ERA Forum (2020) 21:379–393
https://doi.org/10.1007/s12027-020-00629-3

ARTICLE

Privacy in emergency circumstances: data protection and the COVID-19 pandemic

Emanuele Ventrella[1]

Published online: 28 September 2020

Abstract The way we conceive our privacy and the importance which we attach to the protection of our personal data has been heavily impacted by the COVID-19 pandemic. By first providing legal insights on the general discussion about the balance between the fundamental right to privacy and the general public interest, this article describes the most critical and controversial processing operations employed by states to contain the pandemic and mitigate its effects. A focus on the increase in cybercrime during the pandemic then provides insights on the relevant risks and remedies for the security of personal data.

Keywords Privacy · Cybercrime · GDPR · Contact tracing · Covid-19

1 Introduction

In the span of just a few months, the COVID-19 pandemic has changed the way we work, socialise and think, impacting almost every aspect of our economy, society and mental health. The way we conceive our privacy and the importance which we attach to the protection of our personal data has also been heavily impacted by this groundbreaking event. As it has put into perspective other fundamental rights which until then we would never have accepted seeing restricted by state measures, the pandemic has required us to balance privacy with health and security.

By first providing legal insights on the general discussion about the balance between the fundamental right to privacy and the general public interest, this article will describe the most critical and controversial processing operations employed by states

✉ E. Ventrella
emanuele.ventrella@trilateralresearch.com

1 Data Protection Advisor, Trilateral Research Ltd., London, UK

to contain the pandemic and mitigate its effects.[1] A detailed focus on the European approach to such methodologies and technologies will demonstrate how the highest standards in terms of privacy and data protection can still be maintained, even in exceptional circumstances. Finally, in analysing the increase in cybercrime-related risks to the security of personal data during the pandemic, the article will delineate examples of technical and organisational measures that can be implemented as remedies.

2 Privacy in emergency circumstances

2.1 The fundamental right to privacy and the general public interest

In order to conscientiously analyse the privacy implications of the COVID-19 pandemic, a preliminary and general discussion on privacy and personal data rights is necessary in order to ensure the temptation of partisan argumentation is resisted. Privacy and the right to data protection are fundamental rights, yet they are not absolute rights. According to philosophical tradition, a right is absolute when it outweighs every other element, including other rights and freedoms, including the moral imperative of saving human lives, and the protection of the efficiency of an economic system.[2] States of emergency, national interests, and exceptional circumstances have in the past allowed for temporary limitations of fundamental rights such as the right to privacy. Having been defined as "a threat for every country, rich and poor" by the Director-General of the World Health Organisation (WHO), the COVID-19 pandemic is an exceptional circumstance which led countries worldwide to declare states of emergency.[3]

According to Art. 52(1) of the Charter of Fundamental Rights of the European Union, limitations on the exercises of the rights and freedoms recognised by the Charter may be made only if they genuinely meet *objectives of general interest* recognised by the Union.[4] Specifically concerning privacy, Art. 8(2) of the European Convention on Human Rights enumerates the legitimate aims that may justify an infringement upon the right to respect for private and family life

> "[...] in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection

[1] Preliminary versions of the first two sections of this article were published in the form of blogposts by Trilateral Research Ltd: "COVID-19 and Data Protection in Emergency Circumstances", 16 March 2020 (available at: https://www.trilateralresearch.com/covid-19-and-data-protection-in-emergency-circumstances/) "Desperate times call for desperate measures? Understanding the privacy risks of digital-contact tracing in the COVID-19 fight", 2 April 2020 (available at: https://www.trilateralresearch.com/dpo/desperate-times-call-for-desperate-measures-understanding-the-privacy-risks-of-digital-contact-tracing-in-the-covid-19-fight/).

[2] For a complete discussion on rights and highlighting the difference between absolute and fundamental rights, see *Wenar* [22].

[3] WHO Director-General's opening remarks at the media briefing on COVID-19, 5 March 2020 (available at: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—5-march-2020).

