**Data protection in times of Covid-19**

**Comparative perspectives from Europe and beyond**

Yseult Marique

Olivia Tambou \*

**Abstract**

From a comparative perspective the Covid-19 pandemic provides a unique grand-scale life experience: nearly all countries have been confronted with a similar issue, that of quickly fighting the pandemic, balancing individual health with the sustainability of the national health system, and juggling economic imperatives with the duty to care for the most vulnerable individuals in society. Access and use of data are key to this difficult balancing exercise. One question arises: is the Covid-19 pandemic conducive to developing shared legal strategies or does it reinforce cultural legal features when it comes to data protection?

*Blogdroiteuropeen* asked experts in data protection to reflect on key developments in their national systems. No definitive answer is possible as Covid-19 is not over yet. However, this preliminary information leads to the identification of six trends underlying the Covid-19 crisis and its impact on data protection. First, all countries were not equal before the pandemic due to differences in their factual and legal backgrounds. Secondly, constitutional techniques proved resilient to a large extent in general and in particular when it comes to data protection. Thirdly, the effectiveness of data protection legislation is connected to its embeddedness in the wider legal context. Fourthly, tracking the spread of Covid-19 through tracing apps may turn out to be a unicorn defeated by data protection even though different technologies have been attempted. Fifthly, aggregation of data or collective harvesting of data in some form has been implemented to very different extents, provided some data protection requirements are met. This leads to the final trend: the ever more articulated pressure on the European Union to decide how far it wants to reclaim its digital sovereignty, and what this would entail concretely. As legal systems may have to cope with the long-term consequences of Covid-19 all over the world it may be useful to take stock of these emerging trends before designing any grand scheme for post-Covid-19 society.

1. **Introduction**

Beyond its economic and social consequences the Covid-19 pandemic may prove to be a turning point in our European approach of balancing individual rights and wellbeing with collective needs and values. Although there may be differences in the modalities implementing this precarious balance across Western countries, individual human lives – in their physical, mental and social aspects – are normally seen through the prism of freedom, equality and dignity. Our welfare state is built on this premise. Our human rights discourse seeks to flesh it out legally.[[1]](#footnote-1) Our scientific progress and its public funding are legitimized by enhancing it. The Covid-19 pandemic puts this model to the test. Privacy, access to and use of data become key interfaces between the social and individual trade-offs citizens are faced with. The Covid-19 pandemic thus moves us to reflect on our respective national priorities when we are confronted with drastic moral dilemmas. Different world visions compete where strategies for dealing with collective and individual challenges diverge. Documenting the legal developments behind the Covid-19 pandemic in Europe and beyond in a relatively systematic way to enable comparisons between countries, Blogdroiteuropeen seeks to answer the following question: is the Covid-19 pandemic conducive to developing shared legal strategies or does it reinforce cultural legal features when it comes to data protection?

By the end of July 2020 Blogdroiteuropeen had published thirty contributions.[[2]](#footnote-2) These contributions can be broadly divided into the following six main categories: 1) twelve contributions providing a general overview of data protection issues in times of Covid-19 in one specific jurisdiction (France, Germany, Greece, Hungary, Lithuania, Portugal, Slovenia, Spain, Sweden, the Netherlands, and the UK); 2) five contributions focusing on issues arising from tracing apps (Belgium, Germany, Ireland, Italy, and the UK); 3) three contributions focusing on issues arising in the context of e-learning (Germany, Italy, and Spain); 4) two contributions pertaining to surveillance techniques (France, and Spain); 5) three contributions discussing transversal issues (Zoom, platform workers, and immunity passports); 6) six contributions discussing jurisdictions outside Europe (Australia, Brazil, Canada, Israel, Japan, and South Africa).

These contributions do not provide definitive answers to our research question as Covid-19 is not over yet. However, they advance preliminary information about six trends underlying the Covid-19 crisis. First, all countries were not equal before the pandemic due to differences in their factual and legal backgrounds. Secondly, constitutional techniques proved resilient to a large extent in general and in particular when it comes to data protection. Thirdly, the effectiveness of data protection legislation is connected to its embeddedness in the wider legal context. This effectiveness is tested most by the large swathes of social and professional behaviours that now depend more (explicitly) on private intermediaries than before. Fourthly, the individualisation of control over the spread of Covid-19 through tracing apps may turn out to be a unicorn defeated by data protection (among other complex factors of success) even though different technologies have been attempted. Fifthly, the alternative to individualisation of control, aggregation of data or collective harvesting of data in some forms, has been implemented to very different extents, provided some data protection requirements are met. This leads to the final trend: the ever more articulated pressure on the European Union to decide how far it needs, wishes and is able to define its identity alongside its digital sovereignty, i.e. its ability to coordinate cross-border movements of data, the interoperability of the underlying systems and the architecture needed to run them. As legal systems may have to cope with the long-term consequences of Covid-19 all over the world, it may be useful to take stock of these emerging trends before designing any grand scheme for post-Covid-19 society.

1. **Not all countries equal before the pandemic**

From a comparative perspective the Covid-19 pandemic provides a unique grand-scale life experience: nearly all countries have had to confront a similar issue, that of quickly fighting the pandemic, balancing individual health with the sustainability of the national health system, and juggling economic imperatives with the duty to care for the most vulnerable individuals in society. However, all countries were not equal before the challenges posed by the pandemic. Three objective differences contribute to explaining (partly) the strategies adopted by countries to fight the pandemic and shape the choices available to them in terms of data protection.

First, the pandemic did not hit all countries in the same order and with the same intensity. The actual route of the pandemic remains shrouded in uncertainty, and the reasons why some countries may have appeared to cope well with the disease at first may have been misunderstood.[[3]](#footnote-3) However, some countries were hit before others, and within countries some regions were affected more intensively than others. Depending on this timing, more or less understanding of the disease may have been available when decisions had to be taken, hence shaping the kind of information countries were choosing to retrieve about their citizens or the types of behaviour they were seeking to prevent or monitor in their overall population or identified vulnerable groups. Furthermore, some countries had past experience either with recent epidemics or with health crises in a broad scope. These countries may have had governance structures in place to respond to the pandemic. The extent to which they actually listened to these structures varied – the UK is a case in point here.

