The International Journal of Human Rights

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/fjhr20

Health, privacy and liberty: a call for digital governance during (and after) the pandemic

Vera Lúcia Raposo

To cite this article: Vera Lúcia Raposo (2023) Health, privacy and liberty: a call for digital governance during (and after) the pandemic, The International Journal of Human Rights, 27:3, 529-551, DOI: 10.1080/13642987.2022.2132234

To link to this article: https://doi.org/10.1080/13642987.2022.2132234

Published online: 14 Oct 2022.

THE INTERNATIONAL JOURNAL OF HUMAN RIGHTS
2023, VOL. 27, NO. 3, 529–551
https://doi.org/10.1080/13642987.2022.2132234

Routledge
Taylor & Francis Group

Health, privacy and liberty: a call for digital governance during (and after) the pandemic

Vera Lúcia Raposo

Nova School of Law, Nova University of Lisbon, Lisbon, Portugal

ABSTRACT

The COVID-19 pandemic has boosted the development and use of technology by increasing the use of previously existing technological resources, such as maps identifying population movements; assigning new uses to previously existing technological mechanisms, such as the use of facial recognition for monitoring infected people; and encouraging the development of new technologies, such as apps that ascribe risk codes to citizens. Without these digital measures, the pandemic would probably continue to expand, or, alternatively, entire populations would have to be quarantined for months (or even years), with significant consequences arising from either scenario. Technologies provide tools to avoid those scenarios. However, digital measures come at a price to our rights, namely our rights to privacy and liberty. Precautions and limitations ought to be imposed on the use of these technologies, forming a code of digital governance for COVID-19.

ARTICLE HISTORY
Received 9 March 2021
Accepted 26 September 2022

KEYWORDS
COVID-19; technology; surveillance; privacy; rights and liberties; digital governance

1. Introduction

Technological tools have been widely used by several governments to handle the COVID-19 pandemic.[1] The tasks that technologies are performing in the health crisis are not completely novel. Many of the tasks considered necessary to handle a pandemic – such as contact tracing and monitoring sick and isolated[2] or quarantined people – used to be carried out by human operators. Technologies allow these tasks to be performed faster and more efficiently. Thus, they have been integrated into health policies to combat the spread of the virus.[3]

Many of these digital tools impose limitations on individual rights and liberties. Under normal circumstances, governments (at least, liberal democracies) would most likely not be allowed to use them.[4] In this respect, the pandemic has been a game changer.[5]

This paper begins by highlighting the main digital intrusions taking place during the COVID-19 pandemic under the designation 'pandemic digital measures' (PDMs).[6] It is not possible to discuss every kind of digital tool in detail; this analysis covers the ones most frequently used.

CONTACT Vera Lúcia Raposo vera.lucia.raposo@novalaw.unl.pt Nova School of Law, Nova University, Portugal

Subsequently, the paper analyses the relationship between fundamental rights and PDMs. The use of technology to combat COVID-19 is concerning from the perspective of fundamental rights, especially privacy, civil liberties (e.g. freedom of movement and of association) and equality.[7] Therefore, PDMs cannot be accepted without further discussion.

The paper highlights an underlying conflict: on the one hand, technology is posing major threats to fundamental rights; on the other hand, without technology, the entire population risks undergoing an extended lockdown, with various consequences for rights and liberties entailed by long-lasting quarantines.[8] Although limits must be imposed on PDMs, technology is an essential non-pharmaceutical measure (alongside other measures) to handle the new coronavirus.

Finally, based on the pros and cons identified, the paper lists the requirements to be imposed on PDMs in light of the applicable laws in Europe, namely those issued by the European Union and the European Council. These requirements form a code of digital governance to be respected both during and after the pandemic.

2. Technologies used in the COVID-19 pandemic

The defining feature of a pandemic caused by a virus is that it spreads quickly. To stop a pandemic, it is crucial to know where the virus is and prevent it from spreading any further. Unfortunately, this requires information about people's whereabouts and the power to restrict their freedom of movement.[9] Technology is more effective in restricting movement than are police, who must manually check the activities of individuals.[10] However, whether the use of technology is less stringent than the use of police remains to be seen.

2.1. Mobile applications

Mobile applications (apps) are amongst the most used digital tools in the fight against COVID-19. Of their many functions, contact tracing is the most frequently used. Contact tracing is a well-known method of handling infectious diseases. Traditionally performed by human operators, it is now mostly carried out using technology, leading to the development of digital contact tracing.[11] The aim of digital contact tracing is to measure the spatial proximity of users and, based on the resulting data, inform people who have been in contact with an infected individual and provide information and guidance on how they can protect themselves and others, such as recommending testing and/or quarantine.[12]

Digital contact tracing takes different forms.[13] It can operate via Bluetooth or GPS;[14] it can provide information on proximity or location;[15] data can be stored in the user's personal device (decentralised system) or in a central database (centralised system);[16] and it can be voluntary or mandatory.[17] These features in turn determine the kind of problems it raises and the level of acceptance it gains in its different versions.[18]

A slightly different modality of contract tracing uses QR codes scanned by apps. In China, citizens are asked to scan QR codes affixed in venues with a WeChat app.[19] If someone tests positive for COVID-19, people who have been in the same places will be notified.

New Zealand, Thailand and Taiwan have apps that transmit users' locations and enable the authorities to check whether quarantines and isolations are being violated.[20]

The Taiwanese location tracking system sends an alert to authorities if an infected person breaches isolation by moving away from a so-called 'electronic fence'.[21] To ensure that people do not avoid enforcement by leaving their phones at home, the government requires them to answer an automated phone call twice a day.[22] In Poland, electronic fences are imposed by mandatory selfies that the quarantined or isolated person must send to health authorities.[23]

A deeply controversial form of technology for managing COVID-19 is an app that assigns users a risk code based on information that they provide, together with other data such as the places they have visited, and the amount of time spent in each place. A paradigmatic example of this is the Chinese Alipay app, which runs on Alipay and WeChat.[24] The Alipay Health Code system uses location data and other health data to assign each person a colour code according to the level of infectious risk they pose. This colour code determines the person's freedom of movement:[25] red entails a 14-day quarantine, yellow entails a 7-day quarantine and green allows free movement. An individual's code must be shown and checked at all services.[26]

2.2. Web-based maps with aggregated data

In California, the authorities use maps provided by Facebook to check social distancing.[27] The use of information in this way is not entirely new, as Facebook maps were previously used to track population movements in the event of natural disasters. Similarly, Belgium's Data Taskforce Against Corona uses telecommunication and epidemiological data to create maps showing the spread of the virus and identifying high-risk zones.[28]

With these maps, compiled or summarised individual data (aggregated data) are typically used to identify trends or conduct statistical and comparative studies. The data are anonymised, i.e. the individuals concerned cannot be identified; thus, there are relatively minor implications for privacy.

2.3. Wearable devices

Under certain conditions, several jurisdictions impose wearable devices on their citizens, such as electronic bracelets or ankle locators. One of the functions of these devices is to control compliance with quarantines or isolations. The devices share the user's locations with local authorities by GPS or Bluetooth in connection to a mobile phone app, thus alerting authorities whenever a person leaves a permitted perimeter.[29] Wearable devices also have other functions. For example, the wristband device used in Antwerp, Belgium aims to enforce social distancing by ensuring that workers keep a safe distance between them, while also enabling contact tracing if necessary.[30] A trend is emerging in using wearable devices to check symptoms. These devices collect and transmit the user's biometric data to the health authorities[31] and can even analyse and interpret the data themselves. The device provides the user with a diagnosis and will recommend or impose isolation if the test is positive for COVID-19.[32] In a study taking place in Liechtenstein, volunteers wear bracelets that detect their symptoms (e.g. body temperature) and alert authorities to cases of infection even before the individuals themselves are aware of it.[33]

2.4. Facial recognition

In some countries, quarantine and isolation are monitored using facial recognition cameras. This is the strategy used in Russia and China,[34] and other countries may follow this path to control people's movement during the pandemic.[35]

FRT works with facial images, that is, biometric data,[36] a type of data included in the scope of the GDPR.[37] The main challenge of biometric data is that they are almost impossible to change in case the person is tracked. Unlike a password, which is easily changed, our faces and our eyes remain untouched all our life.[38] This particularity also makes biometric data one of the most effective ways of recognising and identifying individuals.

Facial recognition was expressly mentioned in the European Commission's White Paper on Artificial Intelligence released in 2020.[39] The Commission is well aware of the risks posed by facial recognition technology and recommends restrictions on its use. However, the white paper does not go much further than to suggest 'appropriate' or 'adequate' safeguards. The understanding of these adjectives will obviously vary among the member states, which may create some disparities between the solutions they put in place.