[4] Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

of health and morals or for the protections of the rights and freedoms of others."[5]

The European Union General Data Protection Regulation (henceforth GDPR or Regulation)[6] adds details to these considerations. Recital 4 provides that data protection should always be considered in relation to its function in society and balanced against other fundamental rights. In addition, Art. 23(1) GDPR allows Member States to restrict data subject rights, as well as the data protection principles outlined in Art. 5 GDPR, as long as this is done by way of a legislative measure and respects the essence of those same fundamental rights and freedoms. These restrictions, provided that they are embodied in necessary and proportionate measures of a democratic society, should aim to safeguard, among other things, "important objectives of general public interest [...] including monetary, budgetary and taxation matters, public health and social security".[7]

2.2 The need to process personal data during a pandemic

In the specific circumstances of a pandemic, processing personal data is necessary in order to take appropriate measures to contain the spread of the virus and subsequently mitigate its effects.[8] First, the processing of certain types of personal data (such as name, home address, workplace, travel information) can be useful to understand whether an individual might have visited affected areas or met with people exposed to the virus. Secondly, the processing of special categories of personal data (such as health data, including diagnostic test results) is crucial to understand whether an individual shows infection-related symptoms.

Data controllers, be they public or private organisations, continue to be subject to standard data protection rules even in emergency circumstances. In the first place, their obligation to rely on a legal basis remains essential to guarantee the lawfulness of processing operations. Relevant personal data other than special category data can be processed for the purposes outlined above in accordance with both Art. 6(1)(d) and (e) GDPR. While the first legal basis allows processing personal data that is necessary to protect the vital interest of individuals (*i.e.*, to save lives), the second can be relied upon to safeguard the public interest or in the exercise of official authority vested in the controller. Given that public interest can only be determined by the law of the Union or of a Member State, Recital 46 GDPR explicitly mentions the monitoring of epidemics as circumstances in which the processing may serve both important grounds of public interest and the vital interest of data subjects.[9]

[5] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[7] Art. 23(1)(e) GDPR.

[8] *Ienca, Vayena* [11].

[9] Recital 46 indeed clarifies that '[s]ome 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 hu-

Concerning health data, a legal basis for processing can be found in Art. 9(2)(i) GDPR, and further guidance is provided by Recitals 52 and 54 GDPR. According to the Regulation, the processing of special categories of personal data is permitted when it is necessary for reasons of public interest in the area of public health, "such as protecting against serious cross-border threats to health".[10] To make this legal basis actionable, not only guidance and directions are to be provided by public health and other relevant authorities, but also suitable, specific safeguards should be implemented due to the sensitivity of these categories of data.

Although it might seem that controllers have ample room for manoeuvre when choosing the appropriate legal bases for processing personal data to contain the spread of a virus, an assessment on proportionality remains the cornerstone in the application of measures that should neither be excessive nor discriminatory. Proportionality considerations should assist in prioritising and safeguarding the human dignity of individuals. For example, divulging the identity of a vulnerable person (such as an individual tested positive for the virus) is rarely necessary and – in most cases – alternative measures that avoid the identification of individuals could be equally effective in warning others of potential exposure.

3 Tracking individuals to contain the spread

3.1 The use of location data and digital contact tracing

During recent outbreaks, such as SARS in 2003, information and communication technology (ICT) tools were deployed to rapidly detect sources of infection, clusters of cases and transmission routes.[11] The COVID-19 pandemic facilitated the dissemination of these methods and instruments, specifically through the use of location data to support the response to the pandemic and by means of tracing contacts of affected individuals to limit the spread of the virus.

First, location data was collected for the purpose of producing statistics on the aggregated movement of individuals, irrespective of their health status.[12] Such data would allow governments to monitor and assess the overall effectiveness of their containment measures (*e.g.*, lockdowns). The use of location data implies that electronic communication service providers or information society service providers' applications would share aggregated and anonymised datasets indicating the geographical

manitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situation of natural and man-made disasters.'

[10] Art. 9(2)(i) GDPR. Additionally, Recital 54 specifies that 'public health should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the cause of mortality'.

[11] *Ting, Carin, Dzau et al.*, [20].

[12] For example, Google has provided COVID-19 Community Mobility Reports, aimed at providing movements trends over time in response to policies aimed at combating the spread of the virus in over 139 countries worldwide. For additional information, see https://www.google.com/covid19/mobility/.

position of terminal equipment (*e.g.*, a smartphone) with public officials, allowing them to track population movements. Although using such techniques would require efforts to remove the ability of linking the data with identified or identifiable natural persons, research has shown that anonymising location data is harder than expected since mobility traces of individuals are inherently unique and highly correlated.[13]

Secondly, contact tracing is a monitoring process employed to prevent further transmissions of viruses and which aims to trace back people who have been in close contact with someone who is infected. It can be broken down into three basic steps:[14]

1. contact identification: the practice of identifying contacts, usually by asking about the infected person's activities and the roles and activities of the people around them.
2. contact listing: the practice of listing contacts of an infected person, informing them of the meaning of their contact status, as well as the necessity to take appropriate measures like quarantine or voluntary isolation.
3. contact follow-up: the practice of regularly following-up with all contacts to monitor symptoms and tests for signs of infections.

