable of using facial recognition to alert those who were not wearing masks in public, and mobile applications to control travel (Xinhua, 2020) (Borak, 2020). In this way, billions of personal data were collected daily, either through surveillance cameras (200 million are scattered throughout the territory) or through location data from mobile phones or social networks. Facial recognition software has been linked to citizens' criminal records by assigning them a QR code (generated through the Alipay Health Code app) and classifying them as "green", "yellow" or "red", according to the risk they carry. The measures were already common at a central level. The novelty arises when, for the first time, local police forces also begin to create their own surveillance systems (TVI, 2020).

In South Korea, citizens who have breached mandatory quarantine have been forced to wear electronic bracelets which have the ability to alert the authorities whenever a person tries to remove them or leaves their confinement space (Lusa, 2020b). In addition to the surveillance cameras, the authorities have accessed credit card data, and the resulting movement of users, to identify possible transmission chains of the virus (Wray, 2020). The information has been collected from a variety of sources including CCTV footage, cell phone records, and credit card receipts of "confirmed COVID-19 patients" to post "the precise movements (without names) of everyone who tested positive — everything from the seat numbers they occupied in movie theatres to the restaurants where they stopped for lunch" (Engelberg et al., 2020).

In Taiwan, the National Health Insurance Administration (NHIA), and the National Immigration Agency, combined their databases to enable the government to track the 14-day travel history of citizens alongside health information tied to their NHIA identification card. Individuals identified as high risk are then monitored electronically through their mobile phones (Wang et al., 2020).

In India, a government district in the state of Kerala used geo-mapping of quarantine locations, CCTV recordings, and call record data to "track down over 900 primary and secondary contacts of a family who returned from Italy carrying the COVID-19 infection" (Varma, 2020).

Israel has used advanced technologies to tackle a second wave of contamination (thermal cameras to measure the temperature of a crowd or algorithms connected to large databases to determine the new sources of contagion in real-time) (Tilt-L and Como Israel usa, 2020). In March, Israel announced its plans to use the same digital technologies normally used by the ISA (Israel Securities Authority) to monitor terrorist groups to track the spread of COVID-19 (França, 2020) (Lubell, 2020). However, a few weeks later, in April, the Israeli Supreme Court held that the COVID-19 surveillance resulting from emergency regulations was only appropriate when the threat's dimension was still uncertain – which was no longer the case (Chachko, 2020).

In Argentina, those who are caught not complying with the quarantine are forced to download the tracking application and located through the smartphone's GPS signal (Gershgorn, 2020). The Moroccan police, on the other hand, will have a mobile application that allows them to track the movements of citizens and identify those who disobey the rules of the state of emergency (Lusa, 2020c).

It should be noted that there are already a number of countries where the pandemic is being used to erode democracy. In Russia, in addition to strengthening the use of technology for mass scrutiny, new rules have been approved against fake news about the virus, which could be reflected in increased persecution of independent media – something that is also being applied in Serbia and Turkey. In Hungary, the fight against the coronavirus includes arresting the critics of Viktor Orbán that opposed him through social media platforms. Anyone accused of spreading rumours, fake news, or other information that could create social turmoil, can be sentenced to up to 5 years in prison — and criticising the government through social media is now framed as such. With the argument of protecting public health, data of people infected or suspected of being infected is now disclosed (Sahuquillo et al., 2020) (Sandford, 2020). In Israel, the Likud party, that won a majority of seats in the most recent election, used the health emergency to prevent the opposition from taking control of parliamentary procedures (Sahuquillo et al., 2020).

According to the Democracy Report 2020 (Lührmann et al., 2020) of the University of Gothenburg, which studied, on a global scale, the effects on democracy of emergency measures aimed at containing the pandemic by limiting rights and freedoms, those same measures aggravated the decline of democracy in at least 82 countries.

There are therefore enough reasons for more than 100 human rights organisations, civil liberties activists, and consumer groups around the world to issue a collective declaration on COVID-19 and electronic surveillance, calling on governments to use tracking technologies only if they are carried out strictly in accordance with human rights principles (Soguel, 2020).

