Institute of
European
Democrats

Call for Papers "Geopolitics & Values: what is the real power of the EU?"

AGAINST THE EXCEPTION
Public policy for knowledge and privacy

Author: S. Velasco SARA

Brussels, December 2020

Rue Montoyer, 25
1000 Brussels
Belgium

Web: www.iedonline.eu

This Research Paper was elaborated on the basis of independent research. The opinions expressed here are those of the Contractor and do not represent the point of view of the Institute of European Democrats.

With the financial support of the European Parliament

EXECUTIVE SUMMARY

The launch of Covid Tracking Apps throughout EU countries has raised the issue of citizens' rights to privacy and protection of personal data. The right to a private life distinct from the public space of society evokes the traditional two spheres born out of the social contract: the public and private spheres. Under the declaration of States of Exception, Governments have gained access to their citizens' private spheres, which had commonly been the spaces for resistance to public powers, therefore both Governments and citizens should benefit from a debate regarding the position of users' when installing apps and transferring their data. It is an opportunity to use Exception against itself to take steps to introduce public policies on behalf of users' rights.

Short bio

Sara S. Velasco is a double major in law and political sciences at Universidad Carlos III (Madrid, Spain), now working as the European postgrad studies manager at the same university. After her postgrad studies in intelligence analysis she has collaborated as an independent researcher with the International Affairs and Foreign Policy Institute in Madrid, as well as the Research Institute for European and American Intelligence Affairs.

Introduction

The coming of the 21st century, the technologization of society and the hyper expansion of the internet through all the levels of human life and social interaction have seen the rise of a new world: the digital world. The set of rules established for the analog world, product of the social contract, had set their own institutional system of checks and balances, with a separation of the public and private spheres, that sometimes had excluded certain individuals.

The advent of the digital world brought the same structures to human life and social interaction into the internet, but many of the checks and balances that had evolved to answer challenges that arose in the analog world were not yet ready to protect users while navigating the web. It is the case of Covid Tracking Apps, which have sprouted in most European Union (EU) Member States, complying at least formally with the EU General Data Protection Regulation (GDPR), but that also raise a lot of questions regarding their survival when the State of Exception is over, their inclusiveness of every sector of society, the management of such sources of data and the new systems of protection in the economy of information.

Public and private

Liberal democracies are the result of the configuration and balance of two different spheres - the public and private spheres- accordingly, political theory has pointed out those contractual projects that mark the emergence of liberal modernity. “Contract theory was the emancipatory doctrine *par excellence*, promising that universal freedom was the principle of the modern era” (Pateman, 1988:p.39).

The classical conceptions of social contract authors, such as Locke, Hobbes and Rousseau, demonstrate a series of common elements such as the idea of the individual as the central subject that gives their consent to become part of a society. Hence, the idea of an individual that accepts leaving the state of nature to live in a society is the single essentially revolutionary element of the social contract. Even when taking as a referent Hobbes’ political theory, it is individuals who agree to accept the Leviathan as a warranty for their security.

Under this premise- the contract- the modern era has seen a substantial change in the way individuals express consent. Today, when giving “likes” online, citizens become part of the new contract. They transform from individuals to users in the digital public sphere.

On another hand, in the social world there has always been room for resistance in the private sphere, and so it has been conceptualized by authors such as Locke. The private sphere is the place where individuals have to develop their own freedom (in the modern way as defined by Constant, 1819), the private development of oneself, where political power cannot intervene. This underlines the importance of natural and property rights as elements of resistance against the potential despotic power of the State.

However, this construction of the social contract has been built over a certain set of omissions. It is fair to ask whether the new world of the digital public sphere is reproducing the omissions of the analog reality or whether it is introducing new ones.

The classic social contract theory omits that the contractors in this case are individuals (who become citizens), an attribute that does not belong to the entirety of society. Specifically, women were excluded from this contract, which became more of a sexual contract, and they were disregarded to the private sphere, without the right to raise their voice in the public sphere.

Amongst the several conditions for this exclusion, one of the main ones was that the fathers or husbands were the ones to subscribe to the social contract, thereupon excluding women from the decision-making (Pateman, 1988:pp.77).

In this sense, one must review these types of omissions in relation to the digital world. The new apps open the possibility of accessing a new space, but they may not be neutral in the ways they pretend to be, and instead bring into the digital contract old omissions in their implementation, such as gender perspective. The fact that this issue is in general not addressed when using new apps may suggest that they reproduce the same omissions from the configuration of the analog public and private spheres.