Traditionally carried out through questionnaires and interviews to infected people, in recent years contact tracing has started to rely also on ICT.[15] With COVID-19, the employment of ICT tools has become increasingly common and countries across the world have placed confidence in 'digital contact tracing apps' to mitigate the consequences of the emergency. With the exception of China and few other countries, such tools have not included the processing of location data and have tried to avoid the collection of extensive amounts of data in a centralised server.[16]

For example, the most commonly implemented digital contract tracing systems have required the installation of an app on the smartphones of as many people as possible.[17] For it to work effectively, the majority of the population of an affected country has needed to be involved, including individuals with symptoms, people in quarantine or isolation, people travelling to high risk areas, or simply whoever wanted to get alerts on the overlaps of their activity maps with those of infected individuals.

By first cryptographically generating temporary identifiers every few minutes, these kinds of apps would use Bluetooth Low Energy Technology to detect whether two smartphones, and therefore two people, have come into close physical proxim-

[13] *Thompson, Warzel*, [21]. For an analysis about the privacy-related benefits of aggregated location data, see *Hoffman-Andrews, Crocker*, [10].

[14] The three steps-definition of contact tracing is implemented in WHO reports and publications. A complete definition is available at *WHO* [23].

[15] Among the first smartphones' applications developed for contact tracing, the Go.data app was launched during the Ebola outbreak in the Democratic Republic of Congo. Additional information is available at: https://www.afro.who.int/news/speeding-detection-slow-down-ebola-smartphone-app-game-changer-contact-tracing-hotspots.

[16] Contact tracing applications processing location data have been implemented in China (*Mozur, Zhong, Krolik* [15]) and South Korea.

[17] Epidemiologists and researchers at the University of Oxford have found that to radically reduce the number of infections, about 56% of the population or about 80% of smartphone users should use the app. *Servick* [18].

ity.[18] Once this proximity is reached and maintained for long enough to represent meaningful contact, the two apps would share the identifiers among each other. An encrypted list of logged identifiers would then be stored locally on the phone. In case an app user is diagnosed with COVID-19, a verification method involving healthcare professionals would confirm the health status of the affected individual without keeping records on his or her identity. The list of contacts would then be shared in a secured way with public authorities.[19]

When someone's phone is included in the list of identifiers held by an individual diagnosed with COVID-19, that someone would receive a notification by public authorities, together with follow-up information as to whether quarantine or self-isolate. This potentially affected individual would then be required contact local health authorities to monitor symptoms and get tested for the virus. The sooner this testing takes place, the faster public authorities would be able to trace additional contacts related to this person.

3.2 The European approach

Since the use of location data and digital contact tracing apps to manage the health crisis has been implemented first in countries that are often criticised for a suboptimal protection of individual rights, privacy experts in Europe have looked with a certain degree of suspicion at their possible implications. The most common objection concerned the intrusiveness of these measures as well as their power to enable mass surveillance, creating a dangerous environment that could allow governments to continue collecting sensitive information well beyond the emergency.[20] Nonetheless, Data Protection Authorities in the EU and the European Data Protection Board (EDPB) have underlined how data protection rules should not and are not intended to hinder the measures that need to be implemented in the fight against the COVID-19 pandemic.[21] On the contrary, data protection should be considered an essential tool in building the necessary social trust that guarantees the effectiveness of these measures.

[18] *Ferretti et al.* [9].

[19] When a user is declared infected, contact tracing applications can send to a server either the history of proximity contacts that has been obtained through scanning, or the list of their own identifiers that were broadcasted. This contributes to the difference between centralised and decentralised approaches to digital contact tracing. Under the centralised approach, the identifiers of the infected user and those of its contacts are stored in a central database, enabling increased visibility of the data by governments and health services. Examples of such approach have been implemented in France and the UK. Under the decentralised approach, identifiers are generated by the user's phone and only the identifiers broadcasted by the infected user are shared with the backend server. Examples of this approach are countries adopting the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) protocol. *DP-3T* [5]. On 10 April 10 2020, Apple and Google announced the development of application programming interfaces (APIs) in support of the decentralised approach.