3. The threat to fundamental rights

3.1. Privacy and personal data protection

Privacy is one of the concerns raised about the use of PDMs[40] – not only traditional privacy but, more importantly, its modern version, the right to data protection.[41] In the last decade, there has been a vertiginous move towards the protection of privacy.[42] In Europe alone, in addition to the protections afforded by each national jurisdiction, privacy is protected by European law (such as the General Data Protection Regulation,[43] the e-Privacy Directive,[44] and the Charter of Fundamental Rights)[45] and by the European Convention of Human Rights.[46]

In recent years, privacy concerns have taken centre stage. The pandemic has created a kind of contra-movement to this trend, making citizens more willing to accept State intrusions in the name of public health.[47] Privacy concerns did not disappear, but people became more willing to accept some digital intrusions on privacy, which eventually will perdure after the pandemic.[48] PDMs were not peacefully accepted by the community, but one may wonder if they would have even been accepted at all if there hadn't been a pandemic. Public health is a powerful justification for many controversial measures. Surveillance has invaded our private spheres and collected our private data. The government, or some entity acting on its behalf, knows where we are and where we have been. Using this data (big data), it can even predict where we intend to go. The 'system' knows which people we connect with, our habits and our secrets. Moreover, all of this information can be (and sometimes is) disclosed to the police or even to the community at large. South Korea relies on cameras and credit card activity to track location. The locations of infected individuals are publicly disclosed without identifying them, although features such as age, nationality, and gender, as well as more private information such as overnight stays at motels, are published,[49] potentially revealing an individual's identity.

A striking example of PDMs being used to invade people's rights and the resulting pushback from courts took place in Israel. During the outbreak, the Israeli government seized access to the cell phone locations of infected individuals for the purpose of contact tracing. The Israeli executive branch used national security laws as the legal basis for such measures and mobilised the Israeli Intelligence Service (Shin Bet) to carry out this work. The Ministry of Health informed the Shin Bet of the patients who had tested positive for COVID-19, and the Shin Bet informed the Ministry of everyone who had come into contact with those patients in the previous 15 days.[50] The identified individuals then received a message to stay at home. In a notable judgment, the High Court of Justice[51] ruled that this practice 'severely violates the constitutional right to privacy'.[52]

Less controversial is the Singaporean app TraceTogether, which has aroused interest in other countries because it is totally voluntary and thus presents a low level of threat to fundamental rights.[53] The app does not collect location data, but only information on the proximity,[54] time and duration of contact with other app users. These data are encrypted and stored on the app users' devices, but access can be provided to public authorities, so it combines features of both the centralised and decentralised models. From a privacy perspective, the decentralised model is preferable, as the data are not sent to a centralised source.

Facial recognition has also raised issues in this regard, as it deals with particularly sensitive private data.[55] Therefore, Article 9 of the GDPR imposes special requirements on the use of 'biometric data for the purpose of uniquely identifying a natural person'. Given the sensitive nature of this technology, a prior data protection impact assessment (Article 35 GDPR) is required.

With risk codes, privacy concerns arise from the fact that the user must show the code to several different people during the day, thus sharing their travel history and other personal details. More concerning still is a recently introduced feature of the Alipay app that allows third parties to check someone's code by entering their identity number.[56]

Most intrusions on privacy happening during the pandemic are particularly objectionable because they take place in scenarios in which people have a 'reasonable expectation of privacy' (even though I assume that many are more tolerant of such intrusions because they came under the label of public health). This concept has been used by the ECtHR[57] to refer to situations where people do not believe themselves to be in the public sphere and thus do not expect to be 'watched' (in the sense of having their movements and personal data collected). Consider the example of home surveillance. There is a reasonable expectation of privacy at home, by definition a private place, and this expectation is violated when the government installs cameras in a person's house. This expectation also exists (albeit to a lesser degree) when a person goes to the supermarket or for a walk in the park, as the mere fact that the person is in the outside world should not open the door to this kind of surveillance.[58]

Tracking people certainly entails an intrusion on privacy, but the degree of intrusion does not differ hugely from what is already experienced in day-to-day life, sometimes also violating 'reasonable expectations of privacy'. The same type of information is already being collected by electronic health records,[59] social media,[60] search engines[61] and apps that collect users' locations and other personal information.[62] Privacy breaches are certainly a problem when technology is used in an irregular manner,[63] but this is a general problem in the digital world,[64] not a novelty brought by PDMs.

3.2. Personal freedoms

PDMs also intrude on personal freedoms, specifically individuals' ability to make free decisions on routine aspects of their lives, such as whether to use smartphones and wearable devices, which can be used as tracking mechanisms, to establish location (some contact tracing apps collect people's location,[65] which is a sensitive data under the GDPR) and even to identify COVID-19 symptoms.[66] PDMs can also condition decisions on where to go (freedom of movement) and whom to meet (freedom of assembly), as individuals might fear locations where the risk of infection is high, or might avoid getting in close contact with other people.[67] For instance, some PDMs work with colour codes, which prevent people from visiting certain venues (including the workplace); the so-called 'health fences' inhibit free movement; facial recognition cameras track a person's movement around the city;[68] and information provided by Web-based maps can lead to the closure of certain regions or districts.

Even before the pandemic, wearable devices were used to scrutinise people's movements,[69] but in the past they targeted people who had been convicted of crimes and whose alternative was imprisonment. While it is true that some people with pandemic-related wearable devices have infringed quarantine or isolation rules, it remains difficult to view them as criminals,[70] as the use of criminal law to enforce public health is controversial.[71]

Significant concerns involving PDMs are the possibility of algorithmic errors and the consequent peril of 'mislabelling' someone, restricting his/her liberty without any sound justification.[72] The health risk codes used in China are supposedly assigned according to objective criteria such as travel history, symptoms and previous contacts with people who have tested positive. However, there have been complaints about the coding mechanism in China, as it is unclear which criteria are used to merit a given code.[73]

Indirectly, other liberties may be affected. It has been reported that the information registered in the Alipay Health Code – personal information, recent travel data and health status – is shared with the police, who have been using it for several illegitimate purposes, such as to repress freedom of religion.[74]

Violations of freedom of expression have also been pointed out by the Human Rights Council of the UN[75] and the European Union Agency for Fundamental Rights.[76] When people know they are being watched, they change their behaviour and the way they express themselves, constituting an infringement on their freedom of expression.

3.3. Discrimination

Some of these technologies are not entirely reliable and the interpretation of their results is frequently subject to prejudice. These problems are particularly notable in facial recognition technologies. Even in normal circumstances, the use of this technology raises issues of accuracy. According to the European Union Agency for Fundamental Rights (FRA), 'an algorithm never returns a definitive result, but only probabilities'.[77] The use of face masks, which hide noses and mouths, further weakens its accuracy.[78] The reliability of this technology has been particularly questioned because it is biased against some ethnic groups, as demonstrated by a recent study by the US National Institute of Standards and Technology.[79] This technology learns to 'recognize' people with

the photos used to train it, and the more the number of photos with individuals from a given ethnic group or a given gender, the more accurate will be the results regarding those individuals. In contrast, if a certain group is underrepresented in such images, chances are people from that group will be wrongly 'identified'. For instance, many facial recognition systems are trained predominately with photos from white males, thus leading to higher percentages of misdetection of anyone that is not white or not male.[80] Social and racial bias, in turn, can undermine the chance to judicially contest the facial recognition result, impairing due process rights, because the individuals who are suffering negative consequences due to misidentification (for instance, being sanctioned for allegedly having disregarded the isolation order) are also the ones who face greater obstacles to activate administrative remedies or access courts to correct the error.

Problems also arise when a particular group of people is targeted as being infected. Geolocalisation makes it possible to know a person's location at a given time. In Seoul, several infections were detected in LGBTQ nightclubs and bars, but when public health authorities sought to contact people at risk so they could be tested, many of them were unwilling to come forward voluntarily. As the geolocalisation system very precisely identified the exact spot of the infection – the LGBTQ nightclubs – the individuals at stake knew that they would be immediately correlated with the LGBTQ way of life and feared they would be stigmatised due to their sexual orientation.[81]

4. PDMs: a threat to fundamental rights or a mechanism to safeguard fundamental rights?

4.1. PDMs and public health

PDMs have a very clear surveillance aim, but surveillance is not – nor should it be – an end in itself. Instead, it should serve other values. The dual aims of public health and surveillance have the capacity to support each other. Suppose the data reveal that in a given community or neighbourhood, the level of compliance with containment measures is low, and people are organising parties in violation of public orders, rapidly leading to the spread of the virus. Based on this information, the authorities can implement more restrictive measures (e.g. quarantines, restricted access to particular places, and/or bans on gatherings) and use technology to enforce them more efficiently than merely health authorities or police force, thus reducing the number of new infections. This is a clear example of public health surveillance. This model of surveillance keeps an eye on you, in the sense that it not only tracks but also takes care of you.