The problem here, besides reproducing old exclusions from the equal use of the public sphere, be it digital or analog, is that these exclusions may even escalate. Just like it happened to women in the 18th century, the new contract may see individuals become users but depriving them of power and room for making decisions. This is the dangerous new omission of a space where secrecy is impossible and there is a surveillance economy that challenges the existence of privacy as the classical context of resistance against the State proposed it, and giving birth to a whole new concept of privacy (Fernández Barbudo, 2019).

The paradox of Exception

Countries around the world and within the EU have taken measures of Exception to fight against the COVID epidemic, such as the limitation of movement of persons, local and national quarantines, etc.

When talking about State of Exception measures, what one is referring to is “that moment in law where the rule of law is suspended precisely to guarantee its continuity, and even its existence” (Agamben, 2005:p.5). In other words, the coronavirus crisis has entailed the limitation of citizens’ fundamental rights on the basis of a greater good: ensuring these same rights’ survival. Invoking the State of Exception means always having to deal with this paradox inherent to the concept. Also, traditionally, it is important to note that Exception has two counterweights: on one side, the time of suspension of rights; on the other side, the control guaranteed by the separation of powers.

However, with the application of models of states of emergency, states of alarm, etc., public administrations have invaded the private sphere through the different measures of Exception taken in every country. This is troubling in the sense that it leaves no room for individuals to have their own space. That is to say, the private sphere is a resistance to the invasion from the political power over the lives of people, while at the same time the public sphere sets the rules for a peaceful society that guarantees rights and controls the state of nature’s outrages where, as Hobbes puts it, *homo homini lupus*. There is a balanced and symbiotic relationship of both spheres that, when the State of Exception is applied, gets disrupted for a greater good: the suspension of rights so that they can keep on existing in the future.

Still, what happens if this control is exercised in the digital world where there are no evident power counterweights? Actually, the great platforms led by global private enterprises have full control over the new data economy, whereas, paradoxically, public power has little strength before the big tech multinational corporations. How can different countries create digital tools with a public utility for, in this case, management of a sanitary crisis? How can governments monitor without punishing? How to confront the challenge of getting data while still keeping citizens’ privacy while bearing in mind the impossibility of secrecy in cyberspace. This is a 21st century version of the paradox of Exception that has been transferred from the analog world to the digital one.

Contact tracing Covid Apps

In March 2020 the coronavirus pandemic arrived in Europe, expanding in a matter of weeks throughout the continent and causing most EU Member States to declare states of emergency or alarm, different versions of the State of Exception. Quarantines fostered the expansion of the digital world and the platform economy, and new tools and problems arose.

In the case of information and communication technologies, there are six main functions that can be extracted from their application: management of information for crisis management, publishing public information for citizens, providing digital services to citizens, monitoring citizens in public spaces, facilitating information exchange between citizens and developing innovative responses to Covid (Meijer & Webster, 2020:p.267). Now most countries quickly adopted ways to publish information on the pandemic for the public. Both TV, social networks or the internet were flooded with constant updates, recommendations and institutional communications. In the case of monitoring, gathering and managing information concerns arose, precisely because under the State of Exception declared, Governments were invading the private sphere through digital means. What is more, in some Member States, providing location data became mandatory as a means to ensure that citizens were complying with mobility restrictions, which was the case in Poland, Lithuania or Slovakia (Dumbrava, 2020:17).

The launching of Covid Tracking Apps appeared as one of those policies that brought together technology and fighting the pandemic. However, they were not supported in every country, nor were they mandatorily implemented, even if they were promoted from the public institutions.

According to the European Commission, out of the 27 Member States in the EU, there are three categories depending on the national standing towards Covid tracking apps. The Commission's classification was made in june 2020, and has been updated as follows:

Table 1. Classification of EU Member States by App policy

No plans to launch an app	Luxembourg, Sweden
Preparing to launch an app	Greece
Launched an app	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain

Source: EU Commission, updated by 12 december 2020

The reasons for rejecting the adoption of an app were diverse. In Sweden for example there were both ethical and political reasons, being the first the compliance with the GDPR, and the second because the Government expected an EU App, and did not want to invest in a tool that would become obsolete (Svenonius in Meijer & Webster, 2020:p.263).