4. Final considerations

This piece discusses a changing reality in terms of both the emergence and implementation of technologies (e.g. contact tracing apps) or in terms of the measures governments are adopting in response to the ever-changing pandemic context.

Presently, many governments are rushing to put electronic surveillance systems in place with minimal ethical considerations or informed debate within their societies. This reality varies widely from country to country, some governments are more intrusive than others, and, as previously mentioned, some are using the opportunity to install technologies to reinforce the political surveillance of citizens. The technology at the disposal of the States to control the pandemic has enormous potential for surveillance which often threatens individual privacy.

All over the world, in many countries, the pandemic has been the engine (or pretext) for deteriorating the quality of democracies and undermining human rights compliance, including in those with a strong democratic tradition. Even though in some countries this aggravation was already a tendency before the pandemic. We have presented examples of countries with authoritarian regimes that use emergency measures to harass their opponents even more severely or to silence protests.

People's resistance to installing apps is related to the privacy invasion fear, namely, they fear that their location will be known – from the physical place where one is a lot of information can be used for political or commercial purposes. The question of mistrust towards the guarantee of anonymity is also relevant, for instance, personal health data can be used by insurance companies. Additionally, the future use of the data may be questioned, because if it is not destroyed, it may be appropriated by others (the large digital platforms or the State itself) and used for other purposes. In certain circumstances, another resistance may be related to the requirement to guarantee the fulfilment of citizens' rights, enshrined in the constitution and in the law of democratic countries.

Finally, it should be noted that one of the questions that arises is that most surveillance measures are a threat to privacy and democracy, we are facing not only the risk of normalisation but also of surveillance creep which is, as previously mentioned, a strong tendency after new surveillance measures or technologies are implemented in response to a crisis. It is also important that citizens are informed in order to participate in the debate regarding surveillance measures and the way technologies are designed since they pose serious threats to both privacy and democracy.

It is known that ICTs made the distinction between what is considered public and private much harder, as Habermas (Habermas, 1984), (Habermas, 1998) asserts, privacy preservation is imperative in order for people to be free and capable of expressing their opinions and decisions in the public sphere. Citizens are becoming more aware that their political activity is increasingly monitored, this can involve a more self-constrained political activity or, in some cases, even demobilise their political activity altogether (Simões, 2011).

We would like to wrap up this piece by asserting that contemporary societies were already going through a period of increasing uncertainty, with the fight against the COVID-19 pandemic, the threats to privacy and democracy are becoming even more severe.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Antónia do Carmo Barriga: Conceptualization, Writing - original draft, Supervision. **Ana Filipa Martins:** Conceptualization, Writing - original draft, Writing - review & editing. **Maria João Simões:** Conceptualization, Writing - original draft, Writing - review & editing. **Délcio Faustino:** Conceptualization, Writing - original draft, Writing - review & editing.

References

Bartlett, J. (2018). *The People vs Tech – how the internet is killing democracy (and how we save it)*. New York: Dutton – Penguin Random House LLC.

Boersma, K., & Fonio, C. (2018). Big data, surveillance and crisis management. In K. Boersma, & C. Fonio (Eds.), *Big data, surveillance and crisis management* (pp. 1–16). New York: Routledge.

Borak, M. (February 28, 2020). *Chinese police now have AI helmets for temperature screening*. Abacus. https://www.scmp.com/abacus/news-bites/article/3052879/chinese-police-now-have-ai-helmets-temperature-screening [10-04-2020].

Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Broad, E. (2018). *Made by humans, victoria*. Melbourne: Melbourne University Press.

Büscher, M., Perng, S.-Y., & Liegl, M. (2015). Privacy, security, liberty: ICT in crises. *International Journal of Information Systems for Crisis Response and Management, 6*(4), 72–92.

Chachko, E. (May 5, 2020). *The Israeli Supreme Court checks COVID-19 electronic surveillance*. Lawfare. https://www.lawfareblog.com/israeli-supreme-court-checks-covid-19-electronic-surveillance?fbclid=IwAR1h2gJi1JzWN25A2RDAHa8Uzozm2OXQB-5rNj-bjfaVTX5quxWcyhwAGgQ [14-09-2020].