[20] *Ram, Gray* [17]. *Amit, Kimhi, Bader et al.* [1].

[21] Since February 2020, multiple national supervisory authorities have released guidance on their websites to tackle the processing of personal data in the context of the COVID-19 pandemic. On 19 March, the European Data Protection Board adopted a formal statement on the topic *via* written procedure. The full statement is available at: https://edpb.europa.eu/our-work-tools/our-documents/outros/statement-processing-personal-data-context-covid-19-outbreak_en.

Concerning the use of location data, national laws implementing the Directive on privacy and electronic communication (henceforth ePrivacy Directive) [22] set the conditions to lawfully process traffic and location data.[23] While the first can only be shared with public authorities or other third parties once it has been anonymised by electronic communication service providers, the latter always needs the prior consent of users to be transmitted. Where the information is directly collected from the user's device, such as location data, the access to this information must be strictly necessary to provide information society services that have been explicitly requested by informed users. It is important to notice that, where location data is effectively anonymised, that data is no longer personal data and can be processed without taking into consideration the obligations of the GDPR.[24] Additionally, in accordance with Art. 15 of the ePrivacy Directive, exceptional legislative measures adopted by Member States can restrict the scope of the rights and obligations provided by the ePrivacy regime.[25] These national legislative measures should have the sole purpose of safeguarding public security, and would only allow restrictions that constitute a necessary, appropriate and proportionate measure within a democratic society. At the same time, Member States should put in place adequate safeguards to guarantee, among other things, the right to a judicial remedy for users of electronic communication services.

With specific regard to digital contact tracing applications, the European Data Protection Board has defined a "grave intrusion into people's privacy" the large-scale monitoring of contacts between natural persons.[26] For this reason, it has conditioned the legitimacy of such instruments to the voluntary adoption by the users, as well as to the respect of precise technical and privacy-related requirements and obligations. While the voluntariness of such tools represents a pre-condition allowing data subjects to decide freely whether or not to use the applications (without suffering from

[22] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in electronic communications sector.

[23] Art. 6 and Art. 9 ePrivacy Directive.

[24] According to the European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak [6], for anonymisation to be effective it should pass the "reasonability test" and be able to remove the ability to link the data with an identifiable natural person against any "reasonable" effort. Three criteria should be taken into consideration to evaluate the robustness of anonymisation: (i) singling-out (*i.e.*, isolating the individual from the group); (ii) linkability (*i.e.*, linking two records concerning the same individual together); and (iii) inference (*i.e.*, deducing previously unknown information about the individual with significant probability).

[25] According to Art. 15(1) ePrivacy Directive,

> 'Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restrictions constitute 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 electronic communication systems, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member states may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on the European Union.'

[26] *European Data Protection Board Guidelines 04/2020* [6].

any disadvantage in case they refuse to use it), the other requirements interrelate legal considerations with functional recommendations. These requirements, as outlined by the European Data Protection Board, are illustrated and summarised in the following sub-sections.

3.2.1 Lawfulness, fairness and transparency

Contact tracing applications involve the storage and/or access to information stored in terminal equipment. For this reason, such applications must process information in compliance with Art. 5(3) ePrivacy Directive.[27] Insofar as concerns the GDPR, where the processing employed by contact tracing applications does not involve special categories of personal data, the recommended legal basis for such processing can be found in Art. 6(1)(e) GDPR (*i.e.*, public interest). On the other hand, where these applications involve the storage of health data (*e.g.*, in order to monitor the health status of an infected individual), in addition to the above legal basis, Art. 9(2)(h), or (i) can allow such processing on the basis of it being necessary for the purposes of preventive or occupational medicine and healthcare, or for reasons of public interest in the area of public health. While consent[28] and explicit consent[29] still represent valid legal bases for the processing of personal data and special categories of personal data in the context of contact tracing applications, the mere fact that the use of such applications takes place on a voluntary basis does not imply that these are recommended legal bases. In fact, where controllers decide to rely on consent and explicit consent, the strict requirements making such legal bases valid must be met.[30]

Insofar as concerns transparency, for digital contact tracing applications to be compliant with the EU data protection regime, users should have a clear understanding of what is entailed in the use of such applications at any time and should always remain in control of their data. For this to be possible, users must be provided with clear and understandable information about the processing, as well as with the option to exercise their data subject rights *via* the application itself.