The ethical question is a fair one. Regardless of how the perception of privacy has changed due to the Covid crisis, respect for private life and protection of personal data have been recognized as fundamental rights by the Charter of Fundamental Rights of the EU (articles 7 and 8). Therefore, a framework was laid very early by the EU for these matters.

Today, competence emanates from article 16 of the Treaty on the Functioning of the EU (TFEU) which provides that the Parliament and the Council are competent in making rules by ordinary legislative procedure regarding the processing of personal data both in EU institutions and Member States. Through the TFEU, previous European regulations on data protection which were divided into two pillars[1] converged in the single GDPR. This Regulation and the ePrivacy Directive constitute the basis for any further European stand on this matter.

The Commission very early on published a recommendation 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”, calling for a common approach to support national authorities. While understanding all the benefits of implementing tracking apps, concerns arose regarding certain measures such as geolocation of individuals, health risk rating and centralization of data, all factors that directly affected fundamental rights and freedoms like the aforementioned ones of articles 7 and 8 in the Charter of the EU.

Following this recommendation, the Commission published a communication for “Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection” where it laid out several checkboxes to ensure “a trustful and accountable use of apps”. The first one calls for national health authorities (or other authorities acting on behalf of public institutions) should control the implementation and management of the apps, as well as monitor compliance with GDPR rules, data gathering and storage, and several other aspects derived from the usage of such apps (Annex 1). The importance of having national institutions be in charge of these policies derives directly from the need to ensure a minimal intervention in the private sphere of users’ digital world. The only way to guarantee rights and protection in this context of Exception is the mediation of the State, more when taking into account that these may very well be the first apps created in a context of Exception, and subject to very specific conditions.

Out of the EU Member States that have effectively implemented apps by November 2020, the management of the apps and data has not always been exclusively held by Governments, giving a variety of solutions. Most of the apps have been developed by cooperation between public institutions and IT companies, universities or other centres for research. However, the majority of countries have left management, data processing and storage to national authorities. Cooperation with private companies for such an enterprise is not only useful but necessary (since data communication depends entirely on telecommunication companies), however, Governments monitor and manage the implementation of these apps, while making sure that GDPR is being thoroughly respected.

[1] Data protection for private and commercial purposes, with the use of the Community method; and data protection for law enforcement purposes, at intergovernmental level.

Table 2. Development and management of European Member States Covid Apps

EU ME	Development	Management
Austria: Stopp Corona	-	Austrian Red Cross
Belgium: CoronAlert	Independent specialists including ICT, security, privacy and legal protection. Extensive security audit made by an external party (NVISO)	Sciensano, the Interfederal Committee for Testing & Tracing
Bulgaria: ViruSafe	Local IT	Ministry of Health
Croatia: Stop COVID-19	-	Ministry of Health
Cyprus: CovTracer	RISE- three public universities of Cyprus, the Municipality of Nicosia, and the Max Planck Institute for Informatics, Germany, and, the University College London, United Kingdom	Public health authorities
Czech Republic: eRouška	Several volunteers under the initiative Covid19CZ	Ministry of Health of the Czech Republic, the National Agency for Communication and Information Technologies
Denmark: smitte stop	Danish Ministry of Health, the Danish Patient Safety Authority, the Danish Health Authority, the Danish Agency for Digitisation and Netcompany	Danish Patient Safety Authority
Estonia: HOIA	Cooperation between the state and Estonian companies	Health and Welfare Information Systems Center
Finland: Koronavilkku	Finnish Institute for Health and Welfare	Finnish Institute for Health and Welfare
France: TousAntiCovid	Inria and the Fraunhofer Heinrich Hertz Institut, Germany	Ministry of solidarity and health, and private entities such as Inria, ANSSI, Orange and Dassault
Germany: Corona-Warn-App	Commissioned by the Federal Government, developed by Deutsche Telekom and SAP, with support of the Fraunhofer-Gesellschaft and the Helmholtz Center for Information Security (CISPA). Supervised by the	Federal Government