Ciobanu, R.-I., et al. (2014). Big data plataforms for the internet of things. In N. Bessis, & C. Dobre (Eds.), *Big data and internet of things: A roadmap for smarts environments* (pp. 3–34). Cham: Springer.

Dowd, T. (April 9, 2020). *Snowden warns governments are using coronavirus to build 'the architecture of oppression'*. Vice https://www.vice.com/en_us/article/bvge5q/snowden-warns-governments-are-using-coronavirus-to-build-the-architecture-of-oppression [12-04-2020].

Engelberg, S., Song, L., & DePillis, L. (March 15, 2020). *How South Korea scaled coronavirus testing while the U.S. Fell dangerously behind*. ProPublica. https://www.propublica.org/article/how-south-korea-scaled-coronavirus-testing-while-the-us-fell-dangerously-behind (14-04-2020].

Finn, R., Watson, H., & Wadhwa, K. (2018). Mining social media for effective crisis response: Machine learning and disaster response. In K. Boersma, & C. Fonio (Eds.), *Big data, surveillance and crisis management* (pp. 38–56). New York: Routledge.

França, A. (March 21, 2020). *Israel vai monitorizar telemóveis para combater o coronavírus. Nem toda a gente considera que isso faz bem à saúde (democrática)*. Expresso. https://expresso.pt/coronavirus/2020-03-21-Israel-vai-monitorizar-telemoveis-para-combater-o-coronavirus.-Nem-toda-a-gente-considera-que-isso-faz-bem-a-saude–democratica- [15-04-2020].

Gershgorn, D. (April 9, 2020). *We mapped how the coronavirus is driving new surveillance programs around the world*. OneZero. https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9 [18-04-2020].

Google. (April 10, 2020). *Apple and Google partner on COVID-19 contact tracing technology*. https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/ [19-04-2020].

Grind, K., McMillan, R., & Mathews, A. W. (March 17, 2020). To track virus, governments weigh surveillance tools that push privacy limits. *The Wall Street Journal*. https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841?mod=hp_lead_pos3 [12-04-2020].

Habermas, J. (1984). *Mudança Estrutural da Esfera Pública*. Rio de Janeiro: Edições Tempo Brasileiro.

Habermas, J. (1998). *Between facts and norms: Contributors to a discourse theory of law and democracy*. Cambridge: Polity Press.

Hamet, P., & Tremblay, J. (2017). Artificial intelligence in medicine. *Metabol*, (69), 36–40. https://doi.org/10.1016/j.metabol.2017.01.011

Hamilton, I. A. (March 23, 2020). *Poland made an app that forces coronavirus patients to take regular selfies to prove they're indoors or face a police visit*. Business Insider. https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3 [12-04-2020].

Harari, Y. H. (March 20, 2020). *The world after coronavirus*. The Financial Times. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75?fbclid=IwAR1ucVmXDQapaiS2_Lo0IDyqCkzCahpU0WU0gr06MJTYQ47pBgdm-4eoEV0, 25-08-2020.

Lubell, M. (March 14, 2020). *Israel to use anti-terror tech to counter coronavirus 'invisible enemy*. Reuters. https://www.reuters.com/article/us-health-coronavirus-israel/israel-to-use-anti-terror-tech-to-counter-coronavirus-invisible-enemy-idUSKBN21113V [17-04-2020].

Lührmann, A., Maerz, S., Grahn, S., Alizada, N., Gastaldi, L., Hellmeier, S., Hindle, G., & Lindberg, S. (2020). *Autocratization surges-resistance grows: Democracy report 2020*. V-Dem Institute https://www.v-dem.net/media/filer_public/f0/5d/f05d46d8-626f-4b20-8e4e-53d4b134bfcb/democracy_report_2020_low.pdf, 06-09-2020.

Lusa. (April 11, 2020). *Covid-19: Coreia do Sul vai usar pulseira eletrónica para quem violar quarentena*. Visão. https://visao.sapo.pt/atualidade/politica/2020-04-11-covid-19-coreia-do-sul-vai-usar-pulseira-eletronica-para-quem-violar-quarentena/?fbclid=IwAR1rxucfzqmRl-9ta072qI5F3l4AYzyGQMCceeJo4dsPzbT_NUCakCWqFik [18-04-2020].