3.2.2 Purpose limitation

According to the European Data Protection Board, the purpose of digital contact tracing applications must be that of supporting, and not replacing, manual contact tracing

[27] According to Art. 5(3) ePrivacy Directive, the use of electronic communication networks can be only allowed on condition that the concerned user is provided with comprehensive and clear information about the processing. Where the processing is strictly necessary to provide a service explicitly requested by the user, explicit consent is not required.

[28] Art. 6(1)(a) GDPR.

[29] Art 9(2)(a) GDPR.

[30] On 4 May 2020, the European Data Protection Board published an updated version of its Guidelines 05/2020 on consent under Regulation 2016/679 [7]. The Guidelines detail the elements of valid consent: that it be freely given (absence of imbalance of power, absence of conditionality, absence of detriment), specific (specification of purposes against function creep, granularity, separation of information about data processing and other matters), informed, and an unambiguous indication of wishes. The higher standards required for explicit consent are also detailed, specifying how signed statements are not the only way to give an express statement of consent.

performed by qualified health personnel. Applications must be part of a wider public health programme and used only until the point when traditional contact tracing can alone be employed to manage the amount of new infections. Purposes must be specific enough to exclude further uses of these tools, avoiding that apps can be subsequently implemented for commercial or law enforcement purposes that are unrelated to the management of the COVID-19 health crisis. The monitoring of compliance with quarantine and confinement measures, or the overall drawing of conclusions on the location of the user, should be excluded from the available purposes of digital contact tracing applications.

3.2.3 Data minimisation

The amount of data processed or exchanged by contact tracing applications must be reduced to the strict minimum. Where the application requires the use of a centralised server, the data processed by that server should be limited. Unrelated information or information which is not needed (such as communication identifiers, messages, call logs, *etc*.) should not be collected. Information on users' proximity to one another can and should be collected without processing location data. Other than to the extent to which it is strictly necessary, health data should not be collected except on an optional basis and for the purposes of contact follow-up: *i.e.*, assisting in the decision-making process of informing the user.

3.2.4 Accuracy

Although the occurrence of false positives could be unavoidable, contact tracing applications must necessarily employ methods of data correction and/or verification of subsequent analysis results. Since the erroneous identification as a virus carrier can have a high impact on individuals (*e.g.*, being forced to self-isolation until tested negative), risks to data accuracy must be clearly communicated to the data subject. By inviting developers to keep open the source code of the application and that of its backend, and making publicly available its technical specifications, the European Data Protection Board indicates its wish that any concerned party would audit the code. Wide scrutiny, by stimulating improvements in the code, can also contribute to ensure transparency and correct possible bugs. An evaluation protocol should be developed to ensure the effectiveness of the application from a public health viewpoint is progressively validated throughout all stages of deployment.

3.2.5 Storage limitation

The pandemic should not be used as an excuse to put in place disproportionate data retention mandates. The principle of storage limitation should be respected by taking into consideration the true medical needs for storing data (*e.g.*, epidemiology-led justifications such as incubation periods). Once the COVID-19 crisis is over, as a general rule, all personal data kept and processed by contact tracing applications should be anonymised or erased. The "return to normality" must include a strategy to stop the collection of identifiers (*e.g.*, by automatically uninstalling or deactivating

the application), initiating a process to delete all collected data from all both mobile applications and servers' database. Deletion of the application must coincide with the deletion of all locally collected data.

3.2.6 Integrity and confidentiality

Although the European Data Protection Board has endorsed both decentralised and centralised approaches for digital contact tracing applications, the initial phase of the app development should include accurate considerations of the advantages and disadvantages of these approaches.[31] Adequate security measures should be put in place to make sure possible disadvantages and risks to individuals are mitigated. To secure the data stored in both servers and applications, state-of-the-art cryptographic techniques must be implemented.[32] The adoption of mutual authentication methods between servers and applications can be used to avoid impersonation and the creation of fake users.

The use of the application should not allow users to be directly identified by other users. Potentially exposed individuals can be identified by public authorities only with their agreement. The status of users who report as having tested positive for the virus in the application must be verified in a secure way by, for example, providing a single-use code linked to healthcare professionals.

3.2.7 Accountability

The controller of any contact tracing application should be determined to ensure accountability. While in some cases national health authorities could be the designated controllers, other controllers may also be envisaged. Where multiple digital contact tracing applications across EU Member States are interoperable, any operation or set of operations for the additional purpose of ensuring interoperability beyond the national level should be assessed separately.[33] This additional and separate processing should have individual controllers or joint controllers clearly identified.