During the pandemic, PDMs have been used to plan better public health measures, for instance by identifying the places people visit most frequently and the reasons they go there. This allows mechanisms to be created to better protect people in those places (e.g. by providing free masks), to check whether social distancing is being respected, to reduce crowds (e.g. by restricting access to those locations) or even remove the need to go to such places (e.g. providing the same service in a different and more secure location).

This is not to say that PDMs are a miraculous solution to the pandemic or that PDMs alone can do the job. However, PDMs can be an extremely valuable tool for containing

the virus when used in conjunction with other non-pharmaceutical measures (e.g. face masks, hand sanitiser, massive testing, social distancing) and pharmaceutical measures.

4.2. Fundamental rights and the alternatives to PDMs

The assessment of how PDMs affect fundamental rights must also have into consideration how the corresponding alternative also affects those rights.[82] In the absence of PDMs there are two main alternatives: either strict lockdowns and massive quarantines or letting people get naturally infected.

The first – widespread quarantines and strict lockdowns[83] – was implemented in some liberal democracies (Italy, for instance). However, the paradigmatic model of such a strategy comes from a non-liberal democracy, China, with consequences that have been repeatedly and harshly criticised by scholars.[84] The loopholes of such a strategy soon became clear. To begin with, the practical issue of compliance: as referred to by the Imperial College study (the one that dictated the change of heart of the UK Executive in its pandemic policy), massive quarantines can only lead to positive results if maintained for a long period of time. However, the more they drag, the less they are complied with,[85] mostly due to their phycological effects on humans.[86] Not only physical liberty is affected, but also economic and social rights.[87] Massive quarantines are especially severe for manual labourers, for whom telework is not an option; many have lost their jobs and their livelihoods. Most of them do not have an economic reserve to rely on.[88] Quarantined families are deprived of income, they might lose their houses and even starve.[89] The effects of the lockdown will be felt in the long term, with families losing their homes and their access to health care and education. The livelihoods of entire populations are at stake. Quarantines can result (and have resulted) in severe economic consequences, especially for the poorer and more fragile members of society. They lead to food deprivation[90] financial hardship, disruption of education (children are deprived of education, especially the ones without digital resources to receive at distance education)[91] and eventual annihilation of professional prospects for today's youth, not to mention serious effects on mental health.[92] These consequences combined are the perfect setting for a global disaster.[93]

Therefore, and despite the initial benefits of this strategy,[94] authorities quickly realised that it was not a viable enduring solution. Although essential in the short term, such lockdowns are untenable in the long term from a legal, economic, and social perspective. Some of the studies advocating confinement have fallen short by considering only public health, disregarding other types of assessment, such as ethical, legal, and economic evaluations.[95]

The second strategy – herd immunity – consists in letting life continue as usual. In its purest version, it does not involve any type of PDMs. People would be asked to use masks and keep up social distancing, but controlling compliance would become a challenge, as it is not possible to have a police agent on every corner. Manual contact tracing would be necessary to inform people if they had been in close contact with someone infected, but we lack sufficient trained staff to trace every contact. Moreover, the particularities of this infection (around half of the infections happen before the infecting person feels any symptom, making it difficult to remember every single contact that took place in a period when the person did not know he/she was infected) make traditional contract

tracing non-effective.[96] Infected or potentially infected individuals would be asked to isolate or quarantine, but unless everyone was kept in secure facilities enforcement might become a challenge. Low compliance with many of the required public health measures (such as wearing a mask or maintaining proper distance),[97] inability to reach people in a quick and efficient way for precise contact tracing,[98] and lack of public health surveillance[99] would most likely lead to an increase in the number of infections. Thus, 'freedom' from technology would come at the price of health and even human lives.

This strategy was not effectively carried out in any country, as far as we know.[100] Even though it was initially praised by some – the UK and Sweden – soon it became clear that a pure herd immunity strategy in a disease with such a high mortality rate would lead many to death. Unlike the first assumptions, it was not enough to protect the so-called 'vulnerable' (the elderly, people with comorbidities) because even young healthy people were dying.[101] Health, and even life, would have been seriously affected by this strategy.

4.3. PDMs, rights and liberties

In the absence of a pandemic (or a similar catastrophe), most forms of PDMs would be unlawful. The pandemic has the power to change this assessment, and the legitimacy of PDMs must be considered in this context.

The most effective way to eradicate a virus is through vaccination. Currently, we have several pharmaceutical mechanisms to deal with the virus, but at the very beginning of the pandemic we had not, and in future pandemics chances are we have neither a vaccine nor a clear prospect of obtaining one in the near future.

PDMs act as an alternative to quarantines and lockdowns.[102] With the assistance of PDMs, an infected person can stay in his/her own home while being monitored for compliance with the imposed measures.[103] In addition, the PDM may monitor the person's health through telemedicine. Despite privacy intrusions, it is still less intrusive than hospital or home isolation controlled by security forces or health workers. Likewise, compared with long-lasting home confinement to prevent the spread of the virus, it is less intrusive to use digital contract tracing in return for the freedom of movement. Digital contract tracing allows people to continue with their daily lives (although with the additional safety measures of masks, sanitiser, and social distance), only quarantining if they come into contact with an infected person.

In a superficial assessment, the choice between using PDMs or not amounts to a choice between protecting life and health at the expense of some liberties (with PDMs) or favouring rights and liberties but risking health and even life (without PDMs). This is the classic tension in pandemics: public health versus rights and liberties.[104] However, upon deeper examination, the use of technology in this scenario may also be seen as a way to protect rights and liberties. There is a paradox here: the same technology with the potential to endanger our rights can also safeguard them from other (more severe) threats.

5. PDMs and digital governance

In times as challenging as these, governments should have a greater margin of discretion, and their scope of intervention should be broadened. Nonetheless, the pandemic does not provide *carte blanche* to move outside the law, much less against the law. A health

crisis justifies additional restrictions on individual rights, but in no way annuls the rule of law.[105]

A rights-based approach should inform the nature, scope and timeframe of the digital measures being used. 'The more intrusive the technology is, the stricter the test [the requirements to fundamental rights restrictions] must be'.[106] To ensure appropriate digital governance during the health care crisis and beyond, PDMs must comply with a set of principles and restrictions forming a digital governance code. This concept refers to the general principles imposed on the restriction of rights and liberties, now applied to the specific case of digital intrusions.

5.1. Legitimate aim

The aim of any digital intrusion is of the utmost importance. The aim must be relevant enough to justify the use of measures that would be unlawful in any other circumstance.[107] Public health is one of the legitimate aims and

> may be invoked as a ground for limiting certain rights in order to allow a State to take measures dealing with a serious threat to the health of the population or individual members of the population.[108]

PDMs can enable the preservation of human lives. Moreover, although they may intrude upon our rights and liberties, PDMs are themselves a tool to protect those same rights and liberties from more draconian interventions.

Due to the paramount importance of the aim, PDMs can only take place in service of that specific aim. However, there have been reports of deviations in this regard. For instance, the data provided by Chinese health codes are allegedly communicated not only to health authorities for public health measures but also to the police for different purposes.[109] In Korea, health information is being shared with agencies in charge of combating bioterrorism.[110] Some of these 'additional aims' may be valuable, but their *prima facie* legitimacy does not justify the change of purpose.

5.2. Legal ground

As for any other measure that limits rights, a clear legal ground is required. Both national laws and international documents allow for the restriction of rights in certain circumstances. For instance, Article 15 of the ECHR allows derogations in times of emergency, including public health emergencies. Several of its norms also allow restrictions on specific rights: Articles 8 (right to respect for private and family life), 9 (freedom of thought, conscience and religion), 10 (freedom of expression) and 11 (freedom of assembly and association) protect relevant values such as 'health', a term that refers to public health as well as individual health.[111] Several United Nations documents allow derogations to the rights thereon proclaimed in public emergencies, such as Article 4 of the International Covenant on Civil and Political Rights (ICCPR) and paragraph 14 of the Syracuse Principles.

Nonetheless, it should be recognised that such provisions inadequately address the specific challenges raised by PDMs, precisely because of their novelty. Human beings have never before been faced with such threats, and it is only natural that existing

regulations are insufficient.[112] For future situations, it is recommended to elaborate on specific acts, able to provide a more adequate legal basis for the restrictions of rights by virtue of digital intrusions.

5.3. Necessity, proportionality and adequacy

The general criteria guiding the limitation of fundamental rights require a previous assessment of necessity, proportionality and adequacy,[113] the three dimensions of the classic proportionality principle.[114] This safeguard is connected to an idea of limits: measures that limit fundamental rights shall themselves be limited. This core idea is proclaimed in major human rights documents, as in Article 52(1) of the CFREU.

