Tracking the outbreak and far beyond: How are public authorities using mobile apps to control Covid-19 pandemic

Monitorizando muito mais do que o surto: como as autoridades públicas estão a usar aplicações móveis para controlar a pandemia de Covid-19

Rita Basílio de Simões

Universidade de Coimbra, Faculdade de Letras, Coimbra, Portugal
Instituto de Comunicação da NOVA — ICNOVA, Lisboa, Portugal
rbasilio@fl.uc.pt
ORCID ID: 0000-0001-6356-6042

Inês Amaral

Universidade de Coimbra, Faculdade de Letras, Coimbra, Portugal
Centro de Estudos de Comunicação e Sociedade — CECS, Braga, Portugal
inesamaral@gmail.com
ORCID ID: 0000-0003-4929-4866

Sílvio Santos

Universidade de Coimbra, Faculdade de Letras, CEIS 20, Coimbra, Portugal
silviocorreiasantos@gmail.com
ORCID ID: 0000-0002-6208-7311

DOI: https://doi.org/10.34619/bpcg-nb43

Abstract: COVID-19 brought tremendous challenges to the world during 2020. The consequences of the pandemic are still hard to estimate. However, the socio-economic crisis that hit every nation, from major developed economies to least developed countries is transversal and quite visible. Despite the existence of various context-specific approaches, there is a global effort that stands on three main areas: scientific research, ultimately focused on finding a cure or a vaccine; technological use to support social changes on domains like work, distance-learning or risk detection; and governmental measures promoting lockdown, isolation and safety practices. This research is focused on the use of technology to improve the response to the pandemic in a globalised network society by tracking patterns of interaction between people. The use of self-tracking apps has been pushed by various governments, raising concerns regarding surveillance, social control and data collection. We analyse through the walkthrough method a group of 13 mHealth apps that were supported by public authorities during 2020. Stemming from a critical sociological perspective of contemporary uses and consumptions of digital media, we gather data that promotes a deeper understanding of the role that this kind of apps has in normalising surveillance practices for political purposes and their potential impact in everyday life.

Keywords: Covid-19; mHealth apps; government surveillance; self-tracking; affordances.

Resumo: *A COVID-19 trouxe ao mundo desafios tremendos durante 2020. As consequências da pandemia ainda são difíceis de estimar. Contudo, a crise socioeconómica que atingiu todas as nações, das principais economias desenvolvidas aos países menos desenvolvidos, é transversal e bem visível. Apesar da existência de várias abordagens específicas, há um esforço global que se apoia em três áreas principais: investigação científica, orientada, em última análise, para encontrar uma cura ou uma vacina; uso de tecnologia para apoiar mudanças sociais em domínios tais como o trabalho, a educação a distância ou a deteção de risco; e medidas governamentais que promovem práticas de confinamento, isolamento e segurança. Esta investigação centra-se no uso da tecnologia para melhorar a resposta à pandemia nas sociedades em rede globalizadas, monitorizando padrões de interação entre as pessoas. O uso de aplicações de auto monitorização foi impulsionado por vários governos, desencadeando preocupações em relação à vigilância, controlo social e recolha de dados. Recorrendo ao* walkthrough method*, analisamos um grupo de 13 aplicações de* mHealth *lançadas por autoridades públicas durante 2020. Partindo de uma perspetiva sociológica crítica dos usos e consumos contemporâneos dos* media *digitais, reunimos dados que promovem uma compreensão mais profunda do papel que este tipo de aplicações tem na normalização das práticas de vigilância para fins políticos e o seu impacto potencial na vida quotidiana.*

Palavras-chave: *Covid-19; aplicações de* mHealth*; vigilância governamental; auto monitorização;* affordances.

Introduction

Proclaimed as a pandemic by the World Health Organization (WHO) on 11 March 2020 (WHO 2020), COVID-19 combines a public health threat and a socioeconomic crisis that seem to be changing human lives in unprecedented ways. In response to governments' lockdown measures to limit the spread of the contagious virus following the WHO orientations, schools, universities, all sorts of businesses, stores, and restaurants were closed worldwide. In an attempt to "flatten the curve" of infections during the outbreak, lockdown measures have included, besides self-isolation, with people complying a required 14-day period at home, mandatory quarantine, and monitoring practices for policy governance. Amidst the crisis, the institutional responses comprised both the promotion of "social distancing" and the implementation of surveillance procedures through digital technologies and digital data analytics.

While COVID-19 pandemic is not the first public health crisis to require that governments and public health authorities implement lockdown and surveillance measures, the current situation has an exceptional nature, considering the widespread usage and integration of digital technologies into everyday practices and routines of life. COVID-19 crisis arose in a globalised network society (Castells, 1996), marked in the last years by an environment of deep mediatisation (Hepp, Breiter, & Hasebrink, 2018), and by the routinary use of information technologies to the inspection of individual's data and patterns of interaction, with people actively participating in it.

In some locations, with the advent of COVID-19 existing and new digital technologies began to be harnessed by governments and public health authorities to improve the effectiveness of lockdown measures and population control. Mobile health applications (mHealth apps), in particular, were quickly put into service of the self-monitoring and self-tracking of people's data and encounters as a way of "policing the infection" (Lupton, 2020). Despite growing concerns about the social, economic and political implications of these facilities for information collation and tracking, they are seemingly unifying the efforts and concerns of law enforcement and public citizens.