Secondly, leadership is transformed in times of crisis.[[4]](#footnote-4) All countries were not in an equal position on that score, with different factors being potentially relevant. For instance, the political situation may have been diverted from the Covid-19 pandemic towards other political priorities at first. The UK was engrossed in post-Brexit discussions when the Covid-19 virus struck. Other countries were experiencing political turmoil. However, the Covid-19 pandemic succeeded in focusing the energies of political leaders. For instance, the political uncertainty predating the Covid-19 pandemic in Belgium, Ireland and Israel does not seem to have had noticeable negative consequences for the ways in which the pandemic was tackled in practice. Media have relayed another leadership difference: female leaders have adopted different strategies to address the pandemic, leading to more balanced results.[[5]](#footnote-5) One could probe beyond this feminist approach to look at the training in and/or familiarity with sciences for some leaders. German *Kanzlerin Merkel* and Irish *Taoiseach* (Prime Minister) *Varadkar*[[6]](#footnote-6) adopted a more preventative stance towards the Covid-19 virus than leaders dismissive of its gravity, such as President *Bolzonaro* in Brazil.[[7]](#footnote-7) Finally, some leaders personally experienced the effects of Covid-19. This meant that they were out of action for a crucial period of the crisis, yet this may have brought home the seriousness of the infection. British Prime Minister *Johnson* is the best illustration of this situation. These leadership factors may have framed strategic decisions about national priorities and how information and data could be relied upon in meeting these priorities.

Thirdly, differences in the population and their vulnerabilities to Covid-19 and its long-term consequences are slowly starting to be better understood. In the early days of the pandemic it rapidly became apparent that elderly people were more vulnerable to the virus, explaining the high rates of mortality in countries such as Spain and Italy, and specific issues with care homes in the UK. Now, other vulnerable groups are also better identified, with a more sophisticated understanding of what makes them more vulnerable to the virus in terms of contracting it or in terms of the symptoms developed. This explains the attention focused on obesity in the UK, for instance.[[8]](#footnote-8) In addition, some socio-economic situations such as poverty or working conditions add up and can lead to hot spots of Covid-19 cases at times[[9]](#footnote-9) – such as the outbreak of Covid-19 among Tönnies meat workers in Germany.[[10]](#footnote-10) If countries at large present different profiles in terms of age pyramid, general health of the population, and socio-economic factors, these differences have also consequences in terms of the type of data that may be needed at an individual level to organise efficient management and prevention of the virus. If prophylactic measures are taken, bodies in charge of devising and implementing these measures will need to amass a lot of data at both general and individual levels. The level of granularity required in the data may depend on how our lifestyle is predicated on individualistic or more collective choices. Key questions about allocating a (non-)identifying number to citizens may resonate very differently across countries, regions and groups. They may also depend on the ways in which social security and other public services are siloed or work in networks.[[11]](#footnote-11)

1. **Covid-19, emergency and resilience of constitutional techniques**

When the Covid-19 pandemic broke out many governments were taken aback. With few exceptions,[[12]](#footnote-12) they at first dismissed the gravity of the situation and postponed decisions, pondering which strategy was most suitable. Given the high level of information uncertainty and conflicting scientific advice about the illness, its communicability and its effects, governments engineered a high-level response: primary and/or secondary legislation was adopted to organise the health emergency at a general level or specific measures pertaining to various aspects of the crisis. Swift adaptations were needed.[[13]](#footnote-13)

Versteeg and Ginsburg have analysed how this health emergency has affected the allocation of powers between the legislative, the executive and the judiciary across more than hundred countries. Their core argument is that a significant portion of these states of emergency have not left the executive ‘unbound’.[[14]](#footnote-14) They identify three types of constraints on the executive: legislative involvement, judicial enforcement, and/or resistance of subnational units. Our project tends to concur with the general argument made by Versteeg and Ginsburg, namely that this state of health emergency has come hand in hand with a series of counterbalancing constraints to the powers granted to the executive. Analysing the effect of the health emergency on data protection requires adaptation, however. First, data protection is not only a matter of protecting individuals against the executive but also of organising the circulation of information in such a way that commercial operators do not extract profit from data to the detriment of data subjects. Secondly, even when data protection legislation is concerned with state/executive interference, it is a technical sub-set of wider constitutional arrangements, meaning that other constitutional grounds (*e.g.* freedom to circulate or to protest) may have been more forthcoming for judicial challenges in the heat of the crisis. Finally, the main actors of data protection are slightly different from those active in general politics, especially with many countries having a dedicated entity for data protection following their ratification of Council of Europe Convention nr 108 and its additional protocol.[[15]](#footnote-15)

Our project identified three types of control and/or resistance *vis à vis* the executive in the particular case of data protection. First, parliamentary involvement – sometimes even enhanced despite the physical limitations required by social distancing in times of Covid-19 – has been developed with a special focus related to data protection. Examples can be found in Belgium,[[16]](#footnote-16) France,[[17]](#footnote-17) Israel,[[18]](#footnote-18) Portugal,[[19]](#footnote-19) and the UK.[[20]](#footnote-20) Secondly, administrative decisions, executive orders and legislation pertaining to data protection have been challenged before courts in France,[[21]](#footnote-21) Brazil,[[22]](#footnote-22) and Israel.[[23]](#footnote-23) Thirdly, data protection authorities[[24]](#footnote-24)have been on the frontline to either advise the government on the emergency legislation or to provide guidelines on specific issues relating to the Covid-19 pandemic. Some data protection authorities have confirmed their high profile. For instance, the French data protection authority set clear limits on the development of the *StopCovid* app and investigated the use of drones*.*[[25]](#footnote-25)The Italian data protection agency was the first to adopt guidelines on e-learning.[[26]](#footnote-26) The Portuguese data protection agency also adopted guidelines on the same topic, among others.[[27]](#footnote-27) The Swedish data protection agency sought to inform the public on concerns related to the employee-employer relationship, distance learning and live-streaming graduations.[[28]](#footnote-28) The Irish data protection authority issued guidelines on data protection during the crisis, with practical advice on the dangers linked to the increased use of video-conferencing services.[[29]](#footnote-29) Activities carried out by other data protection authorities have proved to be less convincing. For instance, the Belgian data protection authority did not succeed in making its voice heard despite being supported by a well-organised civil society.[[30]](#footnote-30) Other countries reached out to the tried and tested strategy of enhancing the visibility of a political concern by setting up a dedicated agency. In the UK a draft piece of legislation aims at the creation of a Digital Contact Tracing Human Rights Commissioner.[[31]](#footnote-31)

This state of affairs, where different types of restraint can be identified, should not leave us complacent, however: more control mechanisms do not equal appropriate or efficient control.

1. **Data protection legislation: embeddedness and effectiveness**

The resilience of data protection in these times of health emergency can be approached at the level of principles and in the concrete challenges it has met.

1. **Constitutional level**

At the level of principles data protection can be embedded more or less strongly within the legal and constitutional framework of a national system – meaning that weakening data protection may demand more or less sophisticated devices.