	Federal Office for Information Security (BSI), the Federal Commissioner for Data Protection and Freedom of Information (BfDI) and the Robert Koch Institute	
Hungary: VirusRadar	Nextsense and Ministry of Innovation and Technology	Hungarian State
Ireland: Covid Tracker	Government Team with Apple and Google	Health Service Executive and the Central Statistics Office
Italy: Immuni	Government (Minister of Health, Minister for Technological Innovation and Digitisation, the Regions, the extraordinary Commissioner for the Covid-19 emergency) and the public companies Sogei and PagoPa	Health Ministry
Latvia: Apturi Covid	Latvian ICT industry and science, experts from the University of Latvia, TechHub Riga co-founder Andris K. Bērziņš and others. The Government and the Crisis Management Council Secretariat and NATO StratCom also participated in the process of app development	Center for Disease Prevention and Control
Lithuania: Korona Stop	Instructed by the Ministry of Health, commissioned by the National Public Health Centre under the Ministry of Health	Ministry of Health
Malta: COVID Alert Malta	The Malta Information Technology Agency, in collaboration with the Ministry for Health and the Malta Digital Innovation Authority	Government of Malta
Netherlands: Corona Melder	Ministry of Public Health, Welfare and Sport in partnership with the National Institute for Public Health and Environment and the municipal health services	Ministry of Public Health, Welfare and Sport
Poland: Stop COVID	A coalition of Polish IT companies that prepared and developed it at the request of the Ministry of Digitization, which on October 6, 2020 was incorporated into the Chancellery of the Prime Minister in cooperation with GovTech Polska, under the supervision of the Chief Sanitary Inspectorate	Chief Sanitary Inspectorate

Portugal: StayAway Covid	Institute of Systems and Computer Engineering, Technology and Science and the Institute of Public Health of the University of Porto, with the support of the companies Keyruptive and Ubirider	Foundation for Science and Technology
Romania: First Contact	NGO Noi, Cetățenii, with other volunteers	NGO Noi, Cetățenii
Slovakia: ZostanZdravy	Slovak volunteers and academy members	Professional Society for the Electronic Health Cards of Citizens
Slovenia: #OstaniZdrav	National Institute of Public Health and the Ministry of Public Administration	National Institute of Public Health and the Ministry of Public Administration
Spain: RadarCOVID	Secretary of State of Digitalization and Intelligence (within the Ministry of Economy and Digital Transformation) with the support of the Ministry of Health	Secretary of State of Digital Administration

Source: own.
*UK not included as the European Commision has already excluded it from

With the European legal framework in mind, almost the entirety of the Member States (24 out of 27) have developed and implemented Covid tracking apps (only two of them managed by non-State actors, which are the cases of Austria and Romania), which amongst other functionalities, have in common the contact monitoring via Bluetooth Low Energy through smartphones, which does not register in any case where the contact took place and any of the identities. This functionality follows the guidelines set by the European Data Protection Board to trace proximity information between users, instead of the tracking of individual movements. Other functionalities vary and may include pandemic updates, health contacts or symptomatic self-assessment.

In any case, it is interesting to see how the EU as an institution has been unable to launch its own app, which in the context of free movement of persons, the foundation of the European citizenship, should be a critical issue. Even if movements are restricted due to quarantines affecting different areas, many Europeans still had to move throughout the territory, and travel restrictions were lifted in the summer months. Centralised information would better help contain the pandemic, as well as the control over who has access to the gathered data.

Policy recommendation

The creation of Covid Tracking Apps has been one of the first of its kind, being one of the digital apps for pandemics made in a context of Exception. It offers a window of opportunity for these types of policies that become a public service but have to be institutionally controlled to preserve users' rights. When citizens using apps give their consent as to the access of that application into their data, they are becoming users. This act of consent is the new social contract, therefore a whole system of checks and balances must be ensured to protect their rights, which may range from civil or social rights, to even fundamental rights which is the case here.

Also, it is important to note the dangers of falling into believing apps are neutral. In this sense, there are at least two gaps to consider (Rogers, 2001):

- First, the access gap. Not every member of society has the same access to either smartphones or internet. In the case of a Covid App this could mean certain sectors of society being more excluded from the radar, lessening its efficiency.
- Second, the usage gap. As mentioned before, there is a danger of bringing into the digital world the same discriminations already existing in the analog world (as was noted by Pateman in the Sexual Contract).

Furthermore, certain measures taken under the Exception period are probably going to stay, therefore taking this chance as an opportunity to review the new social contract, to shield users' rights, could be like using the Exception against itself.