As other surveillance practices, self-tracking applications can be seen as a form of social control with implications for power relations and democratic norms (Simões & Amaral, Forthcoming). Concerns about "big data" have already led to comprehensive overviews of technology as an artefact and a social process, which embodies new social relations and politics (Andrejevic, 2002, 2007; Lupton, 2014; Zuroff, 2015). Zuroff's theory of "surveillance capitalism" addresses digital information gathering as a process that aims to produce revenue and market control by "predicting and modifying human behaviour" (2015, p. 75). This is the institutional logic where technological affordances are designed and implemented. Likewise, the new logic of gathering health information by public authorities and government agencies are blurring the lines between the right to privacy and benefits of digital surveillance, amplifying at the same time authorities capabilities for population control.

Hence, in the face of COVID-19 pandemic, alongside concerns with the crisis impact on social exclusion, racism and stigmatisation (Kwok, 2020; Logie & Turan, 2020; Rahman, 2020), critical social research has also been paying attention to the collective consequences of digital technologies and digital data analytics as epidemiological surveillance systems (French & Monahan, 2020; Kitchin, 2020; Lupton 2020; Selwyn & Jandri, 2020; Yu, 2020).

For some (Kitchin, 2020; Yu, 2020), we are facing unprecedented challenges to civil liberties. For others (French & Monahan, 2020; Lupton, 2020), surveillance dynamics at play are affecting society and human rights in far-reaching ways. According to Lupton (2020), COVID-19 triggered the "digitised quarantine", a new form of health surveillance based in data sets generated by numerous sources and shaped by resonances with law enforcement. While reflecting the "data-utopian visions", the "digitised quarantine" foresees the dangers of data inaccuracies, biases and injustices, destabilising at the same time the meaning of privacy.

In this chapter, we analyse the digital monitoring and surveillance practices by governments and public health authorities through the use of mHealth apps. Stemming from a critical sociological perspective of contemporary digital media uses and consumptions and departing from analytics of governmentality (Foucault, 1991), we examine 13 mHealth apps launched by the initiative of public authorities during the outbreak through the walkthrough method. We question their role in normalising surveillance for political governance and their potential impact in the most individual and intimate domains of our lives.

First, we contextualise and problematise the surveillance practices triggered in the wake of the COVID-19 public health crisis. We present a review of surveillance practices ties with technology and social control, particularly with self-tracking dynamics and the affordances of mobile applications (m-apps). We then analyse 13 institutional mobile health apps harnessed by public authorities to favour the self-monitoring and self-tracking of human bodies and reflect on the possible implications of these new surveillance tools for a post-COVID public sphere.

COVID-19 crisis and surveillance practices

Digital technology has played a relevant role in providing authorised information and health education in previous public health crises (Lupton, 2018). During the new coronavirus (SARS-CoV-2) crisis, digital media have been essential to keep people informed on what is happening. Also, people have been using digital media to stay in touch, ameliorate the effects of isolation (Ohme, Abeele, Van Gaeveren, Durnez, & De Marez, 2020), and maintain meaningful social activities such as formal education (Teräs, Suoranta, Teräs, & Curcher, 2020; Williamson, Eynon, & Potter, 2020). More significantly, once the pandemic was declared, states and public agencies quickly turned to digital technology-led solutions to respond and control the crisis.

According to Kitchin (2020), five primary purposes explain this institutional dynamic:

> *"(1) quarantine enforcement/travel permission (knowing people are where they should be, either enforcing home isolation for those infected or close contacts, or enabling approved movement for those not infected); (2) contact tracing (knowing whose path people have crossed); (3) pattern and flow modelling (knowing the distribution of the disease and its spread and how many people passed through places); (4) social distancing and movement monitoring (knowing if people are adhering to recommended safe distances and to circulation restrictions); and (5) symptom tracking (knowing whether the population are experiencing any symptoms of the disease)"* (Kitchin, 2020, p. 2).

Moreover, governments and public authorities began to use digital monitoring tools that were previously used for law enforcement or criminological purposes. Digital tools

used for counterterrorism were applied to track the phones owned by coronavirus carriers. Surveillance camera footage, smartphone location data, and credit card purchase records were used to track positive cases and their contacts (Kitchin, 2020). Furthermore, in tandem with the announcements of the lockdowns to prevent the spread of infections, several states harnessed the use of mobile apps to monitor individuals, identify infected persons and track people's daily interactions. In result, apps seem to be allowed not only the monitoring of one's self for symptoms of illness but also the tracking of the spread of infected people and their encounters (Datta, 2020; Vaidyanathan, 2020). Thanks to apps, citizens were sometimes invited, other times forced to engage in this new form of dataveillance.

Examples of the widespread institutional use of apps for these purposes can be found in various parts of the world. In late March 2020, besides recurring to CCTV technology and drones, public authorities in India pushed into use contact tracing and quarantining apps to monitor citizens. One of these apps, first launched in the region of Karnataka, uses "selfies" for a facial recognition system that surveills quarantined individuals and ensures they adhere to self-isolation (Datta, 2020). Another app gathers a user's identity, tracks people's movement, and checks in real-time if people who have also downloaded the app are in the proximity of the user (Vaidyanathan, 2020). In some places of China, citizens were required to install an app and scan QR codes when accessing public spaces to validate their infection status and get permission to enter (Kitchin, 2020). Bluetooth enabled apps that detect and store information from nearby phones for contact tracing were launched in several countries, such as Singapore (Woo, 2020), telling people to self-isolate if their phone detects an encounter with someone who is later diagnosed.