If we look at European countries, a double distinction needs to be made. First, data protection may be constitutionally protected. In Spain the constitutional right to data protection cannot be suspended, even in times of emergency.[[32]](#footnote-32) In Switzerland it is also constitutionally guaranteed.[[33]](#footnote-33) The German constitutional court recognises a right to informational self-determination.[[34]](#footnote-34) However, other countries do not have such strong constitutional protection. Secondly, all EU Member States should have implemented the GDPR in their legislation. However, this implementation may be more or less effective. For instance, Slovenia has not yet transposed the GDPR.[[35]](#footnote-35) In Hungary the primary concern is to gain access to administrative documents to ascertain what types of information and data the government retrieves about its citizens.[[36]](#footnote-36)

If we look outside the EU, the GDPR is not supposed to be implemented. However, the “Brussels”/“Strasbourg” effects are noticeable. For instance, Canadian law has been “coloured” by the GDPR.[[37]](#footnote-37) In other countries the Covid-19 pandemic has drawn the attention to the need to have an appropriate legal framework in place. The result of this awareness has been moderate so far. In South Africa the data protection act had been enacted since 2013 but its substantive provisions only came into force in July 2020 in order to address the concerns arising from data protection in times of Covid-19.[[38]](#footnote-38) In Brazil the entry into force of data protection legislation has been postponed a number of times since 2018 with no clarity on when exactly it may eventually happen.[[39]](#footnote-39)

1. **GDPR on the ground and effective data protection**

The data protection model is pluralistic in the sense that, even in Europe, it leaves space for national differentiation in many respects. It leaves to Member States the possibility of regulating to some extent sensitive data such as health[[40]](#footnote-40) or the scope of public interest purposes, which can justify processing personal data without individual consent. Some countries have opted for a “flexible” use of the GDPR to accommodate conflicting priorities.[[41]](#footnote-41) What the Covid-19 pandemic makes difficult is not respect for data protection *per se* but the extent to which there is increased reliance on digital communication for all forms of social, professional and educational relationships. We are mandated to invite strangers, colleagues, students or bosses into our personal space, homes, bedrooms and living rooms, in ways over which we do not necessarily have much control. We may also transfer information and data to them without fully knowing or consenting to it. In this way the strategies used to deal with the Covid-19 pandemic threaten the very core of the intimacy and dignity that data protection is supposed to protect.[[42]](#footnote-42) This happens because some of the major technologies used fall within non-European jurisdictions.[[43]](#footnote-43) It also happens in spheres where either power relationships are already unbalanced (*e.g.* employment) or where the core of the relationship is not supposed to be predicated on commercial means and intrusion into one’s conscience but mutual respect (*e.g.* education). Let us look at each of these points in turn.

First, the increased reliance on digital communication for social and professional purposes can lead to clashes between the European and American approaches to privacy and data protection. This is of course not new but Covid-19 may have brought the stakes behind these two different perspectives closer to home for many. For instance, the extensive use of “Zoom” in professional and personal settings has led to deeper delving into the practice of linking logins with Facebook or LinkedIn or into the American and European descriptions of “Zoom” as either a controller or a processor. Zoom contends that it is a processor, which under American legislation (*i.e.* the **California Consumer Privacy Act)** means that it falls outside the American legislation regulating data protection; while under the European GDPR both processors and controllers have obligations, albeit different ones. Zoom also brings American-type class actions closer to European homes.[[44]](#footnote-44) All this increased digital traffic has heightened the risks of cyber-attacks.[[45]](#footnote-45)

Secondly, the Covid-19 pandemic affects employment relationships in many respects: can employers require employees to undertake medical tests to prove that they have or do not have Covid-19? Should employers provide these tests in order to protect the health and safety of their workplace, as much as they should comply with social distancing? Can or should employers equip employees with tools monitoring employee compliance with social distancing regulations? Is this all leading to surveillance of employees working from home?[[46]](#footnote-46) All these labour law questions are underpinned by access to data generated by employees during their contractual performance.[[47]](#footnote-47) If these questions arise in general terms, workers in the platform economy may be even more vulnerable to these measures as the platforms already have digital access to a broad range of data and can easily remove platform workers from platforms if they do not comply with their requests to hand data over.[[48]](#footnote-48) Data protection issues have also arisen in the context of accessing premises and reliance on thermal cameras. Here the French administrative court has differentiated between two types of practices, depending on whether a temperature was taken in order to prevent a person from accessing premises (with the potential for indirect identification of the person) or only to provide self-information for visitors without any recording of the data or control by agents.[[49]](#footnote-49)

Thirdly, the Covid-19 pandemic invites us to deeply rethink the education and university of tomorrow.[[50]](#footnote-50) Indeed, the pandemic requires schools, universities and public authorities to ponder how to balance the right to education with the rights of data subjects. Schools and universities have been heavily impacted by the Covid-19 pandemic as they present high risks for transmission. They were often among the first to close their doors and their physical re-opening may take time or happen only in stages, leaving open the question of whether online teaching should take over and if so, how. This leaves open a range of questions – from the possible duty of states to organise e-learning (in such a way as to guarantee data protection) to the modalities of this e-learning and the issues entailed by specific aspects of education and degrees giving access to regulated professions. As such the GDPR leaves it to the national state to regulate e-learning when it comes to the processing of personal data.[[51]](#footnote-51) The actual legislative design of e-learning depends on the contextual specifics of each member state. For instance, questions arise when e-learning is indeed encouraged as access to stable on-line services is not shared equally between students. On the other side of the coin, no regulation of on-line education at all means that the education sector may not know what it is allowed to do and, fearing sanctions or negative consequences, may refrain from proactively developing adequate services. This then leaves students in an even more unequal situation, as their socio-economic background may determine whether they will be in a position to compensate for their lack of education (because parents actively provide education or because students get support and advice from friends and family to access available on-line courses, for instance).

In Germany it has been argued that, in order to ensure students are able to exercise their right to participate in public education institutions without their right to informational self-determination being infringed, the *Länder* have to provide information technology infrastructure that conforms to data protection requirements.[[52]](#footnote-52) In Italy the situation is different as universities and schools are primarily responsible for selecting the appropriate means of on-line teaching. As they do not have the infrastructure to do so, schools and universities have relied on external providers. Working within the parameters of the GDPR, the Italian data protection authority has attempted to take a pragmatic stance in not requiring universities and schools to obtain the individual consent of students as long as the on-line teaching tools are relatively standard. However, schools and universities will need to meet their transparency duty towards students. Furthermore, the Italian data protection authority takes into account the risks of on-line teaching turning into a surveillance tool that could jeopardize academic freedom.

Once the principle of on-line teaching is accepted, and the modalities for its provision organised, specific issues arise in relation to proctoring[[53]](#footnote-53) and facial recognition. In Spain attention has been devoted to the online aspects of examinations and especially the collection and recording of images in order to verify the identity of the person taking the examination and to prevent fraud. These measures are understood as key guarantees of the inherent value of academic degrees.[[54]](#footnote-54) In Portugal the data protection agency has also adopted guidelines on remote examination and sought to raise awareness about learning analytics.[[55]](#footnote-55)

The Covid-19 pandemic leaves us with a key societal question, namely the future of education, and in particular the future of a possible “digital university”, in terms of teaching, designing modules, delivering them, supporting students through difficult times and challenging them to do their best, and assessing them – reducing the university experience to a digital relationship with tutors and fellow students. This digital education may not really challenge students to grow and mature in terms of independence and making personal choices in structuring their time and their attention. It will not extract them from their social milieu and confront them with a different world that they need to make sense of and grapple with. This provides a strange experience of otherness in which to refine their identities as adults confronted with the new digitalised world and social and professional relationships.

