Academic Journal of Nawroz University (AJNU), Vol.1, No.1, 2023
This is an open access article distributed under the Creative Commons Attribution License
Copyright ©2017. e-ISSN: 2520-789X
https://doi.org/ 10.25007/ajnu.v1n1a1940

Personal Data Privacy vs Public Interest:

Covid-19 Data Gathering Brings a Personal Data Protection Policy Rethink

Jing Wang [1,2], Dermot Cahill [3,4]

[1] Lecturer in Law at Strathclyde Law School
[2] Researcher, Strathclyde Centre for Antitrust Law and Empirical Study (SCALES) University of Strathclyde, UK
[3] Head of Competitiveness Research at HelpUsTrade.com
[4] Formerly Founder Director, Institute for Competition & Procurement Studies, UK

ABSTRACT

Governments around the world have gathered masses of personal information on their citizens as part of the fight against the Covid pandemic. Citizens, willingly for the most part, yielded such data in order to protect the public good and safety of society. Focusing on personal data gathering, processing and protection for public good, the authors consider how far citizens are willing to accept that their personal data can be collected by governments during a public health crisis. The situation in Europe and in China shall be compared, showing how the "public interest" during Covid-19 was understood very differently in different jurisdictions.

KEYWORDS: Privacy; Public Interest; COVID-19; Sensitive Personal Data; Data Processing; Right to be Forgotten.

1. Introduction

Governments around the world have been able to gather masses of personal information on their citizens as part of the fight against the Covid pandemic.[1] Citizens, willingly for the most part, yielded such data in order to protect the public good and safety of society.[2] In this article, which focuses on personal data gathering and processing, mass surveillance and protection for public good, the authors will consider at which level(s) citizens are willing to accept that their personal data can be collected by governments in a public health crisis. The situation in Europe and in China shall be contrasted and compared, to show how the notion of the "public interest" (the best interests of society) was understood very differently during Covid-19 in different jurisdictions.

Personal data collection can in many instances benefit the public good. For example, fingerprints are used to detect criminals' presence at crime scenes.[3] Airports scan our faces to strengthen border security in the fight against terrorism.[4] Similarly, during Covid-19, personal data collection (including sensitive personal data) and shared data sources were used to combat the global pandemic, empowering State agencies to ensure citizen health safety by using gathered data to conduct mass vaccination programmes, persuading citizen co-operation and supporting community control.[5]

However, the idea that Covid has presented governments with a perfect reason to invade citizens' personal privacy has also been a popular viewpoint globally[6], in particular in some European countries.[7] Although citizens in Europe have already given their personal data to their governments to facilitate the implementation of the massively successful European Union (EU)-wide Covid vaccination plan, they found it harder to contemplate China-style data collection and Covid-personal movement control (e.g., via use of Covid personal movement-confining apps) implemented by personal data driven decisions. The right to personal privacy is protected in fundamental rights instruments such as *the European Convention on Human Rights* (ECHR) Art. 8. It recognises that

personal privacy is not an absolute right and that it can be limited under special circumstances, such as wide scale public health threats.[8] *The European General Data Protection Regulation* (GDPR) confirms that "the processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health, without consent of the data subject."[9] Nevertheless, many citizens are deeply uncomfortable that the State now holds, on a mass scale, up-to-date personal information on them which it did not hold previously on such a comprehensive scale. The EU Early Warning and Response System (EWRS), a tool originally designed to share public health information in the EU and provide notification to the EU Commission[10], which later became a public health threats monitor tool within the EU[11] was never widely accepted by citizens to combat Covid-19.[12] Similar failure can be observed from the roll-out of Government-funded Covid "vaccine passports" which were designed for the public to travel safely through Europe, by allowing them show that they had been vaccinated[13], such as the UK's covid app, which after many millions was abandoned as it could not "talk to" other countries Covid protection systems.[14]

In contrast, in China the relationship between personal data and the public good is undergoing an interesting phase. On the one hand vis the relationship between the citizen and the State, scholars have described it as follows: "[the citizen's] right to personal information should be limited because it should not interfere with the authority of the Chinese government, as the largest data controller, to collect, process, save, and use personal information."[15] However, in an interesting contrast, the *Personal Information Protection Law of China* 2021 (PIPL 2021) does not take the same approach, instead adopting an EU-like approach[16] by providing that while "personal information processors may process personal information when it is necessary to respond to public health threats"[17], it also provides that "personal information processors shall have the obligation to erase personal data when the data are no longer necessary in relation to the purposes for which they were collected"[18] and that where "personal information processors[19] fail to erase personal data, citizens can request them to do so".[20]