Although surveillance is a well-known social process in the context of a public health crisis, the current strategy against COVID-19 is posing renewed challenges, mainly due to the monitoring of one's self for symptoms of illness, and the tracking of one's movements. As other surveillance processes embed within everyday life, it certainly affects "power dynamics, institutional practice, and interpersonal relations" (Brown, 2015, p. 1). More important, though, digital data analytics extend the government's powers of surveillance towards intimate life. Hence, they pose new challenges to civil liberties, data privacy and human rights (French & Monahan, 2020; Kitchin, 2020; Lupton 2020; Selwyn & Jandri, 2020; Yu, 2020), while undermining notions about healthy and abiding bodies and ideal selves.

Surveillance in the convergence culture

Surveillance has become a relevant topic in the 21st century. It is the climax of a movement that Lyon, Haggerty, and Ball refer to as "the dominant organising practice of late modernity" (2012, p. 1). It's not only the issues that arise from peoples' lives behind the screens.

Society faces the conundrum of surveillance everywhere, from supermarkets to airports.

The field of surveillance studies (Lyon, Haggerty, & Ball, 2012) has emerged from the intersection of diverse areas of research that had been focusing on topics that ranged from the war on terrorism to urban safety or the use of mobile media. The evolution of technology has played a vital role in the appearance of increasingly pervasive practices, and more complex social and ethical challenges, primarily since the limits of plain sight have been surpassed. However, technology alone, as it usually is the case, does not explain what has changed: other factors, like "changing governmental rationalities, the rise of managerialism, new risks (or perceived dangers), political expediency and public opinion" have to be taken into account (Lyon, Haggerty, & Ball, 2012, p. 2). Nevertheless, privacy defence mechanisms (either legal or technical) seem to fail in catching up with the evolution of technology.

Currently, technology is present in every interstice of people's lives. The new practices, habits and policies that characterise such a mediated society have shaped a new context for discussing surveillance: today, surveillance is more present and, at the same time, frequently more opaque, while it relates to increasingly blurred boundaries (Lyon, Haggerty, & Ball, 2012, p. 2-3).

The decisive change was brought by Web 2.0 and by the democratisation of access to mobile media. This participatory turn changed the way people relate to the internet and become part of the information flow. This process had a relevant impact on the way society sees the limits and dangers of surveillance. The transformation of a previously apathetic figure of the receptor into a producer (what Bruns [2007] called the "produser"), led to the multiplication of content producers that are part of today's participatory culture (Jenkins, Ford, & Green, 2013). In a permanently connected mode, people became avid viewers of other people's lives, exposing their personal information in unprecedented ways that reveal the growing tension between what was previously defined as public and private. However, the penetration of social media platforms in peoples' lives leads to a rather straightforward problem. As Bruno explains (2012, p. 345-346), surveillance becomes an issue when a possible employer uses this information to decide about hiring someone. Yet, less visible processes occur in the information society. The personal use of the internet generates enormous amounts of data that results mainly from the use of web browsers and apps. That way,

> *social, subjective and cultural processes thus become susceptible to daily monitoring. Data that was previously costly and difficult to access can be collected regularly, automatically and remotely. Behavioural, transactional, psychological, social and locational data are captured in real time without the traditional mediation of interviewers and questionnaires* (Bruno, 2012, p. 348).

This is the era of "participatory surveillance" as Bruno (2012) calls it, following Mark Poster's terms (1990). Willfully or not, citizens permanently give personal information to both public and private services. That is why "dataveillance" is such a relevant topic. Despite

concerns with privacy threats and intrusiveness, users authorise the collection of data to obtain personalised services, a better context-sensitive experience or even the apps' plain use. They make a privacy trade-off that takes into consideration the app value, the perceived intrusion and their own privacy concerns (Wottrich, Reijmersdal, & Smit, 2017). However, research supports the general concerns regarding the rationality of such a deal: "smartphone users are often unaware of the data collected by their apps and express surprise and discomfort when they find out" (Almuhimedi, Schaub, Sadeh, Adjerid, Acquisti, Gluck, Cranor, & Agarwal, 2015, p. 787). This is called an information asymmetry (Almuhimedi et al., 2015), with implications for power-relations (Andrejevic, 2002, 2007; Lupton, 2014; Zuroff, 2015).

Digitised quarantine and the *quantified self*

Surveillance dynamics are also seen as processes and practices related to subjectivity-formation in everyday life (Lupton, 2015; Lupton, 2018; French & Monahan, 2020). In the light of this, "digitised quarantine" (Lupton, 2020) may be seen as profoundly productive, generating new habits and behaviours, embodying new identities and selves. Indeed, in response to COVID-19 pandemic, monitoring one's self for symptoms of illness became a common public health recommendation. Demanding people to act responsibly and be committed to self-monitoring configures a pattern against which all individuals are scrutinised.