1. **Where individualisation of control fails – the devil in the details of tracing apps**

Tracing apps were touted as the wonder solution to addressing Covid-19 at the start of the pandemic. Digital technology would prevail and rescue the world. However, proponents of “technological solutionism” warned us of the consequences of technologies that are not well-understood.[[56]](#footnote-56) Technologies can become addictive for both their users[[57]](#footnote-57) and policy-makers,[[58]](#footnote-58) whilst their virtues are over-rated and the central problems that they are meant to address are left unattended. With a little bit of distance one may be excused for thinking that the discussions regarding Covid-19 tracing apps might have been much ado about nothing. In Australia the whole political rhetoric around the app has strongly abated.[[59]](#footnote-59) It is now seen as ‘the cherry on the cake’, a welcome addition but no longer a priority, in the UK.[[60]](#footnote-60) Sweden is not considering using such a app.[[61]](#footnote-61) Indeed, some apps have had little success in tracing Covid-19 cases. In the first three weeks of its functioning the French *StopCovid* app only notified fourteen people that they had been in contact with infected people.[[62]](#footnote-62)

1. **Technical choices**

Technically, two main options are available: geo-tracking and tracing. The main difference between the two options is that geo-tracking apps “*collect real time data on the precise location and movements of people, …*”.[[63]](#footnote-63) The geo-tracking app model, widespread in Asia,[[64]](#footnote-64) has been globally rejected by the European States. This geo-localisation of infected people was considered to be disproportionate surveillance, not in line with the European rules and values. Beyond this European consensus there are a variety of technical, political and legal modalities in the implementation of contact tracing apps across European States.

Two main approaches to tracing apps exist: either a centralised system or a decentralised system. In the first case all data relating to individuals are centralised in one database, allowing public authorities and/or health researchers to access and process them. In the second case the data are only stored in a decentralised way, *i.e.* in individual phones and other individual devices. At the outset of the crisis the technical challenges were not well-understood. There was a major advantage in a centralised system, namely that it allowed for more state control of the data and for following up on them in the offline world. Australia adopted this approach. At first, the UK did as well. Countries such as Germany oscillated between different options before opting for the decentralised option. This decentralised system is more vulnerable to approximation. A Bluetooth signal may be more or less strong depending on the circumstances or the devices used, it does not include specifics of meetings such as the presence of personal protective equipment, and it relies on individuals updating their details in the system and acting upon an alert that they have been exposed to an infected person. This system also relies on the operating systems of Google and Apple – with the risks that a lot of personal data are transferred to them under the guise of this app. As Google and Apple already access quite a wide range of our personal data, having access to sensitive medical data in addition may have unpredictable negative long-term consequences on individual autonomy. The choice between a centralised and decentralised system became one between channelling information to the public health system, limiting the flow of information not useful for their own needs on the one hand, and enabling infrastructures that Google and Apple will be able to use in the future for their own purposes, well past the Covid-19 pandemic, on the other hand.[[65]](#footnote-65)

1. **Human factor in the loop**

Technology is not the only component in tracing apps by far.Their success depends on many human factors: 1) overall, for the app to work, it is usually accepted that at least 70% of the population should download it; 2) users need to make sure that the app is active, keep it awake and updated and not delete it; 3) users need to input the system when they are tested positive (in some countries this input is only possible after the user’s information has been controlled by the health care system to prevent any false information from being spread)[[66]](#footnote-66) 4) users need to act on an alert of a risk situation; 5) when individuals travel outside their country of reference it is very likely that the app will not work anymore, which creates gaps in the profile of a person, maybe at the point where it would be most important to have the information – airports, crowded beaches, trains, and planes etc. are places where the virus can easily be transmitted.

All this leads us to think that digital technology may be a useful tool if well-managed, implemented and adapted to the specifics of a given country. However, it does not skip the human in the loop. It can only complement the manual tracing that is ongoing.

1. **Proportionality test**

Covid-19 tracing apps raise a key legal question in terms of data protection. Next to presenting security weaknesses of various kinds, these apps also need to comply with the proportionality test to meet the requirements of article 8 of the ECtHR. For interference in the right to privacy to be legal it needs to pass four tests: 1) it needs to pursue a legitimate objective; 2) it needs to be a necessary means to attain this objective, *i.e.* no less restrictive measure is available; 3) it needs to be a suitable means of reaching the objective; 4) it needs to be proportionate to the objective (*i.e.* proportionality *sensu strictu*).

A range of questions arise, however, when this proportionality test is applied to tracing apps. It is first important to identify the exact objective that these apps pursue. Covid-19 tracing apps have multiple objectives. They seek to be a tool informing users of them having potentially been in a risk situation and exposed to a Covid-19 infected person. They seek to inform other users that someone is infected and poses a risk to them. They seek to alert people of these risks so that they take the necessary measures to limit the risks of infecting other people (*e.g.* by self-isolating, by getting tested). They seek to limit the spread of the virus or at least contain it so that the health system is not overwhelmed by infected people. They seek to provide reassurance and some form of minimal self-control by users in resuming their social, economic and educational life as “normal” (as users do not want to have to self-isolate after testing positive, after receiving an alert that they have been exposed to a risky situation they will voluntarily and preventively avoid risky situations, hence contributing to limiting the spread of the virus). All these specific objectives are not articulated at the same level of generality/individuality. For these objectives to be reached Covid-19 tracing apps need to be more or less supported by a broader social and practical set of measures. Depending on this wider set, the app may be more or less a necessary or suitable component. For instance, in countries such as France and Belgium manual tracing is organised.[[67]](#footnote-67) Covid-19 tracing apps may also not meet the suitability test in the sense that for them to work a sufficient number of people need to download and make use of them. A lack of scientific evidence for the efficiency of tracing apps has been highlighted, for instance by the Belgian data protection authority.[[68]](#footnote-68) All in all, the Covid-19 tracing apps need to meet a number of criteria, in terms of privacy by design (e.g. Germany, Italy), voluntary use of the app by users, techniques to minimise data (for instance, pseudonyms and random numbers), and duration of data retention. From the contributions to our project the following overview can be provided.[[69]](#footnote-69)