Where the implementation of digital contact tracing applications involves different actors, be they private or public entities, their roles and responsibilities should be carefully outlined, making sure users are informed. The importance of determining roles, responsibilities and relationships has to be considered in light of guaranteeing the exercise of data subject rights.

[31] The European Data Protection Board has also taken the view that a decentralised solution is more in line with the data minimisation principle and that trust in a central server must be limited. Clearly defined governance rules must be determined to manage the central server and ensure its security, including making the access to all data stored in the central server restricted to authorised persons only. Nonetheless, according to research, decentralised infrastructures promoting individual privacy and autonomy can also become vulnerable to corporate or governmental surveillance like their centralised counterparts (*De Filippi*, [3]).

[32] Examples of techniques that can be implemented include: hash functions, symmetric and asymmetric encryption, homomorphic encryption, Bloom filters, *etc*.

[33] The European Data Protection Board has invited Member States to develop applications that are interoperable with other applications across the EU, so that users travelling across multiple Member States can continue be notified efficiently.

Since the processing of personal data resulting from digital contact tracing applications is likely to produce high risk to the rights and freedoms of data subjects, a data protection impact assessment (DPIA) should always be carried out prior to their deployment.[34]

4 The security of personal data during the pandemic

4.1 The rise in COVID-19-related cybercrime

According to the most recent annual cybercrime report by Cybersecurity Ventures, cybercrime is soon going to replace traditional crime in terms of scale and costs. Growing both in frequency and severity, it is estimated cybercrime will cost the world $6 trillion annually by 2021 (up from $3 trillion in 2015).[35] Representing fertile ground for cybercriminal activities, the COVID-19 pandemic has contributed to this trend by generating a set of unique circumstances that have exposed the vulnerabilities both of society and of organisations. On the one hand, the stress and anxiety caused by the crisis (*e.g.*, the mental health issues caused by the lack of social interactions and physical activity during long periods of lockdown or quarantine) have increased the chances of becoming a victim of opportunistic untargeted attacks.[36] On the other, the fact that organisations have had to adapt in order to survive to the unique societal challenges brought by the pandemic (*e.g.*, the rapid shift from the physical office to the online virtual workplace) has left assets less protected than before for the sake of impulsive and unprepared business continuity.[37]

Both at individual and organisational level, social engineering has represented a useful resource in the hands of cybercriminals, especially during the pandemic. Social engineering is defined as: "the science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity."[38] Being, as they are, the backbone of phishing, social engineering techniques have been implemented by cybercriminals to capitalise on the anxieties and fears of their victims and exploit the pandemic for scams and attacks. In March 2020, phishing was reported to have increased by 600%.[39] Although taking various forms, phishing attacks share the common purpose of convincing individu-

[34] DPIAs for contact tracing apps have been carried out and released by multiple Member States adopting digital contact tracing solutions. In May, it was reported that the UK's NHS Test and Trace Service failed to complete the required DPIA prior to launching the app: https://www.politico.eu/article/uk-test-trace-privacy-data-impact-assessement/.

[35] *Cybersecurity Ventures*, [2].

[36] Opportunistic untargeted attacks are attacks that base the selection of the victim on their susceptibility to be attacked. *Dhanjani, Rios, Hardin* [4], p. 223.

[37] *Panebianco* [16].

[38] *Mouton et al.* [14].

[39] *Shi* [19].

als to give access to information (in most cases personal data), providing fraudulent opportunities both in the cyber and in the real world.

As soon as the COVID-19 pandemic started, malicious actors began registering domains containing the words 'coronavirus', 'covid19' and 'corona'.[40] Using these domains, it was possible for cybercriminals to impersonate government organisations, national health institutions or the WHO, convincing individuals to perform actions under the illusion they were engaging with a legitimate party.[41] Fake institutional websites were used to promise useful information, practical help, as well as opportunities to donate money in solidarity during the crisis. By also attentively following global trends and news, cybercriminals took advantage of the various governmental announcements of policies in support of the citizenry and the economy to spread phishing emails or text messages. In these communications, criminals would share malicious links with individuals who, by entering their personal data, would then fall victims to financial fraud.