The new normal, the previsible expansion of these type of apps, is also going to entail other issues such as, in a context determined by the information economy, who is going to gather, manage and erase the amount of data received by users, or even who is going to compensate citizens for any breaches in their privacy. In addition, these apps are going to affect systems of health, specially in mixed or public systems, while also conditioning private actors that cooperate with public administration in the design and management of the apps.

In conclusion, this document remarks the importance of thinking from a critical perspective regarding public and private spheres in a context of Exception. Institutions should monitor and innovate through public policies from the exception without damaging the rights and freedoms of EU citizens, always bearing in mind that the paradox here lies on the impossibility of guaranteeing secrecy in the digital world.

References

Agamben, G. (2005) *State of Exception*. Chicago, University of Chicago Press

Dumbrava, C. (2020) *Lifting coronavirus restrictions: The role of therapeutics, testing, and contact-tracing apps*, European Parliamentary Research Service

Fernández Barbudo, C. (2019) El nuevo concepto de privacidad: la transformación estructural de la visibilidad. *Revista de Estudios Políticos*, 185, 139-167

Meijer, A. & Webster, C. W. R. (2020) The COVID-19-crisis and the information polity: An overview of responses and discussions in twenty-one countries from six continents. *Information Polity,* 25 (2020) 243-274

Pateman, C. (1988) *The Sexual Contract*. Cambridge, Polity Press

Rogers, E. M. (2001) The Digital Divide. Convergence, 7 (4) 96–111

Legal references

European Commission (2020) *Communication: Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01*, C/2020/2523, OJ C 124I , 17.4.2020, p. 1–9. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29 [Accessed 14 November 2020]

European Commission (2020) *Recommendation: 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) 2296 final. Available at: https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf [Accessed 14 November 2020]

European Parliament & Council of European Union (2002) *Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058 [Accessed 14 November 2020]

European Parliament & Council of European Union (2016) *Regulation (EU) 2016/679*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN [Accessed 14 November 2020]

European Union (2012) *Charter of Fundamental Rights of the European Union*, 2012/C 326/02. Available at: https://www.refworld.org/docid/3ae6b3b70.html [accessed 14 November 2020]

European Union (2008) *Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT [Accessed 14 November 2020]

Web references

Apturicovid.lv (2020) *Apturi Covid*. [online] Available at: <https://www.apturicovid.lv/#en> [Accessed 14 November 2020]

Austria.info (2020) *Austria's "Stopp Corona" App Helps Your Peace Of Mind On Holiday*. [online] Available at: <https://www.austria.info/en/service-and-facts/coronavirus-information/app> [Accessed 14 November 2020]

Bundesregierung (2020) *Corona-Warn-App*. [online] Available at: <https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch> [Accessed 14 November 2020]

Coronalert (2020) *Coronalert - Stay Safe. Protect Each Other.*. [online] Available at: <https://coronalert.be/en/> [Accessed 14 November 2020]

Coronamelder (2020) *Stop the spread of the coronavirus, download CoronaMelder* [online] Available at: <https://coronamelder.nl/en> [Accessed 14 November 2020]

Covid-19.rise.org.cy (2020) *Covtracer*. [online] Available at: <https://covid-19.rise.org.cy/en/> [Accessed 14 November 2020]

COVID Alert Malta (2020) *Malta's Official Proximity Tracing App*. [online] Available at: <https://covidalert.gov.mt/> [Accessed 14 November 2020]

Covidtracker.gov.ie (2020) *COVID Tracker App - Ireland's Coronavirus Contact Tracing App*. [online] Available at: <https://covidtracker.gov.ie/> [Accessed 14 November 2020]

Erouska.cz (2020) *Erouška – I Protect Both You And Me*. [online] Available at: <https://erouska.cz/en> [Accessed 14 November 2020]

European Commission. 2020. *Mobile Contact Tracing Apps In EU Member States*. [online] Available at: <https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en> [Accessed 14 November 2020]

First Contact. 2020. *First Contact - Aplicație Avertizare Contacți.* [online] Available at: <https://first-contact.ro/> [Accessed 8 December 2020]

Gouvernement.fr (2020) *Info Coronavirus COVID-19 - Application Tousanticovid*. [online] Available at: <https://www.gouvernement.fr/info-coronavirus/tousanticovid> [Accessed 14 November 2020].