This context described above presents interesting questions for scholars interested in big data, mass surveillance, use and storage of personal data by the State, as follows: when Covid does eventually come to an end, will the State erase the collected data when the reason for Governments to hold this mass of personal data (voluntarily given by citizens to help the government fight the Covid public health threat) no longer exists? In Europe this debate has centred around talk of "the right to be forgotten" (already part of EU GDPR[21]) to be extended to allow citizens to force Governments in Europe to delete citizens personal data which States have long desired to hold.

Another related question arises in the case of one-party States like China: it has adopted a version of the EU GDPR "right to be forgotten" model in its PIPL 2021[22], so the question arises whether citizens are in a position of certainty or uncertainty with regard to seeking to have their Covid-provided personal data deleted via the "right to be forgotten", at a time when requesting governments or dominant tech giants who collaborate with government on Covid contact tracing apps to erase one's personal data, may not be straightforward.

This Article therefore will consider how to enhance "the right to be forgotten" in China in the personal data context, as well as identifying in which areas the EU-style right to be forgotten can be strengthened in an effort to see if the advent of innovation and mass data gathering presents new challenges for States seeking to take long-term advantage of Covid-

gathered mass data, or whether existing legislation provides an adequate safeguard for citizens.

2. CONTENT

Putting the idea "sharing is caring" into action, personal data collection, processing and sharing have played an important and valuable role across the world for governments taking measures to contain and mitigate the immense threat to public health during the Covid-19 crisis.[23] Covid contact tracing apps were designed to monitor the virus spread and break the chain of infections to reduce infection numbers and save lives.[24] In Europe, tech companies (e.g., Google and Apple) collaborated with governments building GPS-based or Bluetooth-based contact tracing apps for Android and iPhone devices to support governments controlling Covid outbreaks.[25] Simultaneously, China tech giants (e.g., Alibaba and Tencent) collaborated with the government by building in-app mini-programs, namely "JianKangBao", to carry mandatory QR codes which allowed citizen-tracking on Android, iPhone and Huawei devices.[26] JianKangBao collected a broad range of personal data, such as individual user identities, user location and geographical movement, temperature, positive diagnosis information, vaccine record, notifications to exposed users, etc.[27] In comparison, contact tracing apps in Europe, such as NHS COVID-19 (UK), Covid Tracker (Ireland), StopCovid (France), Smittestop (Denmark), CoronaMelder (Netherlands), Immuni (Italy), in general collected the following four categories of person data, namely:

- "individual user identities and location data";
- "Bluetooth identifier codes and associated contact event information";
- "positive diagnosis information and associated information"; and
- "notifications to exposed users".[28]

In the EU and UK "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly [...]."[29] In China, "'personal data' means any information recorded by electronic or other means related to identified or identifiable natural persons, *not including* information after anonymisation."[30] Within the definition of personal data, there is a special category, namely sensitive personal data ('SPD') related to all Covid-19 apps (e.g., health data[31]), which in general shall be prohibited from processing[32] unless "processing is necessary for reasons of substantial public interest"[33], or can only be processed "when there is a specific purpose and sufficient necessity, and strict protection measures are taken".[34] However, the definition of the SPD has not been provided by the EU/UK GDPR, or China PIPL, apart from a list of SPD examples.[35] This causes uncertainty about what should be considered and treated as SPD at the points of data collection and data processing.

In March 2020 the European Data Protection Board (EDPB[36]) adopted the *Statement on the processing of personal data in the context of the Covid-19 outbreak* to combat Covid-19, and "[underlined] that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects."[37] In parallel, an EU GDPR-modelled PIPL came into force in China in 2021, starting a new chapter of data protection for Chinese citizens when their personal data has been widely and mandatorily collected.[38] However, the EU/UK GDPR and Chin PIPL have failed to solve the public's data privacy concerns brought about by the use of contact tracing apps during the pandemic[39], e.g., the public worries about data security and excessive information collection.[40]

3.1 Privacy Leakage: East and West Sharing the Same Concern

Covid-19 contact tracing apps were mandatory in certain countries such as China, Qatar, but voluntary (in other words, opt-in) in other countries, e.g., in Europe.[41] Literature reviews on the tracing apps identified privacy issues such as no mention of data encryption; silence on whether or how the individual could request personal data deletion; and further concerns about anonymised data collection, etc.[42] Given anonymised data is unable to identify individuals on its own, such data has been excluded from personal data protection according to GDPR and PIPL.[43] However, there are possibilities whereby, combining such data *with other data*, can result in anonymised data playing a role in re-identifying individuals.[44] This concern around collection of anonymised data challenges the protection range of the GDPR and PIPL.