Malicious websites have also been used to install malware (*i.e.*, malicious software that can be used to extract data, disrupt service, *etc*.). Among the most relevant malware examples employed during the pandemic, was that malicious actors installed a java-based malware to a copy of the map released by John Hopkins University to track the expansion of the virus across the world.[42] Once the plugin was downloaded, the malware would then gain remote access of user's system, device photos, videos and location data. Other notable examples included fake digital contact tracing apps, employed both in Italy and in Canada that, when installed, took hostage the files on a device by encrypting the data stored in it.[43] If the user wanted to re-gain access to its data, the perpetrators would request a payment (usually in the form of bitcoins).

The latter is the typical example of ransomware, the most common attack on organisations. Normally, cybercriminals would take high-value data and operational assets hostage in order to increase their chances of receiving payments/ransoms. Hospitals, health centres and public institutions have been the preferred target of these attacks during the crisis, since they could not afford to be deprived of their data and systems in such critical circumstances and would be willing to pay. The stretching of resources and personnel numbers in the response to the medical emergency, the COVID-19 pandemic, and the related rise in cybercrime, has demonstrated how the healthcare sector represents the most fragile component of a nation's critical infrastructure.[44]

[40] On 3 April 2020, the European Union Agency for Law Enforcement Cooperation (Europol) published a report on the impact of the COVID-19 pandemic on the cybercrime landscape. The report describes registered domain names as the backbone for many criminal operations. *Europol* [8], p. 6.

[41] *Lallie et al.* [13].

[42] The story of the malware is described in *Mouton et al.* [14]. The original map and coronavirus resource centre is available here: https://coronavirus.jhu.edu/map.html.

[43] Additional information on the Canadian case are available here: https://www.zdnet.com/article/new-crycryptor-ransomware-masquerades-as-covid-19-contact-tracing-app-on-your-device/. Information on the Italian ransomware (named 'FuckUnicorn') is available here: https://www.cybersecurity360.it/nuove-minacce/ransomware/immuni-attenti-alla-finta-app-anti-covid-distribuita-via-e-mail-e-un-ransomware/.

[44] *Khan, Brohi, Zaman* [12].

4.2 Securing personal data through technical and organisational measures

In most cases, cyber threats such as those mentioned in the previous section have an impact on the confidentiality, integrity, or availability of personal data. For this reason, they would probably result in personal data breaches and consequentially force data controllers to act in compliance with a series of obligations and requirements which derive directly from the data protection regime.[45] Specifically, Section 2 of the GDPR is where these obligations can be found.

Businesses and organisation, whether they be private or public entities, are required both to put in place procedures aimed at the protection of personal data and to implement cybersecurity measures at all levels. On the one hand, preventative organisational measures showing consideration of the level of risk and the value of the processed data should be implemented in order to ensure a rapid response. To mention just few of these: data protection risk registers, personal data breach notification procedures, data retention schedules and policies, and business continuity plans. On the other hand, technical measures taking into account of the state of the art of technology, as well as the related costs, should be implemented both in the design phase and at the time of the processing itself. These measures can include two-factor authentication systems, strong password policies and access controls, robust antivirus software and end point protection, patch management and vulnerability management procedures. In addition, and in the light of a holistic approach to data protection and data security, organisations should include training for all staff members as part of their wider cyber resilience strategy.

When interviewed by the author, Philip Amann, Head of Strategy of Europol's European Cybercrime Centre (EC3), provided an analysis of cyber-risks and remedies at this particular moment of crisis. Answering a question on how public organisations should implement measures to increase cyber resilience and mitigate the impact of attacks to the security of personal data, he stated:

> "Cyber security is a shared responsibility and – while technology can provide baseline protection – a strong focus should be put on human factors. This means that ongoing and targeted training, education, and awareness raising are equally important to technology, and complement technology measures to support a high level of cyber security and resilience. [...] Organisations need to manage internal risks and the risks within the environment in which they operate, including the supply chain. This requires having both the technical and organisational measures to ensure the security of systems and information. This includes resources, capabilities, processes and tools to detect, defend and respond effectively and efficiently to cyber attacks. Security, including core principles such as security and privacy by design, needs to be a key element of all business processes and activities of an organisation."[46]

[45] Art. 4 GDPR defines personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

[46] The whole interview is available at: https://www.trilateralresearch.com/cyber-threats-and-pandemics-tackling-risk-through-shared-responsibility/.