|  |  |  |
| --- | --- | --- |
| Specific legal framework (primary or secondary legislation) | *Yes*: Australia, Belgium, France, Italy, Slovenia, South Africa, Switzerland,  *Under discussion*: the Netherlands, the UK (tabled by a parliamentary committee) | *No*: Germany (after discussion); Japan (parliamentary discussions) |
| System | *Decentralised:* Germany, Japan, Ireland, Italy, the Netherlands, Switzerland, the UK | *Centralised:* Australia, the UK (abandoned) |
| Use | *Voluntary:* Australia, Canada, Germany, Hungary, Ireland, Italy, Japan, Slovenia, South Africa, Switzerland | *Mandatory:* Slovenia (for people ordered to isolate) |
| Pseudonyms (and data minimisation) | Germany, Italy, Japan, Switzerland, the Netherlands |  |
| Data retention | * *14 days:* Italy, Japan, Switzerland, the Netherlands * *21 days:* Australia (on phone) * *60 days after the lapse of the quarantine:* Hungary * *18 months:* Lithuania | * *Period proportionate to the incubation period:* Ireland * *At the end of the pandemic:* Australia (all data) * *Until the end of the pandemic and no later than 31.12.2020*: Italy (processing of data) |
| Impact assessment | *Yes:* Germany, Ireland, Italy, the Netherlands | *No:* Japan |

1. **Justification**

The Covid-19 tracing apps also reflect national cultures and differences. Indeed, the use of this technique should be justified in some way, either thanks to a legal provision or thanks to obtaining the individual’s consent.[[70]](#footnote-70) In some countries, such as Lithuania,[[71]](#footnote-71) no such clear ground is provided in the app policy. In France the government introduced the *StopCovid* App following a legislative delegation to the government.[[72]](#footnote-72) In Germany individual consent is relied upon. These justifications for interfering with data protection mean that the social dimension of this practice is differently assessed. If only individual decisions are required where and how is the social debate about using technology in this way happening? How can individual consent be protected (so that it is free and well-informed)? What may happen if/when public and private “gatekeepers” require the use of this app before giving access to places, services, events and the like?

1. **Collectivisation of control and aggregation of data – appeal and downsides**

Tracing apps have caught much media attention because they seem to be ludic. However, they are only the tip of the iceberg, a tip that needs a high level of social support to be useful. Whilst discussions were held on tracing apps governments did not wait idly by. Other means of tracing, manual for instance, were implemented and scaled up. Other means were deployed to monitor the spread of the disease and whether restrictions to the freedom of movement and social distancing were complied with. Two main techniques stand out.

First, control over telecommunication has been used in Belgium,[[73]](#footnote-73) Germany, Israel, and Switzerland[[74]](#footnote-74) – to name a few. No such technique has been used in Ireland.[[75]](#footnote-75) In the Netherlands the adaptation of the Telecommunication Act to the collection of data to monitor crowds and people’s movements in times of Covid-19 has proved to be controversial, with the Parliament refusing to adopt it before the summer recess.[[76]](#footnote-76) A similar bill has been met with resistance for fear of mass surveillance in the Lithuanian Parliament.[[77]](#footnote-77) The situation is unique in Israel as means usually used to combat terrorism – *i.e.* access to communication metadata by the Security Agency and the police – were mobilised in the fight against the Covid-19.[[78]](#footnote-78) In Japan a wide survey was conducted in April using data analytics to survey citizens’ movements.[[79]](#footnote-79) It does not seem that this survey has been more than a one-off event.

Secondly, technologies such as drones have been used to control crowds and monitor whether social distancing regulations are being complied with. In France the supreme administrative court enjoined the Paris police to stop using this technique. The decision was taken once the main bulk of the lockdown was over.[[80]](#footnote-80) In Spain no judicial challenges have been lodged to the use of these drones.[[81]](#footnote-81)

1. **Choosing where to go from here**

Now that the first wave of the Covid-19 pandemic is over and the long-term consequences of living with the virus around have become clearer, strategies need to be designed, and again choices need to be made. Three key questions arise here around European digital sovereignty.

First, the question of the competence of the European Union to take the lead on this matter or the willingness of EU Member States to actively move beyond the limits of EU competences to address the need to develop a common strategy.

Secondly, the material reality that Europeans are moving around across the world, and certainly a lot within the EU territorial space. Therefore cross-border cooperation,[[82]](#footnote-82) technical interoperability, or immunity passports[[83]](#footnote-83) would be needed to support this free movement. The European Commission has issued a [recommendation](https://eur-lex.europa.eu/eli/reco/2020/518/oj) which supports exit strategies through mobile data and apps.[[84]](#footnote-84) Based on this recommendation the eHealth Network, a voluntary network of Member States’ competent authorities dealing with digital health, has prepared a [common EU toolbox for Member States](https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf).[[85]](#footnote-85) In addition, the European Commission has adopted [guidance](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN) in which cross-border interoperability between national apps with different architectures is encouraged.[[86]](#footnote-86) All this being soft law, questions of bindingness and legal certainty in the long term arise. Furthermore, one of the great successes of the EU has been the Erasmus programme: young people have become acquainted with other cultures and lifestyles thanks to spending part of their degrees in another country. What will happen to the benefits of such a European education once all these young people experience European education through Zoom from their bedrooms at home?

Thirdly, European digital sovereignty may mean many different things. It may mean that Europe should develop its own digital architecture[[87]](#footnote-87) or that Europe should not have to bow down to Google and Apple when it comes to finding a way out of the lockdown thanks to tracing apps. Major European countries such as France, Germany and the UK have found that this was not possible. Yet, the success of the apps remains to be proved; Google and Apple might not reap that many benefits from the system after all. This may mean that Europe is in control of its most crucial choices when it comes to deciding between quick illusionary technological fixes and hard-core medical research needs, and that it can give itself the means to deliver on its choices – should it choose to do so**.**

1. **Conclusion: protecting whose data from whom, when and how?**

Our project sought to assess whether a common experience at a global scale such as the Covid-19 pandemic was more of a nature to lead national legal systems to adopt similar strategies or to reinforce pre-existing national preferences, especially when it comes to data protection. All in all, data protection is not merely a question of organizing personal autonomy to protect it from big businesses or intrusive government. Data protection is a part of a bigger whole that reflects the choices made by national legal systems when it comes to their relationships with their citizens.

First, a distinction has to be made depending on whether or not GDPR has been implemented. The GDPR leaves scope for a national margin of appreciation. Outside Europe some countries (Brazil, South Africa) have been moved to implement their data protection legislation that had been put on a backburner before the pandemic. Other countries do not seem to report any concerns with data protection (Japan).

Secondly, differentiation appears when it comes to embracing technologies developed by big businesses such as Apple, Google or Zoom. Some irony looms here. Germany has opted for a tracing app working on Google and Apple technology. More surprising, maybe, due to its usual call for exceptionalism and “public service”, is that France has equally relied on similar technologies for its app but has even more embraced Microsoft technology for its Data Health Hub. The irony goes on because a country, the UK, often pointed to for its liberalism and love of economic actors within public service, has been steadfast in hoping that it would be able to go around these big businesses in developing its own app. It failed when Google and Apple declined to adapt their system to UK requests. Maybe if all the EU countries had been willing to pull together their overall shared power relationship might have been different?