Furthermore, the low downloads rates in Europe (e.g., Ireland—49%; Denmark—38%; England & Wales—36%; Netherlands—26%; France—20%; Italy—17%[45]) exposed the public's data privacy concerns. Protests against COVID data collection, including data relating to geographical movement were seen across Europe, e.g., protests in Barcelona (2021)[46]; Paris and Marseille (2021)[47]; Paris and across France (2022)[48]; Athens, Helsinki, London, Paris, Stockholm and across Europe (2022).[49] In fact, none of the contact tracing apps and Covid vaccine passports have survived in Europe—most were abandoned silently by governments within only a few months after launch.[50]

By contrast, Covid-19 contact tracing apps have run successfully in China due to their mandatory nature.[51] 80% of Chinese citizens support the use of Covid-19 contact tracing apps to combat the virus for the sake of "sharing is caring".[52] However, at the same time, data privacy concerns have also been identified about the apps ability to track users movements, centred around the wide range of data collection; concerns about how long the apps would hold citizens' personal data; and concerns about how Covid-collected data could be used by other apps or platforms either during or post-Covid.[53] Sharing the same concerns, we will now turn to discuss data privacy protection challenges in Europe and China from 3 parameters: (a) sensitive personal data protection, (b) processed data protection, and (c) the right to be forgotten.

3.2 Sensitive Personal Data Protection Challenge

According to big data and computing science research, "SPD is the class to indicate personal data considered sensitive in terms of privacy and/or impact and that require additional considerations and/or protection"[54], which includes data revealing health data, etc.[55] Unauthorised disclosure or misuse of SPD can reflect society concerns at large[56] and often can lead to very high possibility of significant physical, moral, or financial harm.[57] Nevertheless dangers arise with the collection of SPD during Covid because such data was collected and processed via Covid-19 tracing apps, yet no clear definition of SPD (including health data) was offered[58], neither in Europe nor in China.

It may be true that in different occasions and scenarios, the sensitivity of the same category of personal data may vary, therefore dividing SPD from personal data (in general) can be challenging. Despite this, the EU/UK GDPR and China PIPL both provide a list of categories of SPD and require extra protection for the processing of such data[59] where considerations of discrimination and stigmatisation harms are often the evaluation standards[60]: In the EU SPD includes "personal data revealing racial or ethnic origin, political opinions, religious or

philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[61] China listed the following categories as SPD: "biometrics, religious beliefs, specific identities, medical health, financial accounts, movements and associated information, as well as personal information of minors under the age of 14."[62] However, such lists are far from sufficient.[63]

When the Covid vaccine passport — the Covid-19 antibody test certification app (i.e., an immunity certificate allowing the holder travel based on either vaccination or antibody tests) — was introduced in the UK, it had been made clear that the app would gather SPD for the sake of public health and public interest but would not reveal any of that data.[64] However, without a solid definition of SPD in the UK GDPR (which following BREXIT mirrored the EU GDPR), it is unclear which data being collected by the COVID-19 antibody test certification app belongs to the SPD category. Thus, this gives rise to the risk SPD, incorrectly grouped as general personal data, could be revealed either by error or by design.

The leakage of SPD can lead to serious results: For instance, in December 2020 a couple living in Chengdu China tested positive for COVID. One day later, their granddaughter, Ms Zhao, also tested positive. Her movements were published accordingly and the public soon realised that due to the nature of her particular employment (working in pubs and bars), Ms Zhao could potentially infect many people. Ms Zhao's personal information (e.g., name, ID number, phone number, home address, working address) was widely circulated online. Being a victim herself, Ms Zhao ought to seek legal protection for the leakage of her SPD. However, sadly, it turned out that Ms Zhao apologised to the public for being an infector.[65]

Another example of lack of security for SPD also happened in December 2020 when approximately 70 Chinese celebrities' SPD was leaked and circulated online. Due to the misuse of a feature of a Covid tracing app—Beijing JianKangBao, fans using the "Check Other's Health QR Code"[66] feature of the app, could figure out how to track celebrities' movement across China. Some extreme fans used celebrities' personal data (e.g., ID numbers and movement) to follow their idols in flights which affected those celebrities' work and personal life.[67] Hence, for the sake of protecting victims from the leakage of SPD, there is an urgent need for a definition of sensitive personal data to be added into personal data protection acts worldwide.