The principle of necessity only allows restrictive measures as long as they are required to achieve a given purpose (principle of necessity *strictu sensu*), and, of the various mechanisms equally suitable to achieve the purpose, the chosen one should be the least intrusive (principle of the least intrusive measure).[115] Therefore, digital intrusions shall be limited to a minimum level of intrusiveness, in particular, limited in scope[116] and in time.[117] For instance, if contact tracing can be done by measuring users' proximity, there is no reason to collect user's location, a type of data that can provide much more information about the person, such as the church he/she attends (the person is in a synagogue) or even his/her sexual preferences (the person is in a gay bar). Likewise, a measure only needed to control the movement of people under isolation should not be transformed into a mechanism of mass surveillance by the state[118] or a mechanism of control by private companies. Limitations on time would prescribe that existing PDMs be discontinued once the pandemic is considered controlled (because the virus has been eradicated or because the rate of infection is very low), as they are only necessary during the pandemic. However, concerns have been raised regarding the maintenance of digital intrusions, especially surveillance technology, in the post-pandemic period.[119]

The principle of proportionality imposes a balance between the harm resulting to individual rights and liberties and the benefits expected from the restrictive measure.[120] Restrictions on individual rights are only admissible as long as the public health benefits expected from PDMs (for instance, to identify new outbreaks, to promptly alert people about potential infections, or to enforce corresponding health measures efficiently) largely outweigh the restrictions imposed. In the case of wearable symptom checkers, from a strict public health perspective, it is valuable to diagnose the infection as soon as possible, especially because self-reporting may come too late, given the incubation period and the large number of asymptomatic patients.[121] However, due to the degree of intrusion on a person's privacy and the potentially drastic consequences of a positive diagnosis (the patient might be forced to isolate themself, and all of his/her close contacts might be asked to test and quarantine), wearable devices shall not be imposed on citizens.

The principle of suitability can be defined as '[precluding] the adoption of means that obstruct the realization of at least one principle without promoting any principle or goal for which it has been adopted'.[122] In other words, the restriction of a right should only take place if the final aim is effectively achieved. In the example of contact tracing, the accuracy of GPS technology in identifying 'close contacts' is low (ranging from 5 to 20 metres in the open sky, which is insufficient given that the novel coronavirus can

spread within 1 m); and it only works efficiently outdoors and without obstacles (such as high buildings or thunderstorms). Therefore, a public policy requiring citizens to use GPS contact tracing technology would probably fail the suitability test because the resulting restriction of rights would not achieve the objective of monitoring close contact or the spread of the virus. Bluetooth technology imposes less of an invasion of privacy,[123] and it is much more precise in tracing contacts; therefore, it is a more suitable mechanism for contact tracing.[124] Moreover, as subsequent studies showed that the virus spreads easily in poorly ventilated spaces but not so much in the outdoors,[125] it can be questioned how suitable (and efficient) digital contact tracing in open spaces is.

5.4. Voluntary nature

There are many reports of mandatory governmental PDMs (see the case of mandatory selfies imposed by the Polish executive branch).[126] In other cases, PDMs are not imposed by law but are *de facto* mandatory to allow a person to perform basic daily activities, such as the use of colour-coded health codes in China[127] and Macao.[128] Using the code is technically voluntary, but it is required for so many aspects of day-to-day life (such as entering public offices as well as many private facilities) that it is, in effect, mandatory. There are also reports of employers and private companies demanding the use of PDMs in such a way that their workers cannot refuse, under the pressure of losing their jobs or other essential services or benefits.

As a general rule, PDMs should be voluntary, given their impact on individual rights and liberties. Nonetheless, exceptions to this rule must be permitted: (i) when the use of technology is absolutely necessary for the protection of others (i.e. there is no other way to achieve the purpose); (ii) the PDMs effectively reach the targeted purpose; and (iii) the benefits obtained far outweigh the burdens imposed on citizens. In a pandemic scenario, one can assume that these conditions can be met on several occasions. For instance, suppose that an individual infected with a serious and highly transmissible virus keeps violating the isolation order and that the only way to keep him/her confined is by using a digital bracelet that alerts authorities whenever he/she tries to leave the authorised perimeter. This could be a case for mandatory PDMs.

In the case of digital contact tracing, because manual contact tracing is not viable, an app capable of quickly and effectively informing individuals and authorities about close contact with infected individuals (that is, with a minimum margin of error) with sufficient guarantees of privacy could be made mandatory. Considering that the efficiency of these apps depends on their widespread use, a requirement for their use would only bolster its justification. Unfortunately, extant contact tracing apps fail to fulfil these requisites; all of them have flaws in terms of efficiency (Bluetooth-based apps being more accurate but still falling short in terms of precision), and some of them do not provide adequate protection for private data.

5.5. Principles of good administration

This paper uses the concept of 'good administration' in broad terms[129] to encompass several principles connected with the rule of law as it has been stressed by European institutions.[130]

Specifically, good administration encompasses a justification for any actions taken. Any intrusion on rights – in this case, digital intrusion – requires the provision of proper justification by public authorities.[131] The more intrusive a measure is, the more justification is needed to allow it.

Public disclosure is also essential for a rights-informed approach to technology, as public trust is essential when using such potentially hazardous measures.[132] Intrusive measures should be publicly disclosed, and citizens should be clearly informed about their requirements and aims, the consequences of not complying with them, and any other relevant information, including their expected duration. In the case of digital tools collecting personal data, governments should clarify, from the very beginning, which data are being collected, for what purposes, under what conditions they are being collected, and what entities will have access to data.[133] For digital tools using artificial intelligence, the criteria upon which algorithms are based must be made public, as well as their mathematical models.[134] It should be noted that in the technological domain, this requirement may be difficult to accomplish. Intellectual property rights may prevent some information from being disclosed, and highly technical information is often not understood by the layperson.[135]

Connected with the requirement of public disclosure is the requirement of citizens' participation in the framing of digital policies.[136] Specifically, citizens should directly participate in the discussion to determine which technologies to use (for instance, the use of digital fences instead of facial recognition to assure compliance with quarantines/isolations), providing feedback about which trade-offs they are willing to accept in terms of public health versus their rights and liberties.[137]

Governments must implement the user-centred digital practice,[138] which is already in place in several jurisdictions for different types of digital services that governments provide. In the context of PDMs, this requisite dictates, among other things, that the use of digital tools be planned in a way that contemplates how they will be used by citizens and considers the best solutions to protect the users.

Part of good administration concerns providing protection from negative effects. Technology should not lead to additional negative consequences for those who use it. This rule must be understood in two ways. First, the specific user cannot be subject to social ostracism. For example, within a colour code system, it should be guaranteed that the people to which a 'negative' code is assigned are not ostracised or prevented from accessing essential services, even if in a different form (thus, even if a child with a red code is prevented from attending school, suitable educational resources shall be provided, namely using digital mechanisms).

Second, technology should not involve bias and discrimination. Big data and artificial intelligence cannot be used to create stereotypes against specific groups of people, such as by implying that some minorities are less likely to comply with rules. If anything, the aim of technology use should be the opposite: ethnic minorities, those living in poverty, the geographically displaced, children, the elderly and other vulnerable populations are entitled to special protection during a health crisis. People experiencing special burdens or injuries must have some form of legal protection available to them.[139] Even if some limitations on individual rights can be justified to protect and promote public health, those who are particularly affected must be entitled to compensation. This aim requires an oversight mechanism, preferably held by an independent entity.

PDMs must also ensure the accountability of governments, private companies and any person or entity making decisions that have the effect of limiting rights. With PDMs this goal poses additional challenges, as decisions that are potentially harmful to citizens are being made not by human public officers but by software, which in turn involves a wide array of people in its creation.[140] Decisions are being made autonomously not only by machines but by models of artificial intelligence; that is, machines that make decisions based on the knowledge they have acquired themselves. Technological mechanisms should be subject to a monitoring mechanism overseen by humans. Regardless of a technology's reliability, decisions should not be based only on that technology.[141] Instead, human assessment should be required to confirm the techno-decision.[142] Moreover, decisions should not be automatically imposed but should be discussed with the affected individuals before they are implemented.[143]

6. Conclusion

The relationship between PDMs and individual rights and liberties is, as Facebook (also a digital tool) would say, complicated. On the one hand, technology has the potential to be used to control people. On the other hand, PDMs may better safeguard health, individual rights and liberties than alternative approaches such as total lockdowns, which can lead to more severe disruptions to our liberties while letting the infection run free and threaten human survival.

Despite the intrusiveness of technologies currently being deployed in the fight against COVID-19, these technologies are valuable tools both in promoting public health and in protecting individual rights and liberties from more severe constraints, as long as they are safely and effectively used. It is crucial for PDMs use to comply with the rules of digital governance. If that aim is reached, PMDs became a valuable tool in pandemic health crises.