Thirdly, data is not protected in a bubble. Data circulate in specific contexts, such as education, tourism, employment relationships, or health care. Here, national specificities kick in again. What the Covid-19 pandemic seems to suggest is that the GDPR can be implemented creatively by data protection agencies even in unusual circumstances. There are concerns that some technologies are not data protection compliant or that some power relationships or personal wishes/needs may lead individuals to set data protection aside or that techniques such as immunity passports will develop where data protection, personal freedom and equality are put under threat. However, the most striking difference is that some national systems tend to rely on legitimizing encroachment of data protection by individual consent (*e.g.* Germany) while other national systems rely on legal authorization (*e.g.* France, Italy).

Where do we go from here? This research intended to map some of the more prominent choices that will be with us after Covid-19 is over (to the extent that this will happen), especially in relation to the political and social dimensions of data protection. Three core questions emerge. The first question is very general as it pertains to the very ways in which sensitive data and data processing are regulated when it comes to research. Who ultimately gets to be in a position to reconstruct the medical, economic, social and cultural profile of citizens? Do we have more trust in Apple and Google – all American as they are but private “benevolent” actors – or our respective states – with all their flaws but led by politically accountable leaders? This is not a merely rhetorical question. When it comes to health issues such as vaccination and who has enough information to influence which pharmaceutical company will or will not reap the benefits of a large vaccination campaign, our collective and individual health will depend on 1) the quality of the data the research is based on; 2) education; and 3) trust in the overall system. The second question is more transversal to data protection and asks how transparency and fairness in data processing are fostered. The last question pertains more to how solutions can be worked out in crisis situations: is experimentation becoming inevitable? Is it becoming a substitute for prevention? Does it seek to implement the precautionary principle in a certain way? Can we accept “experimenting” with data protection?

1. \* Yseult Marique: Senior Lecturer (University of Essex) and Research Fellow (FÖV Speyer); Olivia Tambou: Associate Professor (University of Paris-Dauphine), External Scientific Fellow (Max Planck Institute of Luxembourg), Founder and Editor of Blogdroiteuropeen.

   *E.g.*: Kai Möller, *The Global Model of Constitutional Rights* (OUP 2012); David Beatty, *The Ultimate Rule of Law* (OUP 2005). [↑](#footnote-ref-1)
2. They are available on Blogdroiteuropeen <<https://blogdroiteuropeen.com/2020/08/01/breaking-for-the-summer-time-to-read-again-the-posts-on-data-protection-issues-and-covid-19-comparative-perspectives/>> accessed 25 August 2020. [↑](#footnote-ref-2)
3. For instance, new information suggests that Vietnam may have resisted the first waves of Covid-19 well because the virus may have originated from this part of the world, creating some level of immunity against its first forms among the population (X, ‘Bat signal – The hunt for the origins of SARS-CoV-2 will look beyond China’, *The Economist*, 22 July 2020, <<https://www.economist.com/science-and-technology/2020/07/22/the-hunt-for-the-origins-of-sars-cov-2-will-look-beyond-china>> -accessed 25 August 2020). [↑](#footnote-ref-3)
4. Chris Ansell, Arjen Boin and Paul 't Hart, ‘Political leadership in times of crisis’ in Roderick Rhodes and Paul 't Hart (eds), *The Oxford Handbook of Political Leadership* (OUP 2014) 418-429. [↑](#footnote-ref-4)
5. # Christine Lagarde, ‘Female leaders have been better at tackling Covid-19, says ECB chief’, *The Guardian,* London, 22 July 2020, <<https://www.theguardian.com/world/2020/jul/22/female-leaders-have-been-better-at-tackling-covid-19-says-ecb-chief>> accessed 25 August 2020.

   [↑](#footnote-ref-5)
6. # Shona Murray, ‘Ireland's premier Leo Varadkar re-registers as doctor during coronavirus pandemic’, *Euronews*, 5 April 2020, <<https://www.euronews.com/2020/04/05/ireland-s-premier-leo-varadkar-re-registers-as-doctor-during-coronavirus-pandemic>> accessed 25 August 2020.

   [↑](#footnote-ref-6)
7. This led scholarship to talk of an “executive underreach”: David Pozen and Kim Lane Scheppele, ‘Executive underreach, in pandemics and otherwise’ (June 30, 2020). American Journal of International Law, Forthcoming, Columbia Public Law Research Paper No. 14-664, Available at SSRN: <https://ssrn.com/abstract=3649816> or [http://dx.doi.org/10.2139/ssrn.3649816](https://dx.doi.org/10.2139/ssrn.3649816) . [↑](#footnote-ref-7)
8. # Haroon Siddique, ‘Coronavirus: Public Health England calls for action on obesity in Covid-19 fight’, *The Guardian,* London, 25 July 2020, <<https://www.theguardian.com/society/2020/jul/25/public-health-england-calls-for-action-on-obesity-in-covid-19-fight>> accessed 25 August 2020; Peter Walker, ‘No 10 plans weight loss drive to ready UK for expected Covid-19 second wave’, *The Guardian,* London, 11 July 2020, <<https://www.theguardian.com/society/2020/jul/11/no-10-plans-weight-loss-drive-to-ready-uk-for-expected-covid-19-second-wave>> accessed 25 August 2020.

   [↑](#footnote-ref-8)
9. <https://www.economist.com/international/2020/07/04/covid-19-is-here-to-stay-the-world-is-working-out-how-to-live-with-it> accessed 25 August 2020. [↑](#footnote-ref-9)
10. # Jon Henley, ‘Global report: Germany orders local Covid-19 lockdowns as Spain boosts tourism sector’, *The Guardian,* London, 18 June 2020, <https://www.theguardian.com/world/2020/jun/18/global-report-germany-orders-local-covid-19-lockdowns-as-spain-boosts-tourism-sector> accessed 25 August 2020.

    [↑](#footnote-ref-10)
11. # Elise Degrave, ‘The involvement of the academic community and civil society in the tracing saga in Belgium’, *Blogdroiteuropeen*, 21 July 2020.

    [↑](#footnote-ref-11)
12. # *E.g.*: in Greece (Vassilis Hatzopoulos, ‘Taming the Covid-19, not the GDPR: The case of Greece’, *Blogdroiteuropeen*, 4 July 2020); in Portugal (Rui Lanceiro, ‘Covid-19 and data protection in Portugal’, *Blogdroiteuropeen*, 2 July 2020); in South Africa (Melody Muson, ‘Contact tracing and data protection during Covid-19 pandemic in South Africa’, *Blogdroiteuropeen*, 29 July 2020).