5 Conclusion

At the time of writing, it is difficult to foresee when – and if – things are going back to 'normality'. When the impact of COVID-19 on privacy and the protection of personal data first started to become visible, privacy experts in Europe denounced the unavoidable "Big Brother" coming out of the privacy *vs*. health trade-off. These fears did not overestimate the potential impact of this catastrophic event. They did however underestimate the power and effectiveness of the European data protection regime. The GDPR, its principles and obligations, passed the first major test of their short existence, demonstrating to the world how high privacy standards can be maintained even in emergency circumstances. On the one hand, supervisory authorities have provided useful guidance regarding the development and deployment of invasive measures used to mitigate the effects of the pandemic. On the other, businesses and organisations may have discovered that compliance with the security-related requirements of the GDPR already provided the necessary technical and organisational measures to combat the rise in cybercrime during the pandemic. Although in many ways, the EU was unprepared for the management of the pandemic, it performed better than others at protecting the fundamental right to privacy of its citizens in a time of health crisis.

References

1. Amit, M., Kimhi, H., Bader, T., et al.: Mass-surveillance technologies to fight coronavirus spread: the case of Israel. Nat. Med. **26**, 1167–1169 (2020). https://doi.org/10.1038/s41591-020-0927-z
2. Cybersecurity Ventures: 2019, official annual cybercrime report (2019). https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/
3. De Filippi, P.: The interplay between decentralization and privacy: the case of blockchain technologies. J. Peer Prod. (7) (2016). Alternative internets. September 14. https://ssrn.com/abstract=2852689
4. Dhanjani, D., Rios, B., Hardin, B.: Hacking: The Next Generation (2009). O' Reilley Media
5. DP-3T: Decentralized privacy-preserving proximity tracing, DP-3T (2020). https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf
6. European Data Protection Board (EDPB): Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (21 April 2020). https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf
7. European Data Protection Board (EDPB): Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1 (4 May 2020). https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
8. European Union Agency for Law Enforcement Cooperation (Europol), Catching the virus – Cybercrime, disinformation and the COVID-19 pandemic (3 April 2020). https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
9. Ferretti, L., et al.: Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science **368**(6491), eabb6936 (2020). https://science.sciencemag.org/content/368/6491/eabb6936
10. Hoffman-Andrews, J., Crocker, A.: How to protect privacy when aggregating location data to fight COVID-19. (2020). Electronic Frontier Foundation, April 6. https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19
11. Ienca, M., Vayena, E.: On the responsible use of digital data to tackle the COVID-19 pandemic. Nat. Med. **26**, 463–464 (2020). https://doi.org/10.1038/s41591-020-0832-5.

12. Khan, N., Brohi, S., Zaman, N.: Ten deadly cyber security threats amid COVID-19 pandemic, TechRxiv (2020). https://www.techrxiv.org/articles/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792
13. Lallie, S., et al.: Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. (2020), arXiv, 21 June 2020. https://arxiv.org/pdf/2006.11929.pdf
14. Mouton, F., et al.: Towards an Ontological Model Defining the Social Engineering Domain. IFIP Advances in Information and Communication Technology (2014)
15. Mozur, P., Zhong, R., Krolik, A.: In coronavirus fight, China gives citizens a color code, with red flags. New York Times, 1 March 2020. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
16. Panebianco, M.: Business continuity & crisis management: riflessioni operative sullo stato d'emergenza Covid-19. Federprivacy, 21 April 2020. https://www.federprivacy.org/informazione/primo-piano/business-continuity-crisis-management-riflessioni-operative-ed-umano-centriche-sullo-stato-di-emergenza-covid-19
17. Ram, N., Gray, D.: Mass surveillance in the age of COVID-19. J. Law Biosci. **7**(1), lsaa023 (2020). https://doi.org/10.1093/jlb/lsaa023
18. Servick, K.: COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? 21 May 2020. https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how
19. Shi, F.: Threat spotlight: coronavirus-related phishing. Barracuda, March 26, 2020. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/
20. Ting, D.S.W., Carin, L., Dzau, V., et al.: Digital technology and COVID-19. Nat. Med. **26**, 459–461 (2020). https://doi.org/10.1038/s41591-020-0824-5. 2020
21. Thompson, S.A., Warzel, C.: Twelve million phones, one dataset, zero privacy. New York Times, 19 December 2019. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
22. Wenar, L.: Rights. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy (2020). https://plato.stanford.edu/archives/spr2020/entries/rights/
23. World Health Organization: Contact tracing in the context of COVID-19. Interim guidance, 10 May 2020. https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19