We learned many lessons from this pandemic. Some of them are very painful ones (how fragile our existence is; how no one, not even the young and healthy, is safe), but all very useful to deal with future health crises. The essential role of PDMs – and also the role of digital governance principles to guide them – was one of those lessons.

Notes

1. China was the first country to use technology to handle a pandemic. Cf. Vera Lúcia Raposo, 'Can China's "Standard of Care" for COVID-19 Be Replicated in Europe?' *Journal of Medical Ethics* (2020), doi:10.1136/medethics-2020-106210.
2. This paper uses 'isolation' to describe the confinement imposed on individuals who are effectively infected, whereas 'quarantine' refers to the confinement of individuals without a positive test for infection. See Laurence Gostin, Ronald Bayer, and Amy Fairchild, 'Ethical and Legal Challenges Posed by Severe Acute Respiratory Syndrome: Implications for the Control of Severe Infectious Disease Threats', 290, no. 24 (2003) *JAMA* 3229, at 3230–323, doi:10.1001/jama.290.24.3229.
3. Mattias Kyhlstedt, and Sarah Wamala Andersson, 'Diagnostic and Digital Solutions to Address the COVID-19 Pandemic: The need for International Collaboration to Close the Gap', *Health Policy and Technology* 9 (2020): 126.
4. This is not to say that democratic governments do not widely use digital tools before the pandemic, even to implement surveillance mechanisms (some of them were considered

lawful). See Vera Lúcia Raposo, 'You Can Run, But You Can't Hide: Digital State Surveillance in Liberal Democracies', *The Digital Constitutionalist*, March 23, 2022, https://digicon.org/you-can-run-but-you-cant-hide/ (assessed May 13, 2022). However, the kind of digital tools being used during the pandemic, and in the specific scenarios for which they are being used, is a novelty brought about by this health crisis.

5. U. Gasser, M. Ienca, J. Scheibner, J. Sleigh, and E. Vayena, 'Digital Tools Against COVID-19: Taxonomy, Ethical Challenges, and Navigation Aid', *The Lancet. Digital Health* 2, no. 9 (2020): e425, https://doi.org/10.1016/S2589-7500(20)30137-0.
6. Some of these digital tools were previously used during the Middle East Respiratory Syndrome Coronavirus (MERS-CoV) outbreak, in 2015. See, for instance, Y. Kim, H. Ryu, and S. Lee, 'Effectiveness of Intervention Strategies on MERS-CoV Transmission Dynamics in South Korea, 2015: Simulations on the Network Based on the Real-World Contact Data', *International Journal of Environmental Research and Public Health* 18 (2021): 3530, doi.org/10.3390/ijerph18073530. However, those were cases of occasional use of a digital tool, instead of a systematic model of digital usage, as in this pandemic.
7. This paper assumes that digital tools do not affect rights considered non-derogable, such as the right to life and freedom from torture and other inhumane or degrading treatment or punishment.
8. Vera Lúcia Raposo, 'Quarantines: Between Precaution and Necessity. A Look at COVID-19', *Public Health Ethics* (2021) phaa037, https://doi.org/10.1093/phe/phaa037.
9. Digital tools are also being used in health care to refill medical prescriptions, follow up on patients (especially COVID-19 patients and chronic patients) and allow people to register their symptoms and obtain diagnoses. These types of digital tools will not be analysed in this paper because they raise different concerns as regards fundamental rights.
10. Michelle M. Mello and C. Jason Wang, 'Ethics and Governance for Digital Disease Surveillance', *Science* 368, no. 6494 (2020): 951, doi:10.1126/science.abb9045.
11. Séverine Toussaert, 'Upping Uptake of COVID Contact Tracing Apps', *Nat Hum Behav* 5 (2021): 183–184, https://doi.org/10.1038/s41562-021-01048-1.
12. See Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser, 'Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing', *Science* 368, no. 6491 (2020): eabb6936, doi:10.1126/science.abb6936; Rita Rubin, 'Building an "Army of Disease Detectives" to Trace COVID-19 Contacts', *JAMA* (2020), doi:10.1001/jama.2020.8880.
13. Li Du, Vera Lúcia Raposo, and Meng Wang, 'COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the Gap for International Pandemic Control', *JMIR Mhealth Uhealth* 8, bo. 11 (2020): e23194, doi:10.2196/23194; Michael Parker, Christophe Fraser, Lucie Abeler-Dörner, and David Bonsall, 'Ethics of Instantaneous Contact Tracing Using Mobile Phone Apps in the control of the COVID-19 Pandemic', *Journal of Medical Ethics* (2020), doi:10.1136/medethics-2020-106314.
14. Privacy International, 'Bluetooth Tracking and COVID-19: A Tech Primer', March 31, 2020, https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer (assessed October 13, 2020).
15. Ibid.
16. Ibid.
17. Daniel Castro and Eline Chivot, 'Turn Contact Tracing Apps on by Default – Europeans Shouldn't Need to Opt In', March 27, 2020, https://iapp.org/news/a/turn-contact-tracing-apps-on-by-default-europeans-shouldnt-need-to-opt-in/ (assessed December 4, 2020).
18. Mello and Wang, 'Ethics and Governance'.
19. WeChat is a Chinese multipurpose app, largely used in that part of the world to send instant messages, connect people by social media and make mobile payments.
20. Mello and Wang, 'Ethics and Governance'.
21. C. Jason Wang, Chun Y. Ng, and Robert H. Brook, 'Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing', *JAMA* 323, no. 14 (2020): 1341.

22. Alex Dubov and Steven Shoptaw, 'The Value and Ethics of Using Technology to Contain the COVID-19 Epidemic', *American Journal of Bioethics* (2020), doi:10.1080/15265161.2020.1764136.
23. Isobel Asher Hamilton, 'Poland Made an App that Forces Coronavirus Patients to Take Regular Selfies to Prove they're Indoors or Face a Police Visit', March 23, 2020, https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3 (accessed January 9, 2021).
24. Minghe Hu, 'Beijing Rolls out Colour-Coded QR System for Coronavirus Tracking Despite Concerns over Privacy, Inaccurate Ratings', *South China Morning Post*, March 2, 2020, https://www.scmp.com/tech/apps-social/article/3064574/beijing-rolls-out-colour-coded-qr-system-coronavirus-tracking (assessed September 15, 2020); Yijiang Lin, 'China's Health Codes Increase Population Surveillance', *Bitter Winter*, July 6, 2020, https://bitterwinter.org/chinas-health-codes-increase-population-surveillance/ (accessed December 9, 2020); Paul Mozur, Raymond Zhong, and Aaron Krolik, 'In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags', *The New York Times*, published March 1, 2020, updated August 7, 2020, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html (accessed December 20, 2020).
25. Hu, 'Beijing Rolls'.
26. The Special Administrative Region of Macao has also resorted to health codes, not via an app but via a website (Vera Lúcia Raposo, 'Macau, a Luta Contra a Covid-19 no Olho do Furação', *Cadernos Ibero-Americanos de Direito Sanitário* 9, no. 2 (2020): 12). Similarly, the Taiwanese approach is to ask travellers to scan a QR code, which redirects them to a website where they can input their health and travel information prior to departure or upon arrival at the airport. Based on this information, the QR code then informs travellers as to whether they can move freely or are required to self-isolate for 14 days (Wang et al., 'Response to COVID-19 in Taiwan').
27. Issie Lapowsky, 'Facebook Data Can Help Measure Social Distancing in California', *Protocol*, March 17, 2020, https://www.protocol.com/facebook-data-help-california-coronavirus (assessed October 17, 2020).
28. Data Taskforce Against Corona, 'Mobile Data to Battle Corona', March 25, 2020, https://www.proximus.be/en/id_b_cl_data_against_corona_taskforce/companies-and-public-sector/blog/news-blog/innovate/data-against-corona-taskforce.html (assessed November 25, 2020).
29. Katitza Rodriguez, Svea Windwehr, and Seth Schoen, 'Bracelets, Beacons, Barcodes: Wearables in the Global Response to COVID-19', *Electronic Frontier Foundation*, June 15, 2020, https://www.eff.org/deeplinks/2020/06/bracelets-beacons-barcodes-wearables-global-response-covid-19 (assessed December 5, 2020); Mary Meisenzahl, 'People Arriving in Hong Kong Must Wear Tracking Bracelets for 2 Weeks or Face Jail Time. Here's How they Work', *Business Insider*, May 4, 2020, https://www.businessinsider.com/hong-kong-has-tracking-bracelets-to-enforce-coronavirus-quarantine-2020-4 (assessed January 4, 2021).
30. Rodriguez, Windwehr, and Schoen, 'Bracelets'.
31. Another digital mechanism used to obtain health information is digital thermometers, which are used in airports and on buses in several jurisdictions (Sera Whitelaw, Mamas A. Mamas, Eric Topol, and Harriette G. C. Van Spall, 'Applications of Digital Technology in COVID-19 Pandemic Planning and Response', *Lancet Digital Health* 2 (2020): e435, https://doi.org/10.1016/S2589-7500(20)30142-4).
32. Cf. Gasser et al., 'Digital Tools Against', e426.
33. Rodriguez, Windwehr, and Schoen, 'Bracelets'.
34. Felix Light, 'Coronavirus Outbreak Is Major Test for Russia's Facial Recognition Network', *Moscow Times*, March 25, 2020, https://www.themoscowtimes.com/2020/03/25/coronavirus-outbreak-is-major-test-for-russias-facial-recognition-network-a69736 (assessed December 5, 2020).