    [↑](#footnote-ref-12)
13. # For an example, see Christian Geminn and Johannes Müller, ‘Covid-19 and data protection in Germany’, *Blogdroiteuropeen,* 6 July 2020.

    [↑](#footnote-ref-13)
14. Tom Ginsburg and Mila Versteeg, ‘The bound executive: emergency powers during the pandemic’ (July 26, 2020). *Virginia Public Law and Legal Theory Research Paper* No. 2020-52, *U of Chicago, Public Law Working Paper* No. 747, Available at SSRN: <https://ssrn.com/abstract=3608974> or [http://dx.doi.org/10.2139/ssrn.3608974](https://dx.doi.org/10.2139/ssrn.3608974) . [↑](#footnote-ref-14)
15. 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, Strasbourg, open to signature on 8.11.2001, entry into force on 1.7.2004. See Olivia Tambou, *Droit européen de la protection des données à caractère personnel* (Bruylant 2020), 2-9. [↑](#footnote-ref-15)
16. A parliamentary motion for a resolution in the federal Parliament asked the government to develop guidelines for the Belgian tracing app. Parliamentary hearings followed. [↑](#footnote-ref-16)
17. The French Parliament has been involved through the adoption of a Law of Health State Emergency and a lively debate on the *StopCovid* Application, see Olivia Tambou, ‘Data protection issues related to Covid-19 in France (Part 1): Issues on health data processing’, *Blogdroiteuropeen*,23 July 2020. This includes in particular hearings from data protection authorities such as the EDPS see, Wojciech Wiewiórowski, Introductory remarks before the committee for European Affairs of the senate of the Republic of France, <<http://www.senat.fr/compte-rendu-commissions/20200427/europ.html>> accessed 25 August 2020. [↑](#footnote-ref-17)
18. Parliamentary approval of the Intelligence Subcommittee was required for the governmental resolutions tasking the Israel Security Agency to have access to telecommunication metadata. [↑](#footnote-ref-18)
19. Doubts about the constitutionality of some of the measures taken by the Executive led them to be ratified by Parliament: Lanceiro (fn 12 ). [↑](#footnote-ref-19)
20. # Oliver Butler, ‘Legislating for the UK Government’s Covid-19 Contact Tracing App’, *Blogdroiteuropeen,* 14 July 2020.

    [↑](#footnote-ref-20)
21. # Olivia Tambou, ‘Data protection issues related to Covid-19 in France (Part 2): Control of some intrusive surveillance by public authorities’, *Blogdroiteuropeen*, 24 July 2020.

    [↑](#footnote-ref-21)
22. # Luca Belli and Nicolo Zingales, ‘Brazilian data protection under Covid-19: Legal certainty is the main casualty’, *Blogdroiteuropeen,* 3 July 2020.

    [↑](#footnote-ref-22)
23. # Amir Cahane, ‘Counterterrorism measures to counter epidemics: Covid-19 contact tracing in Israel’, *Blogdroiteuropeen,* 18 July 2020.

    [↑](#footnote-ref-23)
24. Among our survey, the following countries do not have a data protection agency: Brazil and Japan. [↑](#footnote-ref-24)
25. # Tambou (fn 21).

    [↑](#footnote-ref-25)
26. # Rossana Duccato, ‘Emergency remote teaching and digital data privacy: First instructions from Italy’, *Blogdroiteuropeen*, 16 July 2020.

    [↑](#footnote-ref-26)
27. Lanceiro (fn 12). [↑](#footnote-ref-27)
28. # Patricia Jonason, ‘Covid-19 pandemic and data protection issues in Sweden’, *Blogdroiteuropeen,* 20 July 2020.

    [↑](#footnote-ref-28)
29. Edoardo Celeste, ‘Covid-19 and data protection in Ireland’, *Blogdroiteuropeen,* 13 July 2020. [↑](#footnote-ref-29)
30. # Degrave (fn 11). In Canada as well, the data protection agencies seem not to have had much capacity to control the development of tracing apps (Vincent Gautrais, ‘Tracing applications in Canada: Lessons on how to regulate artificial intelligence – A few words explaining the Covid-19 situation in Canada’, *Blogdroiteuropeen,* 30 July 2020).

    [↑](#footnote-ref-30)
31. # Butler (fn 20).

    [↑](#footnote-ref-31)
32. # Article 55 (1) of the Spanish Constitution (Rosario García Mahamut, ‘Covid-19 and data protection in Spain: An overwiew’, *Blogdroiteuropeen,* 29 June 2020).

    [↑](#footnote-ref-32)
33. # Article 13 (20) Swiss federal Constitution (Alexia Pato, ‘Covid-19 and data protection issues in Switzerland’, *Blogdroiteuropeen,* 10 July 2020).

    [↑](#footnote-ref-33)
34. # Geminn and Müller (fn 13).

    [↑](#footnote-ref-34)
35. # Natasa Pirc Musar, ‘New powers accorded to the police due to Covid-19 in Slovenia’, *Blogdroiteuropeen,* 28 July 2020.

    [↑](#footnote-ref-35)
36. # Petra Lancos, ‘Data protection and freedom of information in Hungary: The latest casualties of Covid-19?’, *Blogdroiteuropeen,* 9 July 2020.

    [↑](#footnote-ref-36)
37. # Gautrais (fn 30).

    [↑](#footnote-ref-37)
38. Muson (fn 12). [↑](#footnote-ref-38)
39. # Belli and Zingales (fn 22).

    [↑](#footnote-ref-39)
40. Although the EDPB adopted guidelines on this topic: see EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, adopted on 21 April 2020. *Add* Tambou (fn 17). [↑](#footnote-ref-40)
41. Hatzopoulos (fn 12). [↑](#footnote-ref-41)
42. Francesco Giacomo Viterbo, ‘The ‘user-centric’ and ‘tailor-made’ approach of the GDPR through the principles it lays down’ (2019) 5 *Italian Law Journal* 631-672. [↑](#footnote-ref-42)
43. This situation will lead to legal issues, especially since the so-called privacy shield (i.e. the adequacy decision regarding the equivalence between American and the European regulation) has been invalidated in CJEU, C-311/18, 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (ECLI:EU:C:2020:559) (*Schrems II*). [↑](#footnote-ref-43)
44. # Alexia Pato, ‘Zoom and the data protection quagmire’, *Blogdroiteuropeen,* 11 July 2020.

    [↑](#footnote-ref-44)
45. # Audrey Guinchard, ‘The interplay of data protection and cybersecurity issues related to Covid-19 in the UK’, *Blogdroiteuropeen,* 15 July 2020.

    [↑](#footnote-ref-45)
46. # Celeste (fn 29).