Following Michel Foucault's work on governmentality (1991), the "modern self" can be understood in an interplay between the processes and practices of the state, on the one hand, and the micromanagement of the self and identity, on the other. To unpack the constructions of responsible subjects mHealth apps convey, we must recognise the effects of the neoliberal transformation of the twentieth century.

The neoliberal drive implied that the management of public health was displaced from the state to the citizens. Personal behaviour and self-responsibility of citizens seem to empty the function of the welfare state. Yet, people voluntarily engaging in self-tracking to promote or manage their health reverberate a different kind of "disruption" of healthcare and public health (Lupton, 2015). Hence, although the idea that one is responsible for regulating one's body precedes our neoliberal era (Sysling, 2002), it seems that participatory surveillance in neoliberal times is changing the body and the self profoundly.

A growing body of scholarship on digital surveillance has been critical on the impact of digital technology, namely considering power relations, inequalities, and commodification through the promotion of voluntary records of individual quantitative data through the 'quantified self' movement (van Dijck, 2014; Lupton, 2018).

Critical research on digital surveillance technologies is concerned with datification being a form of colonizing the life-world (Couldry & Mejias, 2019) as it enables the transformation

of individual and social behaviours into quantified data (Ruckenstein & Pantzar, 2017). Data-driven technologies, within the algorithmic culture of mobile apps and digital platforms, promote the digitization of self-tracking (Lupton, 2016), which facilitates the quantifying of everyday life. Likewise, these technologies promote individualization and self-responsibilisation. The 'quantified self' promotes a "way of co-opting, coordinating and commodifying human activity, enmeshing people in what Foucault (1977) called the microphysics of power, a grid that binds them to an everyday life lived thoughtlessly" (Agger, 2011, p. 122).

The 'quantified self' is anchored to a supposed theory of self-regulation that promotes self-quantification to achieve self-understanding through the analysis of data generated by tracking (Ruckenstein & Pantzar, 2017). Therefore, it presupposes that citizens could take informed actions concerning their body or different experiences.

These mHealth apps launched by governments and public health authorities to digitally monitor positive cases of Covid19 may normalise digital surveillance practices within the promotion of self-tracking as a self-responsibilisation.

Methods

The study aimed to: i) map the first digital public health m-apps created by public authorities (simultaneously available for iOS and Android); ii) critically examine the promotion of self-quantification and self-tracking practices; and iii) identify which digital contact tracing methods are implemented in order to analyse if they promote a normalising of digital surveillance. To achieve these objectives, a search was conducted in the App Store and Google Play during the outbreak, from 1 to 9 April 2020, for apps containing the word "COVID-19". We identified 13 mobile apps that were available in both operating systems and had been created by the initiative of governments and public authorities from different countries. We analysed these apps through the walkthrough method. Taking into account a medium-specific approach (Rogers, 2013) and the affordances of mobile apps (Bucher & Helmond, 2017), we engage directly with the app's interface to analyse functions and features (Light, Burgess, & Duguay, 2018) and digital contact tracing characteristics (Gasser, Ienca, Scheibner, Sleigh, & Vayena, 2020).

The empirical study's first stage was the observation and documentation of the screens, features, and activity flows through the walkthrough method. The second stage focused on analysing the interfaces from a multidimensional approach: apps' functions, features and digital contact tracing characteristics — data type, data source, model of consent (Gasser et al., 2020), and tracing approach (Barrat, Cattuto, Kivelä, Lehmann, & Saramäki, 2020). We move away from questions of representation to consider the extent to which these apps as operational media (Dieter, Gerlitz, Helmond, Tkacz, van der Vlist, & Weltevrede, 2019) are designed to promote and constrain certain behaviours and not merely meanings.

The functions and features dimension considers navigational characteristics and functionalities available through different levels of 'affordances-in-practice' (Costa, 2018), i.e., affordances that depend on their use in a given context or situation.

To identify the digital contact tracing characteristics we defined four variables: i) data type — categorization of data collected into non-identifying personal data, sensitive personal data and non-sensitive personal data; ii) data source — the form of data collection by citizens, Bluetooth, global positioning system (GPS), third party, other; iii) model of consent — the type of agreement for data collection: opt-in consent, opt-out consent and mandatory use (Gasser et al., 2020); iv) typology of digital contact tracing approach: manual contract tracing, surveillance tracing, exposure notification (proximity tracing decentralized), and digitally-sensed proximity network (proximity centralized) (Barrat et al., 2020; Riemer, Ciriello, Peter, & Schlagwein, 2020).

Results and Discussion

Concerning digital contact tracing characteristics, the analysis showed that all the applications are free and follow an opt-in consent (Table 1) — except Coronavirus Australia, which is an information app. Most of the analysed m-apps do not require registration, although it is mandatory in four (STOP COVID19 CAT, Plan Jalisco Covid-19, COVID19 Regione Sardegna, and GVA Coronavirus). However, the record is not directly related to the type of data collected. Results show that there are applications (Bolivia Segura and Asistencia COVID-19) that do not require registration but, with the user's consent through the introduction of the data, will collect sensitive personal data.

Table 1: Walkthrough analysis of digital contact tracing characteristics.