35. Concerns about facial recognition have become particularly prevalent since private companies (Axon, the largest supplier of body cameras for police forces) and city enforcement authorities (in San Francisco) announced that they would drop facial recognition due to its inaccuracy, threats to fundamental rights and potential abuses by law enforcement agents. Cf. Kate Crawford, 'Regulate Facial-Recognition Technology', *Nature* (2019): 272, 565; European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (Publications Office of the European Union, 2019) 3.
36. On the concept of biometric data, Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications* (Springer, 2013), 15–272.

    Biometric facial data shall not be confused with photos not submitted to specific digital techniques (see Recital 51 of the GDPR and recital 29 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data).
37. On the protection of private data see also Data Protection 'Convention 108' and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.
38. Still, there are mechanisms able to trick some forms of facial recognitions. For instance, the use of makeup and forms of 'disguising' the facial features is a common strategy of activists (James Tapper, 'Hiding in Plain Sight: Activists Don Camouflage To Beat Met Surveillance', *The Guardian*, February 1, 2020, https://www.theguardian.com/world/2020/feb/01/privacy-campaigners-dazzle-camouflage-met-police-surveillance?CMP=Share_AndroidApp_Tweet (assessed December 15, 2020).
39. European Commission, European Governance. A White Paper, Brussels, July 25, 2001 (COM(2001) 428 final.
40. Parker et al., 'Ethics of Instantaneous'.

    Note, however, the different understanding of privacy in different jurisdictions. Cf. Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?' *Penn State Journal of Law & International Affairs* 8, no. 1 (2020): 50–117.
41. 'Two separate rights are here invoked: a classic right (protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No. 108). In Charter terms, similar rights are identified respectively in Articles 7 and 8. The Court has recognised the close link between the fundamental rights to privacy and the right to data protection'. Opinion of Advocate General Sharpston from 17 June 2020, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert GbR and Hartmut Eifert*, ECLI:EU:C:2010:353, par. 71.
42. Kristian P. Humble, 'International Law, Surveillance and the Protection of Privacy', *The International Journal of Human Rights* 25, no. 1 (2021): 1, doi:10.1080/13642987.2020.1763315.
43. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).
44. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
45. Charter of Fundamental Rights of the European Union (CFREU).
46. Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).
47. About the use of public health to justify different types of policies, see Ruth R. Faden and Sirine Shebaya, 'Public Health Programs and Policies: Ethical Justifications', in *The Oxford Handbook of Public Health Ethics*, eds. Anna C. Mastroianni, Jeffrey P. Kahn, and Nancy E. Kass (Oxford University Press, 2019), doi:10.1093/oxfordhb/9780190245191.013.

48. Y. Janna Anderson, Lee Rainie, and Emily A. Vogels, 'Experts Say the "New Normal" in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges', *Pew Research Center*, February 18, 2021, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/02/PI_2021.02.18_New-Normal-2025_FINAL.pdf (assessed May 15, 2022).
49. Mark Zastrow, 'South Korea Is Reporting Intimate Details of COVID-19 Cases: Has it Helped?', *Nature* (2020), https://www.nature.com/articles/d41586-020-00740-y (assessed January 4, 2021).
50. D. Halbfinger, I. Kershner, and R. Bergman, 'To Track Coronavirus, Israel Moves to Tap Secret Trove Of Cellphone Data', *NY Times*, March 16, 2020, updated March 18, 2020, https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html (assessed December 15, 2020).
51. High Court of Justice of Israel. 2109/20, 2135/20, 2141/20, 2187/20 *Ben-Meir et al v. The Prime Minister et al.*, April 26, 2020, https://supremedecisions.court.gov.il/Home/Download?path=HebrewVerdicts%5C20%5C090%5C021%5Cv43&fileName=20021090.V43&type=2 (assessed December 15, 2020).
52. Privacy International, 'Israel's Coronavirus Surveillance is an Example for Others – of What not To Do', May 1, 2020, updated July 21, 2020, https://privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do (accessed January 7, 2021).
53. Despite its virtues, TraceTogether never manage to obtain a huge adhesion from the community and somewhere along the way privacy complaints increased, as the Singaporean police was allowed to have access to the data collected by the app, contradicting what had been guaranteed before by the authorities. Cf. Kirsten Han, Broken promises: 'How Singapore Lost Trust on Contact Tracing Privacy', *MIT Technology Review*, January 11, 2021, https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police/ (assessed May 16, 2022).
54. Data on proximity are less intrusive than data on location (Privacy International, 'Bluetooth Tracking').
55. Facial images are personal data, as stated by the European Court of Human Rights (ECtHR) in *Szabo and Vissy v. Hungary*, application no. 37138/14, 12 January 2016, para. 56.
56. Hu, 'Beijing Rolls'.
57. See, for instance, *López Ribalda and Others V. Spain*, applications nos. 1874/13 and 8567/13, 17 October 2019, Grande Chamber; *P.G. and J.H. v. the United Kingdom*, application no. 44787/98, 25 December 2001; *Bărbulescu V. Romania*, application no. 61496/08, 5 September 2017, Grand Chamber.

    About the jurisprudence of the ECtHR on privacy see Özgür Heval Çınar, 'The Current Case Law of the European Court of Human Rights on Privacy: Challenges in the Digital Age', *The International Journal of Human Rights* 25, no. 1 (2021): 26, doi:10.1080/13642987.2020.1747443.
58. See the conclusions regarding privacy and public assemblies in Human Rights Committee of the United Nations, Draft General Comment No. 37 [Article 21: Right of Peaceful Assembly), draft prepared by the Rapporteur, Christof Heyns, July 2019, https://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle21/NGO_International_Center_for_Not_for_Profit_Law.pdf (accessed January 11, 2021), para. 69.
59. Ismail Keshta and Ammar Odeh, 'Security and Privacy of Electronic Health Records: Concerns and Challenges', *Egyptian Informatics Journal* (2020), https://doi.org/10.1016/j.eij.2020.07.003.
60. Radi Romansky, 'Social Media and Personal Data Protection', *International Journal on Information Technologies & Security* 4 (2014): 65.
61. Asunción Esteve, 'The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA', *International Data Privacy Law* 7, no. 1 (2017): 36, https://doi.org/10.1093/idpl/ipw026.

62. Borja Martínez-Pérez, Isabel De La Torre-Díez, and Miguel López-Coronado, 'Privacy and Security in Mobile Health Apps: A Review and Recommendations', *Journal of Medical Systems* 39 (2015): 18, https://doi.org/10.1007/s10916-014-0181-3.
63. Jay G. Ronquillo, J, Erik Winterholler, Kamil Cwikla, Raphael Szymanski, and Christopher Levy, 'Health IT, Hacking, and Cybersecurity: National Trends in Data Breaches of Protected Health Information', *JAMIA Open* 1, no. 1 (2018): 15, doi:10.1093/jamiaopen/ooy019.
64. As referred to by Humble, 'the elements which make up the effective control test over privacy do not fit the digital age' (Humble, 'International Law', 14).
65. Vera Lúcia Raposo, 'Perfect is the Enemy of Good: Digital Contact Tracing As A Tool To Handle Pandemics', *Medicine and Law* (forthcoming).
66. Vera Lúcia Raposo, 'Big Brother Knows that You Are Infected: Wearable Devices to Track Potential COVID-19 Infections', *Law, Innovation and Technology* (2021), doi:10.1080/17579961.2021.1977214.
67. Jonathan Andrew, 'Contact Tracing and Challenges to Privacy', *Universal Rights Group*, May 11, 2020, https://www.universal-rights.org/beyond-the-council/contact-tracing-and-challenges-to-privacy/ (assessed May 14, 2022).
68. The European Union Agency for Fundamental Rights underlines several fundamental rights issues, but some of their considerations must be adapted to the pandemic scenario. For instance, the agency states that facial recognition cameras may inhibit people from moving freely, but the purpose of their use during the pandemic is to prevent people under quarantine or isolation from moving freely for public health reasons. Cf. European Union Agency for Fundamental Rights, *Facial Recognition Technology*, 23–31.
69. Rodriguez, Windwehr, and Schoen, 'Bracelets'.
70. People that contravene the order to isolate or quarantine might or might not be committing a crime, it depends on whether the violation of such order is considered under their national law as a crime (I am not going to discuss if such conduct should be a crime or not, as this question is out of the scope of the current paper).
71. Fernando Londoño Martinez, '¿Responsabilidad Penal para los Infractores de la Cuarentena? Revisión Crítica de los arts. 318 y 318 bis del Código Penal (Nueva Ley n° 21.240): Más Micro que Macro … ', *Criminal Justice Network*, 2020, https://www.criminaljusticenetwork.eu/en/post/criminal-liability-for-quarantine-breakers-critical-review-of-articles-318-and-318-bis-of-the-chilean-penal-code-new-law-no-21240-more-micro-than-macro (accessed May 14, 2022).
72. Hu, 'Beijing Rolls'.
73. Ibid.
74. Lin, 'China's Health Codes'.
75. Human Rights Council, Surveillance and Human Rights. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 2019, David Kaye, A/HRC/41/35.
76. European Union Agency for Fundamental Rights, *Facial Recognition Technology*, 30.
77. Ibid., 9.
78. Patrick Grother, Mei Ngan and Kaynee Hanaoka, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects', *NISTIR* (2019) 8280. https://doi.org/10.6028/NIST.IR.8280. This study concluded that when 70% of a face was covered by a mask the most accurate algorithm still presented a percentage of failure of 5% and the percentages of the remaining ones varied between 20% and 50%.
79. Ibid.