    [↑](#footnote-ref-46)
47. # On the specific issues the Covid-19 pandemic makes arise in the field of employment law, see the special issue: ‘Covid-19 and labour law. A global review’ (2020) (13: n° 1S) *Italian Labour Law e-Journal*.

    [↑](#footnote-ref-47)
48. # Claire Marzo, ‘Covid-19 and data protection in the European Union: A platform worker’s perspective’, *Blogdroiteuropeen*, 25 July 2020.

    [↑](#footnote-ref-48)
49. # Tambou (fn 21).

    [↑](#footnote-ref-49)
50. For one of the initiatives related to this question, see: <https://blogs.ed.ac.uk/ed-decameron/call-for-papers-building-the-post-pandemic-university/> accessed 25 August 2020. [↑](#footnote-ref-50)
51. Article 6 (1) (e) and (2) of the GDPR. [↑](#footnote-ref-51)
52. # Jonas Botta, ‘Data protection first, e-learning second?’, *Blogdroiteuropeen*, 8 July 2020.

    [↑](#footnote-ref-52)
53. This practice led to case law in some countries, such as the Netherlands (Rb Amsterdam, 11 June 2020, C/13/684665/KG ZA 20-481, <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2020:2917> accessed 25 August 2020). [↑](#footnote-ref-53)
54. # Monica Arenas Ramiro and Ricard Martínez Martinez, ‘Online evaluation procedures and data protection: the collection and recording of images in Spain’, *Blogdroiteuropeen,* 1st July 2020.

    [↑](#footnote-ref-54)
55. Lanceiro (fn 12). [↑](#footnote-ref-55)
56. # Gautrais (fn 30).

    [↑](#footnote-ref-56)
57. French Senate, Commission des lois, Mission de suivi de la loi d’urgence pour faire face à l’épidémie de Covid-19, *COVID-19: Deuxième rapport d’étape sur la mise en oeuvre de l’état d’urgence sanitaire*, 29 April 2020, 85. [↑](#footnote-ref-57)
58. # Cahane (fn 23).

    [↑](#footnote-ref-58)
59. # Jake Goldenfein, ‘The political life of COVIDSafe contact tracing in Australia’, *Blogdroiteuropeen,* 27 July 2020.

    [↑](#footnote-ref-59)
60. # Butler (fn 20).

    [↑](#footnote-ref-60)
61. # Jonason (fn 28).

    [↑](#footnote-ref-61)
62. <<https://www.economist.com/international/2020/07/04/covid-19-is-here-to-stay-the-world-is-working-out-how-to-live-with-it>> accessed 25 August 2020. [↑](#footnote-ref-62)
63. See European Parliament News, ‘*Covid-19 tracing apps: ensuring privacy and data protection’* 6 May 2020, <<https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-data-protection>> accessed 25 August 2020. *Add* Matteo Ciucci and Frederic Gouardères, ‘National Covid-19 contact tracing apps’, *European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies*, May 2020. [↑](#footnote-ref-63)
64. But not in Japan. [↑](#footnote-ref-64)
65. Goldenfein (fn 59). [↑](#footnote-ref-65)
66. Italy. In Germany notification through one of the different possible means of communicating information to the system, namely hotlines, also requires a form of verification that no fake positive has been declared. [↑](#footnote-ref-66)
67. See for instance in France the data bases ‘SIDEP’ and ‘Contact Covid’ explained in Tambou (fn 17). [↑](#footnote-ref-67)
68. Degrave (fn 11). [↑](#footnote-ref-68)
69. Additional data on the use and format of Covid app can also be found on <https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/> accessed 25 August 2020. [↑](#footnote-ref-69)
70. We discuss here this aspect in relation to tracing apps. However, similar cultural differences appeared in other respects in this research. For instance, the right to informational self-determination in Germany would entail that students agree to data process online by their educational institutions. In Italy, by contrast, the Data protection authority considers that data processing in the context of online education can be based on the legal basis of article 6 (1) (e) of the GDPR and its Italian equivalent, without the need for students’ consent. [↑](#footnote-ref-70)
71. # Migle Petkevičienė, ‘Protection of personal data during pandemic in Lithuania’, *Blogdroiteuropeen,* 22 July 2020.

    [↑](#footnote-ref-71)
72. See art. 11 of the Loi n° 2020-546 du 11 mai 2020 *prorogeant l'état d'urgence sanitaire et complétant ses dispositions.* [↑](#footnote-ref-72)
73. # Alain Strowel, ‘Les experts de l'UCLouvain vous répondent: "Le traçage téléphonique pose question"’ *Le Vif l’express,* 17 April 2020, <<https://www.levif.be/actualite/belgique/les-experts-de-l-uclouvain-vous-repondent-le-tracage-telephonique-pose-question/article-normal-1278135.html>> accessed 25 August 2020.

    [↑](#footnote-ref-73)
74. Pato (fn 33). [↑](#footnote-ref-74)
75. Celeste (fn 29). [↑](#footnote-ref-75)
76. # Raphael Gellert, ‘Covid-19 & data protection in The Netherlands: Contact tracing app and automated collection of location data’, *Blogdroiteuropeen,* 28 July 2020.

    [↑](#footnote-ref-76)
77. # Petkevičienė (fn 71).

    [↑](#footnote-ref-77)
78. # Cahane (fn 23).

    [↑](#footnote-ref-78)
79. Hiroshi Miyashita, ‘Covid-19 and data protection in Japan’, *Blogdroiteuropeen*, 31 July 2020. [↑](#footnote-ref-79)
80. Tambou (fn 21). [↑](#footnote-ref-80)
81. # Cristina Pauner Chulvi, ‘Drone use in the fight against Covid-19 in Spain’, *Blogdroiteuropeen,* 30 June 2020.

    [↑](#footnote-ref-81)
82. With special issues relating to the border between Ireland and Northern Ireland, see Celeste (fn 29). [↑](#footnote-ref-82)
83. # Inigo de Miguel Beriain, ‘Immunity passports’, *Blogdroiteuropeen,* 27 June 2020.

    [↑](#footnote-ref-83)
84. Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, C/2020/3300, *OJ* L 114, 14.4.2020, 7-15. [↑](#footnote-ref-84)
85. eHealth Network, *Mobile applications to support contact tracing in the EU’s fight against COVID-19 - Common EU Toolbox for Member States*, 15 April 2020. eHealth Network, *Interoperability guidelines for approved contact tracing mobile applications in the EU*, 13 May 2020. *Add* <<https://ec.europa.eu/health/ehealth/covid-19_en>> accessed 25 August 2020. [↑](#footnote-ref-85)
86. Communication from the Commission, Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection (2020/C 124 I/01), *OJ* C 124 I, 17.4.2020, 1-9. [↑](#footnote-ref-86)
87. Along some proposals such as this one: <<https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4> > accessed 25 August 2020. [↑](#footnote-ref-87)