4. PROCESSED DATA PROTECTION CHALLENGES

GDPR and PIPL were designed to protect data privacy of individuals ('personal data owners' or 'data subject') when data controllers collect, process or transfer personal data.[68] For processing personal data during the ongoing global pandemic of Covid, there were underpinning legal justifications: for instance, in the UK, sensitive personal data was allowed to be processed if it "[…] is necessary for reasons of substantial public interest."[69] In the EU, data processing was lawful if "processing is necessary for the performance of a task carried out in the public interest".[70] In China, personal data collection and processing can omit the obtaining of permission from citizens if it is necessary to respond to public health emergencies.[71] The original idea of using data to combat the pandemic aims therefore relies on personal movement and pandemic infection data to help governments draw a comprehensive picture[72]; on how the virus spreads, how to support hospitals to get ready for treating victims; how to guide food supply and PPE (personal protective equipment) supply for the society, etc. However, as the following

will show, collecting SPD in pursuit of the idea of protecting the public interest can also turn out to be a means of harming the public interests when the data has been processed.

In order to answer this question, it is vital to find out whether processed data is eligible to be protected or not under EU/UK GDPR and China PIPL. Processed data may no longer belong to the personal data category if it does not relate to the very individual from whom the data was originally collected.[73] In other words, after the raw sensitive personal data has been collected and processed in pursuance of safeguarding the public interest, a good amount of the processed data can be created which is very unlikely to fall within the definition of personal data (according to the definitions in GDPR and PIPL[74]). This in turn can potentially harm citizens' interests. For example, data collected from Covid contact tracing apps after processing, and dis-connected from individuals, can be used to map out the movement of people[75] and their social activities[76], or to work out people's medical and health history which can benefit health insurance companies and pharmaceutical companies. Similar issues have arisen before. For example, 23andMe (a personal genomics and biotechnology company based in California) announced plans to use the company's more than 12-million person DNA samples for drug research, and unfortunately, the secondary use of such (processed) data falls outside of US data protection acts.[77] Concerns about data misuse led to significant debate about Covid apps security and privacy[78], which in turn led to failure of contact tracing apps in many countries and regions, such as in Europe.[79] Although the ECHR makes it clear that personal privacy can be limited under special circumstances when public health is under threat[80], the failure to spread the use and acceptance of contact tracing apps illustrates that giving away personal data to the government to safeguard the public interest for the duration of the emergency was not considered "safe" by many citizens in Europe. The download rate of Covid contact tracing apps in the EU Member States was less than half of their population and even people who have downloaded the app may have never used the app.[81] In the UK, such concern increased because in 2022, the UK launched an NHS project to sell tens of millions of personal digital medical records (including health data collected during Covid) to a US company—Palatine (one of the world biggest health data platforms) without seeking patient consent, and it has been confirmed that it shall proceed to "provide new insights into the nation's health".[82] These concerns highlight the urge and challenge for EU/UK GDPR to give serious consideration to protecting processed data that currently does not fall into the definition of personal data. Similar concerns also exist in China, but the attitude towards tracing app use is very different.

In China, a much more comprehensive version of a Covid tracing app, named China's Health Code app ('JianKangBao'), was created, operated and technically supported by collaboration between the government[83] and technology companies (i.e., Alibaba and Tencent, who own the dominant online shopping platforms; online payment systems; instant messaging platforms, etc.). Personal data, such as the citizen's ID number, face, mobile number, addresses, geological locations and movements, temperature, positive diagnosis information, vaccine record, and notifications to exposed users, were all collected via JianKangBao.[84] On one hand, similar to the West, concerns about privacy and data misuse by the online platform giants to gain business profits are also present in China.[85] By knowing people's movements, artificial intelligence can easily work out beneficial data for businesses: for instance, realising that which age groups prefer which type of

restaurants, and which tourist destinations attract people with various salary levels, can help businesses target the right markets for the future. Such valuable processed data can be potentially sold on to businesses or research agencies which will for sure constitute a breach of trust in personal data privacy. Currently, China's PIPL does not provide sufficient protection *vis a vis* use of processed data which poses foreseeable risks for citizens.