APP	Country	Data Type	Data Source	Registration	Model of Consent	Tracing Approach
Coronavírus — SUS	Brazil	NIPD	Bluetooth	No	Opt-in	Exposure Notification
Bolivia Segura	Bolivia	SPD	GPS	No	Opt-in	N/A*
Canada COVID-19	Canada	NIPD	Citizens	No	Opt-in	N/A*
Asistencia COVID-19	Spain (restricted to some regions)	SPD	GPS	No	Opt-in	N/A*
STOP COVID19 CAT	Spain — Catalonia Government	SPD	GPS	Mandatory	Opt-in	N/A*
Plan Jalisco Covid-19	Mexico (Jalisco State)	SPD	GPS	Mandatory	Opt-in	Surveillance tracing
Covid-19 UAE	UAE	SPD / NIPD	Bluetooth / GPS	Optional	Opt-in	Exposure Notification
COVID19 Regione Sardegna	Italy (Sardinia Government)	SPD	GPS	Mandatory	Opt-in	Surveillance tracing
TreCovid19	Italy (Trento Government)	SPD / NIPD	Citizens	Optional	Opt-in	Surveillance tracing
BC COVID-19 Support	Canada (Province of British Columbia)	NIPD	Citizens	No	Opt-in	N/A*
Coronavirus Australia	Australia	N/A*	N/A*	No	N/A*	N/A*
CoronAPP — Colombia	Colombia	NIPD / SPD	Bluetooth	Optional	Opt-in	Exposure Notification
GVA Coronavirus	Spain (Valencia Government)	SPD	Citizens	Mandatory	Opt-in	Surveillance tracing

* N/A — not available

As Table 1 shows, apps that have optional registration (Covid-19 UAE, TreCovid19, and CoronAPP — Colombia) only collect sensitive personal data upon user registration. The data source of analysed apps is mostly GPS. However, two apps use Bluetooth (Coronavirus — SUS and CoronAPP — Colombia), one has a double combination of data collection via Bluetooth and GPS (Covid-19 UAE) and four request information from citizens (Canada COVID-19, TreCovid19, BC COVID-19 Support, and GVA Coronavirus).

Through the analysis, it was assessed that the digital contact tracing approach of exposure notification relies on non-identifying personal data and collects data through Bluetooth. This is a non-intrusive approach that is based on the collection of epidemiological data without resorting to sensitive personal data. The user enters data related to COVID-19 infection that is counted for the country's statistics and enables an alert for other users through a notification via Bluetooth.

However, most apps (Bolivia Segura, Canada COVID-19, Asistencia COVID-19, STOP COVID19 CAT, BC COVID-19 Support, and Coronavirus Australia) do not indicate their tracing approach. Among these apps, there is one whose registration is mandatory (STOP COVID19 CAT) and sensitive personal data is collected. This type of data is also collected in two apps that collect data through GPS (Bolivia Segura and Asistencia COVID-19) without information concerning how data will be used. This lack of explanation about the use of user data, whether when requesting non-identifying personal data or sensitive personal data, is worrying because it normalises data collection as a common practice.

Features and functions available on m-apps were analysed from an 'affordances-in-practice' (Costa, 2018) approach. Depending on the context, on the practices through which they are enacted and on the specific digital-material entanglement that is thus configured, affordances variously operate by demanding, requesting, allowing, encouraging or discouraging users' practices (Davis & Chouinard, 2016). Table 2 presents the results of features and functions analysis by "engaging directly with an app's interface to examine its technological mechanisms and embedded cultural references to understand how it guides users and shapes their experiences" (Light, Burgess, & Duguay, 2018, p. 882).

Table 2: Walkthrough analysis of navigational features and functions.

APP	Country	Functions and Features
Coronavírus — SUS	Brazil	Users are guided through a simple menu and on-screen navigation buttons focus on alerts, news and tips. When opening the app, authorization to send notifications is requested; the user can allow or disallow; it is not possible to choose the type of notification. Exposure is included in these notifications.
Bolivia Segura	Bolivia	Users are guided through an on-screen navigation buttons menu referring to information and prevention, official data, news and self-tracking data. When opening the app, authorization to send notifications is requested; the user can allow or disallow, it is not possible to choose the type of notification.
Canada COVID-19	Canada	On the initial screen users are informed of the app's features: the latest updates, trusted resources, and personalized symptom tracking. To advance, users must enable the "start" button. On the second screen, it is mandatory to choose the province/territory. Before using the app, the user can select three options or skip: assess her / his risk, resources about COVID-19 and self-isolation, and the possibility to activate notifications and receive official information. Users are guided through an on-screen navigation buttons menu referring to stats, updates, resources, and self-check (self-assessment and symptom tracker). A dropdown menu presents settings and a "wall of kindness" with acts of kindness happening across Canada.
Asistencia COVID-19	Spain (restricted to some regions)	Users are informed on the first screen of the app's features: instructions and recommendations based on their health situation, health self-assessment, help healthcare professionals, self-assessment every 12h. To advance, users must enable the "start" button. On the second screen, it is mandatory to choose the province/territory. The third screen asks for the mobile number to go forward. App's features allow users to perform self-diagnostic, access prevention and care recommendations, and updated information.
STOP COVID19 CAT	Spain (Catalonia Government)	User's consent and acceptance of conditions and privacy policy of the app is asked on the first screen. App asks for the Personal Identification Code from the health card. On the start screen, there will be the main action button and, depending on the user, there may be secondary actions buttons that will be enabled by clicking next. Start screen displays a self-assessment test. Secondary screens are history, profile and QR code reader.
Plan Jalisco Covid-19	Mexico (Jalisco State)	The first screen asks for mandatory registration. Users are guided through a dropdown menu providing tools for self-isolation, information on Covid-19 in Jalisco, and a self-monitoring test.
Covid-19 UAE	UAE	The first screen asks for optional registration. App asks for permission to use GPS. Users that complete registration and enable location detection can carry out self-monitoring actions. Users are guided through an on-screen navigation buttons menu referring to real-time data (tests, cases, deaths and recoveries), self-assessment tools, resources on preventive measures, news/announcements, psychological advice, and a map with the nearest diagnostic centres.