    The precision of this technology is also undermined by the large number of people that must be identified. Algorithms have traditionally been used to look for a small number of individuals (namely wanted criminals), but now they are required to track a much larger number of people (everyone required to be in quarantine). Cf. Amnesty International, 'COVID-19, Surveillance and the Threat to your Rights', April 3, 2020, https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/ (accessed January 10, 2021).

80. Davide Castelvecchi, 'Is Facial Recognition Too Biased to Be Let Loose?', *Nature* 587 (2020): 347–349, https://doi.org/10.1038/d41586-020-03186.
81. Maria Pia Sacco, Theodora A. Christou, and Anurag Bana, 'Digital Contact Tracing for the Covid-19 Epidemic: A Business and Human Rights Perspective' (2020), www.ibanet.org/Document/Default.aspx?DocumentUid=98ae7850-48cd-4a0f-8424-c999c5bdde84 (accessed January 2, 2021).
82. A detailed analysis of this issue in Autor, *Journal of Law and Medicine*.
83. Several studies have concluded that in the absence of a vaccine, strict quarantines are the only way to handle the pandemic. Eleni Papachristodoulou, Loukas Kakoullis, Konstantinos Parperis, and George Panos, 'Long-Term and Herd Immunity Against SARS-CoV-2: Implications from Current and Past Knowledge', *Pathogens and Disease* 78, no. 3 (2020): ftaa025, https://doi.org/10.1093/femspd/ftaa025

    In 2007 the US Institute of Medicine conducted an intensive study on infectious diseases and concluded that only vaccines and contact tracing could contain this type of virus. The same conclusion is valid for the current situation: until we have an efficient vaccine, only DCT and similar technologies can help to handle the pandemic. Cf. Institute of Medicine (US), *Forum on Microbial Threats. Ethical and Legal Considerations in Mitigating Pandemic Disease: Workshop Summary* (National Academies Press, 2007), 144.
84. Raposo, 'Can China's "Standard of Care"'.
85. Imperial College COVID-19 Response Team, 'Impact', p. 2.
86. S. K. Brooks, R. K. Webster, L. E. Smith, L. Woodland, S. Wessely, N. Greenberg, and G. J. Rubin, 'The Psychological Impact of Quarantine and How to Reduce It: Rapid Review of the Evidence', *Lancet* 395 (2020): P912, doi.org/10.1016/S0140-6736(20)30460-8.
87. A. Pak, O. A. Adegboye, A. I. Adekunle, K. M. Rahman, E. S. McBryde, and D. P. Eisen, 'Economic Consequences of the COVID-19 Outbreak: The Need for Epidemic Preparedness', *Frontiers in Public Health* 8 (2020), doi.org/10.3389/fpubh.2020.00241.
88. Laura Hawryluck, Wayne L. Gold, Susan Robinson, Stephen Pogorski, Sandro Galea, and Rima Styra, 'SARS Control and Psychological Effects of Quarantine, Toronto, Canada', *Emerging Infectious Diseases* 10, no. 7 (2004): 1206.
89. Maria Nicola, Zaid Alsafi, Catrin Sohrabi, Ahmed Kerwan, Ahmed Al-Jabir, Christos Iosifidis, Maliha Agha, and RiazAgha, 'The Socio-Economic Implications of the Coronavirus Pandemic (COVID-19): A Review', *International Journal of Surgery* 78 (2020): 185, doi.org/10.1016/j.ijsu.2020.04.018.
90. Veronica Toffolutti, David Stuckler, and Martin McKee, 'Is the COVID-19 Pandemic Turning into a European Food Crisis?', *European Journal of Public Health* 30, no. 4 (2020): 626, https://doi.org/10.1093/eurpub/ckaa101.
91. Nicola et al., 'The Socio-Economic'.
92. Samantha K. Brooks, Rebecca K. Webster, Louise E. Smith, Lisa Woodland, Simon Wessely, Neil Greenberg, and Gideon James Rubin, 'The Psychological Impact of Quarantine and How to Reduce It: Rapid Review of the Evidence', *The Lancet* 395, no. 10227 (2020): doi.org/10.1016/S0140-6736(20)30460-8.
93. Mello and Wang, 'Ethics and Governance'.
94. Henrik Sjödin, Annelies Wilder-Smith, Sarah Osman, Zia Farooq, and Joacim Rocklöv, 'Only Strict Quarantine Measures Can Curb the Coronavirus Disease (COVID-19) Outbreak in Italy, 2020', *European Communicable Disease Bulletin* 25, no. 13 (2020): 2000280, doi.org/10.2807/1560-7917.ES.2020.25.13.2000280.
95. Imperial College COVID-19 Response Team, 'Impact of Non-Pharmaceutical Interventions (NPIs) to Reduce COVID-19 Mortality and Healthcare Demand' (2020), doi.org/10.25561/77482, at 4.
96. As pointed out by Joel Hellewell, Sam Abbott, Amy Gimma, Nikos I. Bosse, Christopher I. Jarvis, Timothy W. Russell, James D. Munday, Adam J. Kucharski, W. John Edmunds, Centre for the Mathematical Modelling of Infectious Diseases COVID-19 Working Group, Sebastian Funk, Rosalind M. Eggo, 'Mask or no Mask for COVID-19: A Public

Health and Market Study', *PloS one* 15, no. 8 (2020): e0237691, doi:10.1016/S2214-109X(20)30074-7.