Conversely, on the other hand, it could also be said that the collaboration between government and tech giants also demonstrated an effective approach[86] to guarantee the coverage of the Health Code app amongst a large population due to the massive amount of Alibaba and Tencent users among the Chinese citizenry.[87] Contrary to what happened in the EU/UK, the use of the contact tracking app was mandatory in China until December 2022 when the zero-COVID policy was cancelled.[88] Despite critical comments on the loss of privacy, people coped with the Health Code app use due to "the country's unique socio-political environment and cultural heritage and is thus significantly different from Western norms and values built around individual freedom and rights."[89] Such differences can also be seen from the understanding of the right to be forgotten in GDPR and PIPL.

1. THE RIGHT TO BE FORGOTTEN CHALLENGES

The notion of a "right to be forgotten" was introduced by the EU GDPR and soon thereafter was mirrored in many other countries' data protection regimes, such as the UK (2018) and China (2021).[90] EU GDPR provides that: "[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where […] the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed […]"[91] However, this does not mean GDPR and China PIPL apply the same rules when it comes to the personal data that needs to be deleted and forgotten: the PIPL focuses more on the right to be delete data (e.g., "personal information processors shall have the obligation to erase personal data […]"[92]), rather than the right to be forgotten (GDPR).

Issues around the right to be forgotten had appeared in China before the PIPL came into force in 2021. The very first China's right to be forgotten case—*Ren Jiayu v. Beijing Baidu Netcom Technology Co., Ltd.* was filed in 2015. In this case the plaintiff's requested that his name-related search suggestions to be removed from Baidu[93], a widely used search engine, because information thereon harmed his reputation. However, his claim was not supported by Beijing's First Intermediate People's Court as the right to be forgotten did not exist in China's legal framework at the time.[94] However, would the plaintiff's claim be supported if the case was brought to court after 2021? Article 47 of PIPL 2021 provides no legal basis for inaccurate data to be erased, although Article 46 does state that personal information controllers / processors shall have the obligation to correct inaccurate personal data, and complete the incomplete personal data. In other words, the plaintiff's claim based on the right to be forgotten still could not be supported under PIPL.

Another limitation of the PIPL resides in Article 47 PIPL, whereby it is clear that the Law only requires *data processors* to erase personal data. If processors failed to erase, data owners can request them to do so.[95] Such requirements differ from the EU GDPR which requires *data controllers* to erase personal data without undue delay when it is necessary[96]: First, a data processor is not a data controller; instead, the processor is either a person or a public authority, or an agency who processes personal data on behalf of

the data controller.[97] This means unlike in the EU where when the data controller erases personal data, "any links to, or copy or replication of, those personal data" will be deleted synchronously[98], citizens (data owners) in China can only request *data processors* to delete their data individually, while *data controllers* may still store the raw data. Hence, if key data processors in China such as Alibaba and Tencent did not delete Covid-related personal data which they gathered and processed via JianKangBao, citizens would have to contact them separately to seek data deletion post-Covid. However, because of the lack of transparency and information on how citizens' Covid-gathered personal data has been processed, citizens cannot even figure out who the other data processors are after Alibaba and Tencent. They thereby lose their right to erase such personal data completely. Second, in any case where a citizen seeks to request deletion of Covid-provided personal data, citizens will find this is not an easy task. Taking Tencent's WeChat platform as an example, one of the major platforms hosting JianKangBao, there is no link to erase Covid-gathered personal data in the WeChat Security Centre, and no information has been provided when searching "the right to be forgotten" in its Help Centre. We can therefore conclude that the PIPL's provision for requesting data deletion is neither user-friendly nor transparent in practice.

The EU GDPR's right to be forgotten provides better data privacy and protection than China PIPL, notwithstanding that issues remain around seeking an all-encompassing definition of SPD and around data processing. For example, GDPR states that the right to be forgotten does not apply to personal data collected for reasons of public interest in the area of public health.[99] This exemption makes sensitive personal data protection even more difficult for the public, and leaves open the potential risk of data misuse via data processing. Commentators have also argued that it is unlikely to be reasonable to regard all health data as falling within the scope of the public interest exemption to the right to be forgotten.[100] Otherwise, it would be too broad and potentially harm the balance between privacy and the public interest.[101] Therefore, in order to improve the EU-style right to be forgotten, it is necessary to (a) provide a solid definition for SPD, and also (b) offer protection to processed data.