COVID19 Regione Sardegna	Italy (Sardinia Government)	Upon opening the app, authorization to send notifications is requested; the user can allow or disallow, it is not possible to choose the type of notification. The first screen asks for mandatory registration. Users are guided through a menu that allows registration of stays (for travellers), voluntary travel mode, registrations and movements, and settings.
TreCovid19	Italy (Trento Government)	Users are guided through a simple menu and on-screen navigation buttons focus on data, information on COVID-19 and a restricted area to patients in home isolation or under health surveillance.
BC COVID-19 Support	Canada (Province of British Columbia)	Users are informed on the first screen of anonymous use of information and app's features: the latest updates and recommendations from experts. To advance, users must enable the "start" button. The second screen asks for the user's current travel status. Before using the app, the user can select three options or skip: assess her / his risk, resources about COVID-19 and receive the latest updates. Users are guided through an on-screen navigation buttons menu referring to stats, updates, resources, and self-check (self-assessment and symptom tracker). A header menu presents a self-isolation plan for travellers and settings.
Coronavirus Australia	Australia	Users are guided through a simple menu and on-screen navigation buttons focus on numbers, advice, health care services, and other related content. The homepage provides information on a self-tracking app (COVIDSafe app), respiratory clinics or testing centres, restrictions and travel, and news.
CoronAPP — Colombia	Colombia	Upon opening the app, authorization to send notifications is requested; the user can allow, allow for one time or disallow. The first screen asks for optional registration. Users that complete registration and enable location detection can carry out self-monitoring actions. Users are guided through a dropdown menu with information on the app, phone numbers for health and help services, health centres, and data on Coronavirus in Colombia. This information is simplified in a footer graphic on-screen navigation menu.
GVA Coronavirus	Spain (Valencia Government)	When opening the app, users should choose the language. The second screen asks for a personal identification number and date of birth. The app is directly linked to the Valencia health service. It offers the possibility to a person who has been in close contact with a positive case of COVID to fill out a daily self-report to indicate if she/he presents symptoms throughout the day. The self-report option will be available in the app after the first telephone contact with the family doctor and only if the user agrees to follow-up through this system. Users are guided through on-screen navigation buttons that allow users to insert their direct contact, self-monitoring, information on COVID19 and FAQS.

Functions and features of the analysed apps are activated with on-screen navigation buttons. The navigation meets criteria of accessibility (interface without obstacles), functionality (utility of the function for the tasks), and usability (maximising the system's resources concerning effectiveness, efficiency, and satisfaction of use) (Amaral, 2016). Although the navigation is simple, user experience is focused on pre-established features that structure (and collect) users' data. Therefore, technology is intrusive despite surveillance being presented as a self-tracking function in normative models of citizen accountability. Anchored to the 'quantified self' metaphor, these normative models present different affordances for demanding, requesting, allowing, encouraging or discouraging users' practices (Davis & Chouinard, 2016). By emphasising wellbeing, apps may encourage or discourage behaviours under a normalisation of digital surveillance. Apps also afford requests (users engagement), demands (registration), refuse (by making some functions not available for users that are not registered, for instance) and also allow (navigating in a neutral structure, for example). The interrelation of affordances mechanisms in functions and features of analysed apps enhances different interaction dynamics between users and artefacts. Therefore, apps afford in their sociostructural environments concerning the context of use.

Conclusion

Mandatory quarantine and social isolation to limit the spread of the COVID-19 virus (SARS-CoV-2) are two well-known measures to manage populations and sick people in an epidemic crisis. Over time, governments and public health authorities have also used different kinds of technological tools to inform and control citizens and risk groups in response to public health threats. As we say, what seems new since the COVID-19 pandemic has emerged is the role that digital technologies have been playing. Mobile health apps, in particular, are harnessed by public authorities to favour the self-monitoring and self-tracking of individuals' health, movements, and encounters. Despite concerns about the limits of privacy and surveillance, they seem to be unifying the efforts and worries of law enforcement and public citizens. Nevertheless, what our analysis shows is that mobile applications are, above all, disciplinary mechanisms at the service of states.

Recurring to the walkthrough method, we analysed 13 m-apps from the initiative of public authorities from different countries, which are, firstly, statistical tools that allow the collection of data for policy government. At the same time, they are instruments that normalise the practices of self-monitoring and self-surveillance of human bodies, concealing the fact that they are intrusive technologies. All apps are based on opt-in consent, although only a few demand it directly. In these cases, consent is required to use the app. The same happens in cases where access to GPS/Bluetooth or notifications is requested. Without these features,

the use of apps does not make sense since they do not detect cases of exposure, do not collect data and/or do not alert users of exposure to contagion. Hence, while launched as individual and collective security mechanisms, they are powerful tools that promote digital surveillance at different levels: from mobile phone tracking to sensitive personal data collection. Indeed, through m-apps public authorities are able to map personal information, movements and meetings between citizens.