HOIA (2020) *HOIA – Protect Yourself And Your Closest Ones*. [online] Available at: <https://hoia.me/en/> [Accessed 14 November 2020]

Immuni.italia (2020) *Ripartiamo insieme* [online] Available at: <https://www.immuni.italia.it/> [Accessed 14 November 2020]

koronavirus.hr (2020) *Stop COVID-19*. [online] Available at: <https://www.koronavirus.hr/stop-covid-19-723/723> [Accessed 14 November 2020]

Koronastop.lrv.lt (2020) *Lietuvos Respublikos Vyriausybė*. [online] Available at: <https://koronastop.lrv.lt/> [Accessed 14 November 2020]

Old.korona.gov.sk (2020) *Coronavirus | Zostaň Zdravý*. [online] Available at: <https://www.old.korona.gov.sk/en/COVID19-ZostanZdravy.php> [Accessed 14 November 2020]

Portal GOV.SI (2020) *The #Ostanizdrav Mobile Application | GOV.SI*. [online] Available at: <https://www.gov.si/en/topics/coronavirus-disease-covid-19/the-ostanizdrav-mobile-application/> [Accessed 14 November 2020]

Radarcovid.gob.es (2020) *App Radarcovid*. [online] Available at: <https://radarcovid.gob.es/> [Accessed 14 November 2020]

Smittestop.dk (2020) *Download Smitte|Stop*. [online] Available at: <https://smittestop.dk/> [Accessed 14 November 2020]

StayAway COVID (2020) *STAYAWAY COVID*. [online] Available at: <https://stayawaycovid.pt/landing-page/> [Accessed 14 November 2020]

STOP COVID (2020) *STOP COVID - STOP COVID - Portal Gov.Pl*. [online] Available at: <https://www.gov.pl/web/protegosafe> [Accessed 14 November 2020]

Virusradar.hu (2020) *Vírusradar - A Koronavírus Követésére És A COVID-19 Elleni Védekezésre*. [online] Available at: <https://virusradar.hu/> [Accessed 14 November 2020]

Virusafe.info (2020) *Virusafe*. [online] Available at: <https://virusafe.info/> [Accessed 14 November 2020]

Annex 1. Elements for a trustful and accountable use of Apps according to COMMUNICATION FROM THE COMMISSION Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01)

There are ten elements, according to the Commission's communication, to ensure the transparent and controlled usage of COVID tracking apps by national Governments:

- National health authorities (or entities carrying out tasks in the public interest in the field of health) as data controller: to ensure compliance with the EU GDPR and limitations of data access and storage. Other policies, requirements and controls should also be coordinated by these authorities.

- Ensuring that the individual remains in control: the installation should be voluntary, each function should be separated and ask for specific consent, proximity data should be stored in the device and shared only under confirmation of the individual, management of the data should be appropriately transparent, user's rights under the GDPR could not be restricted without sufficient and legal reasoning, and the apps should be deactivated when fulfilled their purpose (by the end of the pandemic) without relying on the deinstallation by the users.
- Legal basis for processing: according to the ePrivacy Directive, accessing and storing information in users phones can only be done with consent of the user, or if it is necessary for the service of the app to function as requested by the user. In this case, only the first option is appropriate, as the information has to be expressly given by the user, therefore excluding tacit forms of consent. Other than compliance with the GDPR, national law should be in any case followed, to ensure legal certainty.
- Data minimisation: there's personal and location data, but both are protected by the GDPR as long as they are not anonymised. Only the data that is relevant to the intended purpose, may be processed.
- Limiting the disclosure/access of data: even health authorities should have access only to the essential information, to guide and inform citizens, which could result in a need to contact individuals via phone call, that could be done through assigning arbitrary identifiers. Supranational institutions would have access to the information provided by Member States.
- Providing for precise purposes of processing: specific, clear, public and transparent purposes depending on each app, and available to the user, such as symptom checker, self-assessment of symptoms, restraining contacts, informing contacts, etc.
- Setting strict limits to data storage: so that it is not kept for longer than necessary, based on sanitary criteria and only until it fulfills its informative purpose.
- Ensuring the security of the data: either stored in the device of every individual, or in a central server with very limited administrative access. Also using temporary user IDs that make tracking of individuals harder, making the source code of the app public, and any other measures of automatic deletion or anonymisation, besides encryption of sent data.
- Ensuring the accuracy of the data: a requirement both for its efficiency (to avoid false positives, for example) and compliance with the legislation.
- Involving Data Protection Authorities: institutions should have a role in the development of the app.