2. CONCLUSION

The EU's GDPR has been described as the gold standard on data protection and a global standard for the digital era since 2016.[102][1] However, the gold standard fails to solve public concerns surrounding data privacy following the Covid pandemic. Alongside mass personal data gathering via Covid contact tracing apps which could be seen across the world with the aim of supporting governments and their citizens to fight Covid, we also see citizens' concerns and criticisms when they were being requested to share more and more of their personal data by governments during a public health crisis. This presents the urge to rethink Personal Data Protection Policy in the context of revising the GDPR.

The authors observe that while citizens, in both East and West exhibit various levels of willingness to share their personal data for the sake of protecting the public good and safety of society, at the same time it must be recognised that both East and West face similar challenges for provision of an adequate safeguard for protecting citizens data privacy and its use, as they all follow the gold standard set by the GDPR, which now is revealed to have some gaps. First gap is the lack of SPD definition: Covid contact tracing apps collected massive amounts of SPD, but

[1] Schünemann, W.J. and Windwehr, J., 2021. Towards a 'gold standard for the norm entrepreneurship. *Journal of European Integration*, 43(7), pp.859-874.world'? The European General Data Protection Regulation between supranational and national

SPD has never been adequately defined by either the EU or UK GDPR nor by China's PIPL. Second, processed data falls outside of the EU/UK GDPR and also outside China's PIPL: After collection, raw data processed via Covid contact tracing apps for the purpose of helping governments draw a comprehensive picture for combatting the virus, falls *outside* the scope of the EU's GDPR, the UK's GDPR and China's PIPL. In other words, processed data will not be protected as SPD because it no longer satisfies the definition of personal data which must be able to identify individuals. Third, given the existing weaknesses in both the GDPR and the PIPL relating to sensitive personal data and processed data, the EU-style right to be forgotten faces ineffectiveness when intended to protect personal data privacy, as the right to be forgotten does not apply to processed data, and can also be exempted from being SPD in pursuit of governments taking steps to promote the public interest.

3. FOOTNOTES

1. Ram, N. and Gray, D., 2020.
2. Latemore, G., 2021.
3. Bond, J.W., 2009.
4. Moujahdi, C. and Assad, N., 2019.
5. Ienca, M. and Vayena, E., 2020.
6. Gvili, Y., 2020.
7. do Carmo Barriga, A., Martins, A.F., Simões, M.J. and Faustino, D., 2020.
8. European Convention on Human Rights (ECHR, 2013), Art. 8(2).
9. European General Data Protection Regulation (GDPR, 2018), Recital. 54.
10. Guglielmetti, P., Coulombier, D., Thinus, G., Van Loock, F. and Schreck, S., 2006.
11. European Centre for Disease Prevention and Control. 2018.
12. Forman, R. and Mossialos, E., 2021.
13. European Council. 2023.
14. Warren, G.W. and Lofstedt, R., 2022.
15. Huang, J.J., 2020.
16. Schwartz, P.M., 2019.
17. PIPL 2021, Art. 13(4).
18. PIPL 2021, Art. 47(1).
19. Whether private or public agencies.
20. PIPL 2021, Art. 47(1).
21. The General Data Protection Regulation (GDPR, 2018), Art.17 regulates the right to be forgotten which includes (1) individuals have the right to have personal data erased; (2) data "controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request."
22. PIPL 2021, Art. 47 states individuals have the right to have personal data erased.
23. Almeida, B.D.A., Doneda, D., Ichihara, M.Y., Barral-Netto, M., Matta, G.C., Rabello, E.T., Gouveia, F.C. and Barreto, M., 2020.
24. Kędzior, M., 2021.
25. Lanzing, M., Lievevrouw, E. and Siffels, L., 2022.
26. Guo, Y., Chen, J. and Liu, Z., 2022.
27. Zhang, Z., 2022.
28. Bradford, L., Aboy, M. and Liddell, K., 2020.
29. GDPR 2018, Art. 4(1).
30. PIPL 2021, Art. 4(1).
31. GDPR 2018, Art. 9(1); PIPL 2021, Art. 28(1).
32. GDPR 2018, Art. 9(1).
33. GDPR 2018, Art. 9(2)(g).
34. PIPL 2021, Art. 4(2).
35. GDPR 2018, