BRIEFING

European Parliament

Tracking mobile devices to fight coronavirus

SUMMARY

Governments around the world have turned to digital technologies to tackle the coronavirus crisis. One of the key measures has been to use mobile devices to monitor populations and track individuals who are infected or at risk.

About half of the EU's Member States have taken location-tracking measures in response to the spread of the coronavirus disease, mainly by working with telecommunications companies to map population movements using anonymised and aggregate location data and by developing applications (apps) for tracking people who are at risk. The European Commission has called for a common EU approach to the use of mobile apps and mobile data to assess social distancing measures, support contact-tracing efforts, and contribute to limiting the spread of the virus.

While governments may be justified in limiting certain fundamental rights and freedoms in order to take effective steps to fight the epidemic, such exceptional and temporary measures need to comply with applicable fundamental rights standards and EU rules on data protection and privacy.

This briefing discusses location-tracking measures using mobile devices in the context of the Covid-19 crisis. It describes initiatives in EU Member States and provides a brief analysis of fundamental rights standards and the EU policy framework, including applicable EU rules on data protection and privacy.

In this Briefing

- Digital technologies against pandemics
- Location tracking
- International context
- Situation in EU Member States
- Fundamental rights standards
- EU policy framework
- European Parliament
- European data protection authorities
- Outlook

EPRS | European Parliamentary Research Service

Author: Costica Dumbrava
Members' Research Service

PE 649.384 – April 2020

EN

Digital technologies against pandemics

With more than 2 million reported cases and over 130 000 deaths worldwide, the coronavirus disease (Covid-19) pandemic has pushed governments to adopt exceptional emergency measures that may have long-lasting effects on societies.

Digital technologies, including 'Big Data' analytics and artificial intelligence (AI), may help to fight the pandemic in a number of ways, including for early detection of outbreaks, tracking and monitoring the spread of the disease, predicting mortality risk, developing clinical devices and solutions (e.g. temperature sensing devices, computed tomography (CT) scanners, robots to disinfect areas), optimising clinical trials of drugs and potential vaccines; and detecting and removing virus-related misinformation online.

A growing number of governments around the world have put forward digital tracking measures aimed at mapping, monitoring, and mitigating the pandemic. Moreover, there are a number of initiatives by researchers and health organisations to develop mobile applications (apps) enabling individuals to share or donate their data to health authorities or scientific institutions in order to study disease. The European Global Navigation Satellite System (GNSS) Agency (GSA) maintains an updated repository of apps that use location data to fight the pandemic. Various companies are using AI-powered data analytics to predict and map the disease by analysing various types of online data, such as search queries and social media content.

Location tracking

Covid-19 is a highly contagious respiratory disease that can spread from person to person through small droplets from the nose or mouth, which are inhaled directly or via contact with infected surfaces. Because close proximity is essential for the transmission of the virus, stopping its spread requires adopting effective social distancing measures. That is why ensuring adherence to confinement rules is essential for their effectiveness.

Location tracking using mobile devices has been advocated as a solution in the fight against the spread of Covid-19. According to a recent research paper, being able to identify and notify contacts immediately after a person is tested positive 'has the potential to stop the spread of the epidemic if used by a sufficiently large number of people with reasonable fidelity'.

Location tracking works by accessing and analysing location and other types of data from various sources. Location data can be obtained from telecommunications companies and other digital technology companies (e.g. owners of mobile operating systems, search engines, social media platforms), or directly from mobile devices via apps that track user location. Location data can also be inferred by analysing other types of digital information such as social media content and other online behaviour. Location tracking can be done at population level – to map population movements, and at individual level – to track and monitor individuals and to identify people who are at risk.

It should be kept in mind that location tracking cannot possibly capture every interaction that could lead to infection (e.g. off-line encounters in the absence of mobile devices). For example, location tracking using mobile devices cannot account for the half of the planet's population that does not have regular internet access. Moreover, over-reliance on location tracking may also create a false sense of security among users.

Mapping population movements

Telecommunications and other digital technology companies that collect user location data can make this data available to health authorities and researchers. Such location data, in anonymised and aggregate format, can be used to map population movements in order to anticipate needs

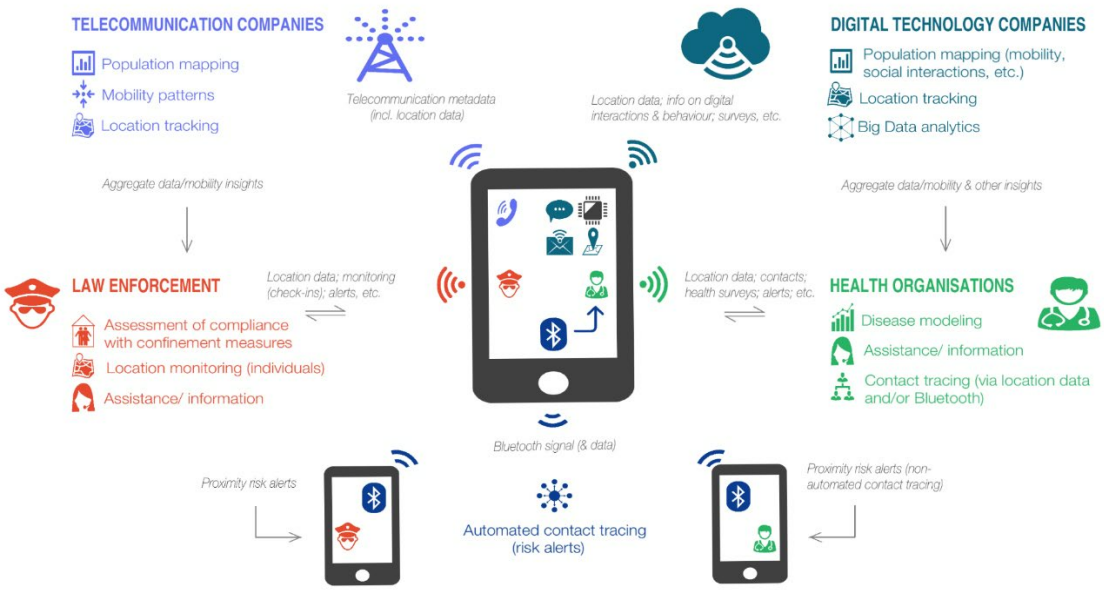
(e.g. identify risk areas) and plan public health resources, as well as to check whether social distancing measures are effective.

Telecommunications and other companies such as Google, Facebook and Uber have long compiled and shared aggregate location data, including for the purpose of fighting pandemics. During the current Covid-19 crisis, a number of companies have started to share aggregate location data and related analytics that show where and when people are gathering. For example, Google has released Community Mobility Reports showing population mobility patterns in 131 countries to help assess the effectiveness of self-isolation rules. According to Google, the reports are created with aggregate, anonymised sets of data from users who have turned on the location history setting on their accounts (which is turned off by default). Facebook has also made maps on population movements available, based on user location and social connections to inform disease forecasting efforts.

Anonymised, aggregate data may be useful for mapping population movements and thus to assess general adherence to confinement measures (which may prompt further measures from law enforcement authorities). However, reducing the spread of the virus may require more precise location data, together with additional information. A study on the 2014 west African Ebola crisis, questioned the effectiveness of location tracking in tackling epidemics, arguing that location data are most useful when cross-referenced with other data (e.g. testing and diagnostics data).

The advantage of using anonymised, aggregate data for mapping population movements is that this approach raises fewer concerns about fundamental rights, such as privacy and data protection. However, the risk of re-identifying the subjects of anonymised data is always present. A growing number of studies show the limitations of existing anonymisation practices,[1] particularly when datasets are mined using machine learning.

Figure 1 – Using mobile phones to track location and trace contacts in order to fight Covid-19



Source: Author, EPRS.

Tracking individuals

The most effective way to map the spread of the pandemic is by collecting real time data on the precise location and movements of individuals, together with information about their health. This can be done by accessing the location data collected and transmitted by mobile devices to telecommunications and technology providers, or directly by extracting the data via dedicated apps (e.g. Covid-19 apps) or other third-party apps that collect such data (e.g. e-commerce, search

engines, social media). Tracking individuals may allow more accurately verification as to whether particular individuals (e.g. persons confined to home quarantine) observe confinement orders. People may be asked to share additional information, such as health updates and images, and to 'check in' regularly (e.g. with law enforcement authorities).

Collecting and sharing individual location data for the purpose of fighting the pandemic raises important concerns about privacy and data protection, while the actual usefulness of such intrusive measures has been questioned. Measures to track individuals have been implemented by countries, such as Taiwan and South Korea, which seem to have effectively contained the virus. However, it is unclear how essential these measures have been in the context of the broader measures adopted by these countries. Taiwan, for example, had set up a public health response mechanism for dealing with pandemics following the 2003 SARS outbreak, which includes a centralised disaster management centre and an integrated information system between health and immigration authorities. The South Korean approach focuses on mass diagnostic testing.

Contact tracing

One challenge for monitoring and predicting the spread of Covid-19 is the fact that infected persons can transmit the disease before they exhibit clear symptoms. Some studies estimate that pre-symptomatic transmission accounts for about 50 % of cases. This complicates efforts to trace the people with whom an infected person has interacted while carrying the virus.

Traditionally, contact tracing has been done by interviewing infected people about their whereabouts in the period before they were tested positive, but these accounts are not always comprehensive. Analysing retrospective location data, which would have been automatically collected and stored on mobile devices, could provide more accurate tracing than individual recollection. Effective contact tracing can help in reducing the spread of the virus and may also enable people to safely re-enter public spaces.

Cross-referencing the location data of different individuals may help to identify and alert people who had been in close proximity to people who have tested positive, thus complementing traditional methods of contact tracing. However, this approach has been criticised because it is not clear how appropriate location tracking is in reducing the spread of Covid-19. This is because a mobile device is typically able to determine its position to an accuracy of between 7 and 13 metres (in urban areas), whereas Covid-19 seems to spread between people who are within a 1-metre distance. Moreover, cross-referencing individual location data typically requires building and maintaining centralised databases of personal data, which poses significant privacy and cybersecurity challenges.

Alternatively, contact tracing can be done automatically using Bluetooth – a wireless technology for short distance data exchange. This method allows data about mobile phones in close proximity to be collected and risk alerts to be sent when the owner of a given phone has been diagnosed positive.

A coalition of experts and scientists from around Europe founded the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) to develop such a decentralised and privacy-preserving technical solution for proximity tracing via smartphones. This proposal does not require the centralisation of location data and seeks to minimise the use of such data. According to a reviewer, however, the proposed solution still presents a number of privacy-related risks as 'sick people who are anonymously reported can be de-anonymised, private encounters can be uncovered, and people may be coerced into revealing their private data'.

Google has also announced that it is working with Apple to enable the development of Bluetooth-based interoperable applications (that work on devices running on different operating systems) for contact tracing. The companies are also working to build such functionality into their operating systems, which has prompted privacy concerns related to the risk of generalising contact tracing capabilities beyond the Covid-19 crisis.

International context

As Covid-19 spread globally, governments have turned to location tracking to help in monitoring and controlling the pandemic.

China obliges citizens to use an app that tracks their movement. The Alipay Health Code system combines location data and other information (e.g. a health survey) to score persons based on their contagion risk, and restrict mobility. Taiwan rolled out a phone-based electronic fence that monitors individuals' movements and alerts police if quarantine is not respected. In Hong Kong, persons who have been placed in quarantine must carry a location-tracking wristband. South Korea has launched an app to monitor people on lockdown and uses a public database of known patients (with additional information about their age, gender, occupation, and travel routes). In Thailand, people arriving at airports are obliged to download an app to help monitor their movements.

Singapore launched a contact tracing app, TraceTogether, which uses Bluetooth technology to keep a log of nearby devices. Data is encrypted and stored on the device, and persons who become symptomatic can voluntarily upload it (in pseudo-anonymised format) into a database, which the Ministry of Health uses to notify the owners of devices which have been pinged by the infected person's phone.

Israel adopted emergency regulations to allow security services to track the movements of people suspected or tested positive for the virus. It has also launched an app to track users' movements and cross-reference the information with data on infection cases. Russia entrusted its Ministry of Communications to develop a mobile-based contact tracing system to help monitor the spread of the virus. The app will request access to users' calls, location, camera, storage, network information and other data. In Iran, the Ministry of Information and Communications Technology developed an app to monitor individuals' location and collect a wide range of other data, such as mobile number, name, and gender.

In the United Kingdom, it is reported that the government is discussing with BT, the owner of one the biggest mobile operators in the country, about using phone location and usage data to monitor the effectiveness of social distancing measures. Similar discussions are taking place in the United States of America between the government and the tech industry, and reports have confirmed that government agencies have started using mobile advertising data to track the spread of the virus. Iceland has launched a voluntary app that tracks users' movements in order to help with contact tracing in Covid-19 cases.

Situation in EU Member States

Austria declared a state of emergency on 14 March 2020. In a statement of 17 March, Austrian telecom operator, A1, confirmed that it has made analyses on aggregate movement of people available to government agencies, for the benefit of the general public.

Belgium adopted emergency measures on 12 March (extended until 3 May). The Ministers for Health and Digital Agenda established a Data Against Corona Taskforce to analyse anonymised data from telecom companies to assess the spread of the virus and identify high risk areas. Initial insights using this data were already reported at the end of March.

Bulgaria declared a state of emergency over the Covid-19 epidemic on 13 March, and the National Assembly voted to extend this until 13 May. The Parliament also passed a law on measures and actions to be taken during the emergency, which among other things, amends the Communications Act to allow police to request telephone and internet operators' data on people placed under compulsory quarantine, in order to monitor their movements, trace contacts and enforce quarantine measures. Internet operators are obliged to retain user data for six months and to forward it to the police upon request. It has been reported that authorities in the city of Burgas have

deployed a drone with a thermal camera to measure the temperature of people in a neighbourhood inhabited predominantly by people belonging to the Roma minority.

Croatia declared an epidemic on 11 March. The Croatian Parliament has been debating a proposal to amend the Electronic Communications Act to make it easier for authorities to access the location data of people who are under prescribed self-isolation. The proposal was met with criticism by opposition Members and the Ombudsman over concerns about fundamental rights. It has been reported that citizens can use an app to report violations of self-isolation orders to police.

Czechia is planning to launch a 'smart quarantine system' to track the movements of persons who have tested positive. The system will require such persons to consent to share data from their mobile phones and payment cards in order to track contacts.

In **Cyprus** it has been reported that the Health Minister was preparing new measures to combat Covid-19, including that isolated cases of infected people will be monitored electronically via a wristband or possibly an ankle bracelet.

France has not taken any concrete initiative on location tracking, but it has been reported that the government is reflecting on a strategy for the digital identification of people who have been in contact with infected persons. Mobile operator Orange confirmed that it has started sharing aggregate and anonymised geolocation data with Inserm, a public research institute fully dedicated to human health, to enable them to 'better anticipate and better manage the spread of the epidemic'.

Germany is exploring introducing an app for tracking new infections and tracing contacts. According to a spokesperson for the Interior Ministry, Germany does not plan to 'evaluate and track cell phone data nationwide'. The German Justice Minister Christine Lambrecht affirmed that tracking apps to help tackle Covid-19 could only be used voluntarily. Deutsche Telekom announced that it was sharing anonymised location data of its users with the Robert-Koch Institute, a research institute and government agency responsible for disease control and prevention. In its guidelines, the Federal Data Protection Authority emphasised the sensitivity of personal data in the context of Covid-19 and reiterated the need to comply with data protection principles.

Ireland is reported to be preparing the launch of an app to facilitate contact tracing. The app will use Bluetooth technology to detect when devices are in close proximity with each other, and will store data about such contacts to facilitate contact tracing in the event of infection.

In **Italy**, government authorities have been working with mobile operators to analyse aggregate data to monitor people's movements. For example, the Lombardy region, which was greatly affected by the virus, began using anonymised location data provided by Vodafone to monitor whether people are observing the quarantine. The government has also announced the establishment of a national task force to review and select technological solutions for combating the spread of Covid-19. The Italian Data Protection Officer has issued a warning against 'do-it-yourself' data collection. To discourage people from violating lockdown orders, the Italian Civil Aviation Authority approved the use of drones by local police to monitor social distancing.

Poland declared a 'state of epidemic threat' on 13 March. The Polish Ministry of Digitalisation released an app called Home quarantine to help ensure that people observe quarantine measures. Accounts are automatically created for all those in quarantine. While in the beginning, people could choose between using the app and receiving regular police checks, the app has now become mandatory for anyone who contracted the virus or is potentially infected (e.g. people returning from abroad). Users are requested to periodically send geo-located selfies to prove they are at home. If they fail to comply, the police will be alerted. The app also gives access to relevant health information and a hotline. While the account is valid for 14 days from date of activation, the data will be retained for 6 years. The information may be shared with police, a central IT centre, and the Centre of Health Information Systems.

Slovakia passed a 'corona bill' on 25 March that allows the Public Health Office to use data from telecoms operators to track the movements of persons infected with Covid-19, and of those in compulsory quarantine, based on their consent. Police and secret services have access to this data and may be able to identify a person after obtaining a court order.

Slovenia debated a proposed law that would allow the police to monitor the location of individuals who opt for self-isolation instead of mandatory quarantine. Due to strong criticism, including from Information Commissioner Mojca Prelesnik, the law was adopted without the controversial provisions.

Spain is planning to use mobile phone location data to track people's movements in order to assess adherence to lockdown measures. A study known as 'DataCovid' will be carried out by the national statistics institute in cooperation with the country's main telecoms operators. It is reported that the Ministry of Health also intends to use location data to launch an app which will alert users to carry out a self-assessment. Such tracking apps have already been released in Catalonia and Madrid.

A more comprehensive inventory of mobile solutions to fight Covid-19 is provided in Annex IV of the common toolbox for EU Member States issued by the eHealth Network (see EU policy below).

Fundamental rights standards

Article 12 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) guarantees everyone the 'right to the highest attainable standard of health'. States parties to the ICESCR (including all EU Member States) are obliged to take effective steps for the 'prevention, treatment and control of epidemic, endemic, occupational and other diseases'. The need to protect public health may justify limiting certain rights 'in times of public emergency threatening the life of the nation'. However, such measures must be lawful, necessary, and proportionate (Siracusa Principles).

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms provides for the right to respect for private and family life. Any interference by a public authority in the exercise of this right must be 'in accordance with the law' and 'necessary in a democratic society' in order to protect the interests of national security, including public safety and 'the protection of health'.

Article 7 of the Charter of Fundamental Rights of the European Union provides for the right to respect of the 'private and family life, home and communications', while Article 8 provides for the right to the protection of personal data. According to Article 35, 'a high level of human health protection shall be ensured in the definition and implementation of all the Union's policies and activities'. Any limitation on the exercise of rights and freedoms must be lawful, proportionate, 'respect the essence of those rights and freedoms' and applied 'only if they are necessary and genuinely meet objectives of general interest recognised by the Union' (Article 52).

The Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe issued a joint statement on 30 March stressing that 'large-scale personal data processing can only be performed when, on the basis of scientific evidence, the potential public health benefits of such digital epidemic surveillance (e.g. contact tracking), including their accuracy, override the benefits of other alternative solutions which would be less intrusive'. On 7 April, the Secretary General of the Council of Europe issued a toolkit for governments across Europe on respecting human rights, democracy and the rule of law during the Covid-19 crisis.

In a joint statement published on 2 April, a group of more than 100 civil society organisations from around the world asked that 'the use of digital technologies to track and monitor individuals and populations is carried out strictly in line with human rights'. The organisations argued that 'an increase in state digital surveillance powers, such as obtaining access to mobile phone location data, threatens privacy, freedom of expression and freedom of association'.

EU policy framework

Towards a EU common approach

The Commission started a discussion with mobile phone operators on 23 March 2020, aiming to obtain anonymised mobile metadata from across the EU to map the spread of Covid-19, in a way that is fully compliant with the General Data Protection Regulation (GDPR) and ePrivacy legislation. According to the Commission, the data will be fully anonymised, will not be shared with third parties and will be stored only for as long as the crisis continues.

On 8 April, the Commission issued a recommendation on developing a common EU approach for the use of mobile applications and mobile data to support social distancing measures and contact tracing in order to limit the spread of Covid-19. The Commission stressed the need to avoid 'a fragmented and uncoordinated approach [that] risks hampering the effectiveness of measures aimed at combating the Covid-19 crisis, whilst also causing serious harm to the single market and to fundamental rights and freedoms'.

The recommendation sets up a process for developing a toolbox consisting of a pan-European approach (including aspects related to methodology, effectiveness, interoperability, security, privacy and data protection) and a common scheme for using anonymised and aggregate data on population mobility to model and predict the evolution of the disease, monitor the effectiveness of social distancing and confinement measures, and inform a coordinated strategy for exiting the crisis. The toolbox will be developed by the Member States, represented in the eHealth Network with the support of the Commission.

On 15 April, the eHealth Network issued the first iteration of a common EU toolbox. The toolbox describes the essential requirements for mobile apps dedicated to fighting Covid-19, which should be: voluntary; approved by the national health authority; privacy-preserving (personal data should be securely encrypted); and dismantled as soon as no longer needed.

On 16 April, the Commission published (legally non-binding) guidance on the development of new apps that support the fight against Covid-19 to ensure that these apps comply with EU privacy and personal data protection legislation. The Commission recommended the use of voluntary apps and the use of Bluetooth communications between devices to determine proximity because this 'appears more precise, and therefore more appropriate, than the use of geolocation data' and because this functionality 'avoids the possibility of tracking'.

The Commission stressed the need to ensure that the individual remains in control, and emphasised the necessity to use an appropriate legal basis for processing personal data that 'provides specific and suitable measures to safeguard the rights and freedoms of data subjects'.

Data protection

Regulation (EU) 2016/679 (GDPR) establishes the rules and principles for the processing of personal data and on the free movement of such data in the EU. As defined in GDPR Article 4, personal data is any information relating to an identified or identifiable natural person (e.g. names, dates of birth, photographs, email addresses, IP addresses). 'Location data' is explicitly mentioned as a potential identifier of a natural person. If location data can be related to an identified or identifiable natural person, this data is considered personal data and its processing falls under the scope of the GDPR.

The GDPR stipulates six principles that must be respected when processing personal data (Article 5). The processing of personal data should have a clear legal basis, and provide data subjects with explicit information and justification about the legitimate purpose(s). The processing of personal

Data Protection Principles (GDPR)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

data should be restricted to data that are adequate, relevant and necessary, and for 'no longer than is necessary'. Processors of personal data should ensure that the data are accurate and adequately protected against 'unauthorised or unlawful processing and against accidental loss, destruction or damage'.

Article 6 GDPR lists six grounds for the lawful processing of personal data. Apart from the case where the data subject gives consent, public authorities can lawfully process personal data if this is necessary for protecting the vital interests of the data subject or of another natural person; for performing a task carried out in the public interest or in the exercise of official authority vested in the controller; and for the purposes of the legitimate interests pursued by the controller or by a third party. Recital 46 states explicitly that 'some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics'.

Health data are a special category of personal data and require a higher degree of protection. The most relevant grounds for processing such data (Article 9 GDPR) in the context of fighting the pandemic are: individual consent; if necessary to protect the vital interests of the data subject; if necessary for reasons of substantial public interest; if necessary for the purposes of preventive or occupational medicine; and if necessary for reasons of public interest in the area of public health. When special categories of personal data are processed on the grounds of substantial public interest, the processing must be based on 'Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject'. Moreover, in line with Article 35, if processing 'in particular using new technologies ... is likely to result in a high risk to the rights and freedoms of natural persons', the controller should carry out a prior impact assessment.

The Court of Justice of the European Union (CJEU) has consistently applied the principles of necessity and proportionality in cases when the EU and the Member States have adopted digital surveillance measures. For example, in its judgment on the Digital Rights Ireland case, the CJEU declared the Data Retention Directive invalid because its requirement for telecoms and internet access providers to retain metadata on all their customers for a period of up to two years for intelligence and law enforcement purposes disproportionately affected privacy and data protection rights.[2]

ePrivacy

Directive 2002/58/EC (ePrivacy Directive), which is currently in the process of being amended, sets out the rules on how providers of electronic communications services, such as telecoms companies and internet service providers, should manage their subscribers' data, and guarantees the rights of subscribers. The Member States must ensure the confidentiality of communications over public networks, while the providers of public electronic communications services have to take appropriate measures to safeguard the security of their service.

Article 9 of the ePrivacy Directive provides that location data other than traffic data 'may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service'. The service provider has the obligation to inform users or subscribers of the type of location data that will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party.

According to Article 15 of the ePrivacy Directive, Member States may adopt legislative measures to restrict the scope of the rights and obligations provided in Article 9. This is permitted 'when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system'.

Medical devices legislation

Mobile applications used to fight the spread of Covid-19 may potentially be classified as medical devices, in which case they will have to comply with specific safety rules. According to the provisions of Regulation (EU) 2017/745 on medical devices (MDR), an app could be deemed a medical device if it is intended by the manufacturer to be used, inter alia, for diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease.

The MDR was supposed to enter fully into force in May 2020, but on 3 April, the Commission adopted a proposal to postpone its application date for one year, to allow Member States, health institutions and economic operators to focus on fighting the pandemic. Parliament voted to approve that proposal on 17 April. The date of the repeal of the currently applicable Directive on medical devices will also be postponed by one year.

European Parliament

The European Parliament has played a key role in shaping EU legislation in the field of personal data protection by making the protection of privacy a political priority. It has consistently insisted on the need to strike a balance between enhancing security and safeguarding fundamental rights, including data protection and privacy.

In a statement issued on 7 April 2020, the Chair of the Civil Liberties Committee, Juan Fernando López Aguilar (S&D, Spain), recalled that the use of smartphone data to tackle the spread of Covid-19 needs to comply with data protection and privacy rules. He stressed that applications used to trace individuals' location and contacts 'could seriously interfere with people's fundamental rights to a private life and the protection of personal data, and are tantamount to a state of surveillance of individuals'. He also called on national data protection authorities to follow current developments closely and on the European Data Protection Board to adopt clear guidance.

European data protection authorities

The European Data Protection Supervisor (EDPS) maintained, in his statement of 19 March 2020, that 'emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period'. He also stated that 'if such measures are introduced, a Member State is obliged to put in place adequate safeguards, such as granting individuals the right to judicial remedy'. In a letter addressed to the Director-General of the European Commission's Directorate-General for Communications Networks, Content and Technology, concerning the Commission's plans to collect anonymised and aggregate location data from telecoms companies, the EDPS asked the Commission to 'clearly define the dataset it wants to obtain and ensure transparency towards the public, to avoid any possible misunderstandings'. He cautioned about relying on third parties to process the information, which need to comply with strict security and confidentiality obligations. The EDPS also maintained that extraordinary measures should be temporary and that the data from mobile operators should be deleted as soon as the current emergency ends.

On 6 April, the EDPS released a statement recalling that any EU or national measures should always respect a number of fundamental principles, including the fact that measures to address the pandemic and with reference to data protection should be temporary with a specific purpose. He also called for a pan-European model of a Covid-19 mobile application, coordinated at EU level.

The Chair of the European Data Protection Board (EDPB) issued a statement on 19 March 2020, saying that data protection rules 'do not hinder measures taken in the fight against the Covid-19 pandemic'. However, she recommended that 'public authorities should first seek to process location data in an anonymous way' and recalled that 'Member States are obliged to put in place adequate safeguards, such as providing individuals of electronic communication services the right to a judicial remedy.' The measures taken should be proportionate and as un-intrusive as possible. The

processing of historical non-anonymised location data is an invasive measure that could be considered proportional only under exceptional circumstances. Such measures need to be subject to 'enhanced scrutiny and safeguards to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation)'.

On 7 April 2020, the EDPB issued a mandate to its expert subgroups to develop guidance on the issues of geolocation and other tracing tools and the processing of health data for research purposes in the context of the Covid-19 outbreak.

Outlook

Together with other digital technologies, location tracking using mobile devices tracking can support measures to fight the spread of Covid-19, in particular by mapping population movements, monitoring the effectiveness of confinement measures, identifying and assisting people, and supporting crisis exit strategies. However, before rolling out such digital solutions, there is a need to carefully assess their technological readiness, effectiveness and implications on fundamental rights.

There are both legal and technological limits with regard to using location data, in particular when this involves the systematic tracking of individual movements. That is why the use of anonymised and aggregate location data is preferable to individual monitoring. Location tracking using mobile applications and alternative solutions based on Bluetooth signals may support contact tracing efforts to identify people at risk. However, the effectiveness of such apps crucially depends on the number of people who are willing and able to use them effectively. The legal and technical aspects of this problem include the need to address key issues related to privacy and security, as well as interoperability. The social aspect of the challenge is that people need to trust that the solution is safe and effective before committing to using it. Upholding fundamental rights standards and adopting effective and transparent public policies are key to ensuring public trust.

Location tracking measures that involve the collection, sharing and analysis of location and related data raise a number of important concerns about fundamental rights, in particular about data protection and privacy. In emergency situations, such as the Covid-19 crisis, Member States may impose limitations on certain rights and freedoms in order to pursue quick and effective measures. However, such measures need to comply with fundamental rights standards and EU law. When it comes to processing personal data, this is lawful only if the processing is necessary for the purpose of achieving a legitimate purpose (e.g. substantial public interest) and on the basis of Union or Member State law which is proportionate to the aim pursued. To limit the impact of emergency measures beyond the crisis it is essential that such measures are designed to be and remain exceptional and temporary. It must be stressed that limitations of fundamental rights, even if justified in exceptional situations, create the risk of broader erosion of fundamental rights and of democratic checks and balances, with negative consequences beyond the crisis.

Despite the challenges, the Covid-19 crisis could be an opportunity to reaffirm the EU's commitment to fundamental rights, as well as to reaffirm the bloc's solidarity and its ability to strike a fair balance between the important values of privacy and security.

MAIN REFERENCES

Ferguson, C., European Union response to coronavirus threat, EPRS, European Parliament, March 2020.

Milt, K., Personal data protection achievements during the legislative term 2014-2019: the role of the European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, April 2019.

Kritikos, M., What if we could fight coronavirus with artificial intelligence?, EPRS, European Parliament, March 2020.

Kurrer, C., What if smartphones could help contain COVID-19?, EPRS, European Parliament, March 2020.

Monteleone, S., Reform of the e-Privacy Directive, EPRS, European Parliament, September 2017.

ENDNOTES

[1] P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review*, 1701, 2010.

[2] J. Frederik, Z. Borgesius and W. Steenbruggen, 'The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust', *Theoretical Inquiries in Law*, vol. 19, 2019.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)