Also significant is that the majority of the 13 m-apps are absent in relation to what governments and public health authorities do with personal data. Some apps request access to truly sensitive personal data, such as health security numbers, travel tickets, information about contacts, details of individual health state. Others, besides requesting sensitive data, are based on a surveillance tracing approach and ask people to repeatedly enter personal data (in some cases, twice a day).

Furthermore, we also saw how these COVID-19 self-tracking apps encouraged people to think about their bodies and their selves through numbers and wellbeing resonances. They promote the 'quantified self', giving way, in Lupton's words, to "an algorithmic subjectivity, in which the body and its health states, functions and activities are portrayed and understood predominantly via quantified calculations, predictions and comparisons" (2015, p. 450).

At a time when we are witnessing a new wave of the COVID-19 pandemic, with governments around the world harnessing m-apps to control the spread of the disease, including in Portugal, we must surely continue to investigate the novel state usages of these digital technologies and problematise the challenges they pose to concepts of self, identity, privacy, and embodiment.

References

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., ... & Agarwal, Y. (2015). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In Proceedings of the 33rd annual ACM conference on human factors in computing systems (pp. 787-796).

Amaral, I. (2016). Modelo Circular da interação: design da interação na esfera do ciberjornalismo. *Observatório (OBS*)*, 10(4), 01–21.

Andrejevic, M. (2007). Surveillance in the Digital Enclosure. *Communication Review, 10*, 295-317. doi: https://doi.org/10.1080/10714420701715365

Andrejevic, M. (2002). The Work of Being Watched: Interactive Media and the Exploitation of Self-disclosure. *Critical Studies in Media Communication, 19*(2), 230-48. doi: https://doi.org/10.1080/07393180216561

Barrat, A., Cattuto, C., Kivelä, M., Lehmann, S., & Saramäki, J. (2020). Effect of manual and digital contact tracing on COVID-19 outbreaks: a study on empirical contact data. medRxiv. doi: https://doi.org/10.1101/2020.07.24.20159947

Bucher, T., & Helmond, A. (2017). The affordances of social media platforms. In J. Burgess, A. Marwick, & T. Poell (Eds.), *The SAGE handbook of social media* (223-253). Sage Publications.

Bruno, F. (2012). Surveillance and participation on web 2.0. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.) Routledge Handbook of Surveillance Studies (pp. 343-351). Oxon: Routledge.

Bruns, A. (2007). Produsage. In Proceedings of the 6th ACM SIGCHI Conference on Creativity & Cognition (pp. 99-106).

Castells, M. (1996). *The Rise of the Network Society*. Cambridge, MA, USA: Blackwell Publishers, Inc.

Costa, E. (2018). Affordances-in-practice: An ethnographic critique of social media logic and context collapse. *New Media & Society, 20*(10), 3641-3656. doi: https://doi.org/10.1177/1461444818756290

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media, 20*(4), 336-349. doi: https://doi.org/10.1177/1527476418796632

Datta, A. (2020). Self(ie)-governance: Technologies of intimate surveillance in India under COVID-19. *Dialogues in Human Geography, 10*(2), 234-237. doi: https://doi.org/10.1177/2043820620929797

Dieter, M., Gerlitz, C., Helmond, A., Tkacz, N., van der Vlist, F. N., & Weltevrede, E. (2019). Multi-Situated App Studies: Methods and Propositions. *Social Media+ Society*, 5(2). doi: https://doi.org/10.1177/2056305119846486

Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon and P. Miller (Eds.), *The Foucault Effect: Studies in Governmentality* (pp. 87-104). Hemel Hempstead: Harvester Wheatsheaf.

French, M., & Monahan, T. (2020). Dis-ease surveillance: how might surveillance studies address COVID-19? *Surveillance & Society, 18*(1), 1-11. doi: https://doi.org/10.24908/ss.v18i1.13985

Gao, G., & Sai, L. (2020). Towards a 'virtual' world: social isolation and struggles during the COVID-19 pandemic as single women living alone. *Gender, Work & Organization*. doi: https://doi.org/10.1111/gwao.12468

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020). Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. *The Lancet Digital Health*. doi: https://doi.org/10.1016/S2589-7500(20)30137-0

Hebblethwaite, S., Young, L., & Martin Rubio, T. (2020). Pandemic precarity: aging and social engagement. *Leisure Sciences*. doi: https://doi.org/10.1080/01490400.2020.1773998

Hepp, A., Breiter, A., & Hasebrink, U. (2018). *Communicative figurations: Transforming communications in times of deep mediatization*. Springer Nature.

Jenkins, H. Ford, S., & Green, J. (2013). Spreadable media: Creating value and meaning in a networked culture. New York: New York University.

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

Kwok, H. (2020). Beyond the anti-racist reason: a postcolonial perspective on pandemic politics. *Health Sociology Review, 29*(2), 122-130. doi: https://doi.org/10.1080/14461242.2020.1785320

Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. New media & society, 20(3), 881-900. doi: https://doi.org/10.1177/1461444816675438

Lyon, D, Haggerty, K. D., & Ball, K. (2012). Introducing Surveillance Studies. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.) Routledge Handbook of Surveillance Studies (pp. 1-12). Oxon: Routledge.