97. Tom Li, Yan Liu, Man Li, Xiaoning Qian, and Susie Y. Dai, 'Mask or no Mask for COVID-19: A Public Health and Market Study', *PloS one* 15, no. 8 (2020): e0237691. https://doi.org/10.1371/journal.pone.0237691.
98. See E. Hernández-Orallo, P. Manzoni, C. T. Calafate, and J. Cano, 'Evaluating How Smartphone Contact Tracing Technology Can Reduce the Spread of Infectious Diseases: The Case of COVID-19', *IEEE Access* 8 (2020): 99083, doi:10.1109/ACCESS.2020.2998042.
99. Steven Teutsch and Stephen Thacker, 'Planning a Public Health Surveillance System', *Epidemiological Bulletin: Pan American Health Organization* 16 (1995): 1.
100. Autor, *Journal of Law and Medicine*.
101. Centers for Disease Control and Prevention, People Who Are at Higher Risk for Severe Illness, 2020, https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/people-at-higher-risk.html?CDC_AA_refVal=https%3A%2F%2Fwww.cdc.gov%2Fcoronavirus%2F2019-ncov%2Fspecific-groups%2Fhigh-risk-complications.html (assessed May 15, 2022).
102. The use of digital tools in the pandemic has been recommended by several studies from various perspectives. Wang et al., 'Response to COVID-19 in Taiwan'; Qing Ye, Jin Zhou, and Hong Wu, 'Using Information Technology to Manage the COVID-19 Pandemic: Development of a Technical Framework Based on Practical Experience in China', *JMIR Medical Informatics* 8, no. 6 (2020): e19515, doi:10.2196/19515.
103. Mello and Wang, 'Ethics and Governance'.
104. Ronald Bayer, 'The Continuing Tensions Between Individual Rights and Public Health. Talking Point on Public Health Versus Civil Liberties', *EMBO Reports* 8 (2007): 1099; I. Glenn Cohen, Lawrence O. Gostin, and Daniel J. Weitzner, 'Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension', *JAMA* (2020), doi:10.1001/jama.2020.8570.
105. Evan J. Criddle and Evan Fox-Decent, 'Human Rights, Emergencies, and the Rule of Law', *Human Rights Quarterly* 34 (2012): 39.
106. European Union Agency for Fundamental Rights, *Facial Recognition Technology*, 22.
107. The requirement of a legitimate aim to collect and process personal data is likewise stated in Article 5/1/b of the GDPR.
108. United Nations, Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights Annex, 1984, par. 25.
109. Privacy International, 'China: Alipay Health Code App Shares Data with Law Enforcemen', March 1, 2020, https://privacyinternational.org/examples/3433/china-alipay-health-code-app-shares-data-law-enforcement (assessed September 26, 2020).
110. Amanda J. Kim and Sangwoo Tak, 'Implementation System of a Biosurveillance System in the Republic of Korea and its Legal Ramifications', *Health Security* 17 (2019): 462.
111. Jonathan Pugh, 'The United Kingdom's Coronavirus Act, Deprivations of Liberty, and the Right to Liberty and Security of the Person', *Journal of Law and the Biosciences* 7, no. 1 (2020), doi.org/10.1093/jlb/lsaa011.
112. Likewise, classic rights proclaimed in national and international documents do not take into account many of these threats, because they have simply never been faced before. This idea is based on the conceptualisation of Henry Shue, where human rights appear as protections against 'standard threats' (see Henry Shue, *Basic Rights: Subsistence, Affluence, and U.S. Foreign Policy* (Princeton University Press, 1980), 13). The risks posed by digital intrusions are, in this light, non-standardised threats.
113. These principles are also basic criteria to evaluate fundamental rights restrictions in the case law of both the ECtHR (see, for instance, *Mouvement Raëlien Suisse v. Switzerland*, application no. 16354/06, 13 July 2012, Grand Chamber; *Fernández Martínez v. Spain*, application no. 56030/07, 12 June 2014, Grand Chamber; *Bărbulescu v. Romania*, application no. 61496/08, 5 September 2017, Grand Chamber) and the European Court of Justice (see, for instance, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner*

Landesregierung and Others, 8 April 2014, para. 52; C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 92; C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó-es Vámhivatal Kiemelt Adó-és Vám Főigazgatóság*, 17 December 2015, paras. 69 and 80–82).

114. See Robert Alexy, 'Constitutional Rights and Proportionality', *Revus* 22 (2014): 51. See also Jonas Christoffersen, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention On Human Rights* (Brill, 2009).
115. In human rights/fundamental rights doctrine, the principle of necessity is commonly equated to the principle of the least intrusive measure (see, for instance, Alexy, 'Constitutional Rights', 53, and the case law of the ECtHR, as analysed in Eva Brems and Laurens Lavrysen, '"Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights', *Human Rights Law Review* 15, no. 1 (2015): 139, https://doi-org.libezproxy.um.edu.mo/10.1093/hrlr/ngu040). In contrast, within public health discussions, both principles are commonly distinguished, although the principle of the least intrusive measure is considered a derivation of the principle of necessity, as it can be seen in James F. Childress, Ruth R. Faden, Ruth D. Gaare, Lawrence O. Gostin, Jeffrey Kahn, Richard J. Bonnie, Nancy E. Kass, Anna C. Mastroianni, Jonathan D. Moreno, and Phillip Nieburg, 'Public Health Ethics: Mapping the Terrain', *The Journal of Law, Medicine & Ethics* 30, no. 2 (2002): 170.
116. The principle of data minimisation is expressly referred to in Article 5/1/c of the GDPR.
117. European Data Protection Board, 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak', adopted on April 21, 2020, https://www.google.com/search?q=EDPB±(European±Data±Protection±Board)%2C±Guidelines±04%2F2020±on±the±use±of±location±data±and±contact±tracing±tools±in±the±context±of±the±COVID-19±outbreak%2C±Adopted±on±21±April±2020&oq=EDPB±(European±Data±Protection±Board)%2C±Guidelines±04%2F2020±on±the±use±of±location±data±and±contact±tracing±tools±in±the±context±of±the±COVID-19±outbreak%2C±Adopted±on±21±April±2020&aqs=chrome..69i57.675j0j4&sourceid=chrome&ie=UTF-8 (assessed July 20, 2020).
118. For more information about the issues raised by governmental mass surveillance, see Nick Taylor, 'To Find the Needle Do you Need the Whole Haystack? Global Surveillance and Principled Regulation', *The International Journal of Human Rights* 18, no. 1 (2014): 45, doi:10.1080/13642987.2013.871109.
119. Amnesty International, 'COVID-19'.
120. Alexy ('Constitutional Rights', 54) adopts, in this regard, the 'Law of Balancing', according to which 'the greater the degree of non-satisfaction of, or detriment to, one principle, the greater must be the importance of satisfying the other'.
121. Whitelaw et al., 'Applications of Digital Technology', e436.

    According to a study by Ferreti et al., 'Between one third and one-half of transmissions occur from presymptomatic individuals' (Ferretti et al., 'Quantifying SARS-CoV-2').
122. Alexy, 'Constitutional Rights', 52.
123. Privacy International, 'Bluetooth Tracking'.
124. Ibid. The EDPB (European Data Protection Board, 'Guidelines 04/2020', 15) also recommends this solution.

    Nonetheless, Bluetooth is not immune to error. Cf. Sacco, Christou, and Bana, 'Digital Contact Tracing', 11.
125. United States Environment and Protection Agency, 'Ventilation and Coronavirus (COVID-19)', nd, https://www.epa.gov/coronavirus/ventilation-and-coronavirus-covid-19 (assessed May 12, 2022).
126. Hamilton, 'Poland Made an App'.
127. Despite their arguably voluntary nature, reports have indicated high pressure from the authorities to use them and the practical inability to conduct daily life without them. Cf. Raposo, 'Can China's "Standard of Care"'; Lin, 'China's Health Codes'.
128. Raposo, 'Macau, a Luta'.

129. This is a principle to which EU institutions, bodies and agencies are obliged, according to Article 41 of the CFREU.
130. See, for instance, European Commission, 'European Governance'.
131. Nuffield Council on Bioethics, 'Ethical Considerations in Responding to the COVID-19 Pandemic', March 17, 2020, https://www.nuffieldbioethics.org/assets/pdfs/Ethical-considerations-in-responding-to-the-COVID-19-pandemic.pdf (assessed January 25, 2021).
132. Cohen, Gostin, and Weitzner, 'Digital Smartphone Tracking'.
133. Article 5/1/a of the GDPR.
134. Article 5/1/a of the GDPR requires data to be processed 'lawfully, fairly and in a transparent manner' and Article 5/2 imposes the accountability of the data controller.
135. Sacco, Christou, and Bana, 'Digital Contact Tracing', 6.
136. In general, see Mark L. Flear and Anastasia Vakulenko, 'A Human Rights Perspective on Citizen Participation in the EU's Governance of New Technologies', *Human Rights Law Review* 10, no. 4 (2010): 661, https://doi-org.libezproxy.um.edu.mo/10.1093/hrlr/ngq039.
137. Tiago Peixoto and Tom Steinberg, *Citizen Engagement: Emerging Digital Technologies Create New Risks and Value* (World Bank, 2019), https://doi.org/10.1596/32495, 60.
138. Ibid., 56.
139. Article 47 of the CFREU.
140. Jake Goldenfein, 'Algorithmic Transparency and Decision-Making Accountability: Thoughts for buying machine learning algorithms', in Office of the Victorian Information Commissioner (ed), *Closer to the Machine: Technical, Social, and Legal aspects of AI* (2019), https://ssrn.com/abstract=3445873 (assessed October 26, 2020), 41.
141. Article 22 of the GDPR.
142. European Data Protection Board, 'Guidelines 04/2020', par. 36; Council of Europe, 'Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe', April 28, 2020, https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7 (assessed July 2, 2020).
143. Ibid., 5.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the University of Macau [grant number MYRG2019-00035-FLL].

Notes on contributor

Vera Lúcia Raposo is currently Assistant Professor of Law and Technology at Nova School of Law, in Portugal, and part-time contributor to the Centre for M edical Ethics and Law, University of Hong Kong (China). In the past, she lectured at the University of M acau (China), the University of Coimbra (Portugal) and the University Agostinho Neto (Angola). She was also of-counsel at the law firm Vieira de Almeida e Associados, in Lisbon, in the departments of health law and privacy law. She is a frequent speaker at academic events worldwide and a member of the Editorial Board of the European Journal of Health Law. She is the author of several studies in Portuguese, English and Spanish (some translated into Chinese), particularly on biomedical law (medical liability, patient safety, gene editing, reproductive issues) and new digital technologies (AI, digital governance, data protection).