Lusa. (April 22, 2020). *Polícia de Marrocos cria aplicação para rastrear movimentos dos cidadãos*. TSF. https://www.tsf.pt/mundo/policia-de-marrocos-cria-aplicacao-para-rastrear-movimentos-dos-cidadaos-12100780.html [24-04-2020].

Lusa. (May 26, 2020). *Cinco países europeus, incluindo Portugal, defendem aplicações de rastreamento*. Público. https://www.publico.pt/2020/05/26/tecnologia/noticia/cinco-paises-europeus-incluindo-portugal-defendem-aplicacoes-rastreamento-1918093 [25-08-2020].

Lyon, D. (2001). *Surveillance society – monitoring everyday life*. Buckingham: Open University Press.

Marr, B. (March 13, 2020). *Coronavirus: How artificial intelligence, data science and technology is used to fight the pandemic*. Forbes. https://www.forbes.com/sites/bernardmarr/2020/03/13/coronavirus-how-artificial-intelligence-data-science-and-technology-is-used-to-fight-the-pandemic/#678525e15f5f [19-04-2020].

Marx, G. (2005). Seeing hazily (but not darkly) through the lens: Some recent empirical studies of surveillance technologies. *Soc. Inq., 30*(2), 339–399. https://doi.org/10.1111/j.1747-4469.2005.tb01016.x, 385.

Marx, G. T. (2007). Surveillance. In W. G. Staples (Ed.), *Encyclopedia of privacy* (pp. 535–544). Westport: Greenwood Press.

Moreira, S. (September 2, 2020). *Apple e Google lançaram aplicação similar à StayAway Covid, que está disponível para os governos que a solicitarem*. Expresso. https://expresso.pt/coronavirus/2020-09-02-Apple-e-Google-lancaram-aplicacao-similar-a-StayAway-Covid-que-esta-disponivel-para-os-governos-que-a-solicitarem [03-9-2020].

Nemitz, P., & Paul. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Phil. Trans. R. Soc. A., 376*(2133), 2. https://doi.org/10.1098/rsta.2018.0089

Nunes, N. (2020). Pandemia e tecnologia – o futuro chegou mais cedo. *Jornal I*. https://ionline.sapo.pt/artigo/689763/pandemia-e-tecnologia-o-futuro-chegou-mais-cedo?seccao=Opini%C3%A3o [20-04-2020].

Pequenino, K. (April 21, 2020). *OCDE alerta sobre uso de tecnologias de rastreio e reconhecimento facial para controlar covid-19*. Público. https://www.publico.pt/2020/04/21/tecnologia/noticia/ocde-alerta-uso-tecnologias-rastreio-reconhecimento-facial-controlar-covid19-1913138?fbclid=IwAR2plMBF7DXyuJLIFNQaAnZwgkmqvmB5XXW1tQ5VhZRYtIcm2Z_GU7tLUlA. April 22, 2020.

Pequenino, K. (May 20, 2020). *Google e Apple lançam suporte para aplicações de rastreio de contágio nacionais*. Público. https://www.publico.pt/2020/05/20/tecnologia/noticia/google-apple-lancam-suporte-aplicacoes-rastreio-contagio-nacionais-1917439 [26-08-2020].

Pequenino, K. (November 8, 2020). *As apps não podem salvar esta pandemia. Especialistas põem eficácia em causa*. Público. https://www.publico.pt/2020/11/08/tecnologia/noticia/apps-nao-podem-salvar-pandemia-especialistas-poem-eficacia-causa-1937562 [08-11-2020].

Pisa, M. (March 20, 2020). *COVID-19, information problems, and digital surveillance*. CGD. https://www.cgdev.org/blog/covid-19-information-problems-and-digital-surveillance?fbclid=IwAR1ucVmXDQapaiS2_Lo0IDyqCkzCahpU0WU0gr06MJTYQ47pBgdm-4eoEV0, 25-08-2020.

Ribeiro, J. M. (2019). *Saúde Digital: Um sistema de saúde para o século XXI*. Lisbon: Fundação Francisco Manuel Santos.