Logie, C. H., & Turan, J. M. (2020). How Do We Balance Tensions Between COVID-19 Public Health Responses and Stigma Mitigation? Learning from HIV Research. *AIDS and Behavior*. doi: https://doi.org/10.1007/s10461-020-02856-8

Lupton, D. (2018). *Digital Health*. London, New York: Routledge.

Lupton, D. (2020). Digitised quarantine: a new form of health dataveillance. https://simplysociology.wordpress.com/2020/02/27/digitised-quarantine-a-new-form-of-health-dataveillance/ 2020 [accessed May 5, 2020].

Lupton, D. (2015). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. Culture, health & sexuality, 17(4), 440-453. doi: 10.1080/13691058.2014.920528

Lupton, D. (2016). *The quantified self*. Cambridge: Polity Press.

Ohme, J., Abeele, M. M. V., Van Gaeveren, K., Durnez, W., & De Marez, L. (2020). Staying Informed and Bridging "Social Distance": Smartphone News Use and Mobile Messaging Behaviors of Flemish Adults during the First Weeks of the COVID-19 Pandemic. *Socius: Sociological Research for a Dynamic World*, 6, 1–14.

Poster, M. (1990). The mode of information: Poststructuralism and social context. Cambridge: Polity Press.

Rahman, S. Y. (2020). 'Social distancing' during COVID-19: the metaphors and politics of pandemic response in India. *Health Sociology Review,* 29(2), 131-139. doi: https://doi.org/10.1080/14461242.2020.1790404

Riemer, K., Ciriello, R., Peter, S., & Schlagwein, D. (2020). Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level. *European Journal of Information Systems*, 1-15. doi: https://doi.org/10.1080/0960085X.2020.1819898

Rogers, R. (2013). *Digital methods*. MIT press.

Ruckenstein, M., & Pantzar, M. (2017). Beyond the quantified self: Thematic exploration of a dataistic paradigm. *New Media & Society, 19*(3), 401-418. doi: https://doi.org/10.1177/1461444815609081

Selwyn, N., & Jandrić, P. (2020). Postdigital living in the age of Covid-19: unsettling what we see as possible. *Postdigital Science and Education*. doi: https://doi.org/10.1007/s42438-020-00166-9

Simões, R. B., & Amaral, I. (2021). Sexuality and self-tracking apps: Reshaping gender relations and sexual and reproductive practices. In E. Rees (Org.). *The Routledge Companion to Gender, Sexuality and Culture*. Routledge. [in press]

Sysling, F. (2020). Measurement, self-tracking and the history of science: An introduction. *History of Science*, 58(2), 103–116. doi: https://doi.org/10.1177/0073275319865830

Teräs, M., Suoranta, J., Teräs, H., & Curcher, M. (2020). Post-Covid-19 education and education technology 'solutionism': a seller's market. *Postdigit Sci Educ 2, 863–878*. doi: https://doi.org/10.1007/s42438-020-00164-x

Utoft, E. H. (2020). 'All the single ladies' as the ideal academic during times of COVID-19? *Gender, Work & Organization*. DOI: http://doi.org/10.1111/gwao.12478

Vaidyanathan, G. (2020). Aarogya Setu: Major Surveillance, Few Safeguards In Modi Govt COVID Tracking App. *Huffpost*. https://www.huffingtonpost.in/entry/aarogya-setu-surveillance-covid-tracking-app_in_5e8d6e26c5b6e1d10a6bdea6?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACal3q2YUpJxRs4DUdGtsEwYvo17oZSni3DLbYwl7ErQnJ5CUgw_VMfx9u0C4G6aHfLZT4P7sgQTa6AD1h5eys_CVcKiSVZcT8D-ohb4jgJP54FmSV_r5_LgLxVMcq7Q0CU2izQFu-t5ElcfmFXDbqZWy8Dve1ulUnuPHmsH_v7D [accessed May 5, 2020].

Williamson, B., Eynon, R., & Potter, J. (2020). Pandemic politics, pedagogies and practices: digital technologies and distance education during the coronavirus emergency. *Learning, Media and Technology, 45*(2), 107-114. doi: https://doi.org/10.1080/17439884.2020.1761641

Woo, J. J. (2020). Policy capacity and Singapore's response to the COVID-19 pandemic. *Policy and Society, 39*(3), 345-362. doi: http://doi.org 10.1080/14494035.2020.1783789

Wottrich, V. M., van Reijmersdal, E., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems, 106*, 44-52. doi: https://doi.org/10.1016/j.dss.2017.12.003

World Health Organization (WHO) (2020). Director-General's Opening Remarks at the Media Briefing on COVID-19—11 March 2020, WHO Director General, Speeches. Geneva https://www.who.int/dg/speeches/detail/who-directorgeneral-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 [accessed May 5, 2020].

Yu, A. (2020). Digital surveillance in post-coronavirus China: A feminist view on the price we pay. *Gender, Work & Organization*. doi: https://doi.org/10.1111/gwao.12471

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89. doi: https://doi.org/10.1057/jit.2015.5