Romm, T., Dwoskin, E., & Timberg, C. (March 18, 2020). *U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus*. The Washington Post. https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2ftechnology%2f2020%2f03%2f17%2fwhite-house-location-data-coronavirus%2f [13-04-2020].

Sahuquillo, M. R., Blanco, S., & Liy, M. V. (March 31, 2020). *Pandemia ameaça facilitar erosão da democracia em países como Hungria e Rússia*. El País. https://brasil.elpais.com/internacional/2020-03-31/coronavirus-poe-a-democracia-de-quarentena.html, 20-04-2020.

Sandford, A. (May 15, 2020). Hungary: 'Critics silenced' in social media arrests as EU debates orban's powers. *Euro News*. https://www.euronews.com/2020/05/14/hungary-critics-silenced-in-social-media-arrests-as-eu-debates-orban-s-powers [20-08-2020].

Simões, M. J. (2011). Surveillance: A (potential) threat to political participation?. In *Icds 2011: The fifth international conference on digital society, gosier, Guadeloupe, France* (pp. 94–99). February 23-28 http://www.thinkmind.org/index.php?view=article&articleid=icds_2011_3_40_10096.

Simões, M. J., & Jerónimo, N. (2018). Rear Window – transparent citizens versus political participation. In A. Saetnan, I. Schneider, & N. Green (Eds.), *The politics of big data – big data, big brother?* (pp. 176–196). London: Routledge.

Soguel, D. (March 20, 2020). *Pandemic dilemma: Emergency surveillance won't be easy to unplug*. https://www.csmonitor.com/Technology/2020/0330/Pandemic-dilemma-Emergency-surveillance-won-t-be-easy-to-unplug [15-04-2020].

Staff, R., & Explainer. (August 5, 2020). *Europe's coronavirus smartphone contact tracing apps*. Reuters. https://uk.reuters.com/article/uk-health-coronavirus-europe-tech-explai/explainer-europes-coronavirus-smartphone-contact-tracing-apps-idUKKCN2510N3 [26-08-2020].

Steiner, C. (2012). *Automate this: How algorithms came to rule our world*. New York: Portfolio/Penguin Group.

Tilt-UOL. (June 26, 2020). *Como Israel usa tecnologia de ponta para impedir segunda onda de covid-19*. Tilt. https://www.uol.com.br/tilt/noticias/afp/2020/06/26/israel-recorre-a-inteligencia-artificial-para-impedir-segunda-onda-de-covid-19.htm [25-08-2020].

TVI, O. (April 7, 2020). *Big Brother" da vida real que a China usou para travar a pandemia de Covid-19*. https://tvi24.iol.pt/videos/internacional/o-big-brother-da-vida-real-que-a-china-usou-para-travar-a-pandemia-de-covid-19/5e8ce6800cf2a5883420007f [19-04-2020].

Varma, V. (March 13, 2020). *Covid-19: How a Kerala district brought nearly 900 people within surveillance net*. The Indian Express. https://indianexpress.com/article/india/kerala/covid-10-coronavirus-kerala-pathanamthitta-district-surveillance-precautions-6311041/ [7-04-2020].

Wang, C. J., Chun, Y., & Brook, R. H. (March 3, 2020). Response to COVID-19 in taiwan: Big data analytics, new technology, and proactive testing. *JAMA Network*. https://jamanetwork.com/journals/jama/fullarticle/2762689?guestAccessKey=2a3c6994-9e10-4a0b-9f32-cc2fb55b61a5&utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_content=tfl&utm_term=030320 [16-04-2020].

Wray, S. (March 12, 2020). South Korea to step-up online coronavirus tracking. In *Smart cities world*. https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109 [09-04-2020].

Xinhua. (March 19, 2020). *High-tech helmets tackle temperature tasks*. China Daily. https://www.chinadaily.com.cn/a/202003/19/WS5e72d914a3101282172805d0.html [24-04-2020].

Antónia do Carmo Barriga, PhD in Sociology from ISCTE- Lisbon University Institute, and Professor at the Department of Sociology of the University of Beira Interior (UBI), Portugal, Researcher at CIES-IUL and associated researcher at CICS.NOVA. She has researched and published in the field of sociology of communication (politics and (new) media.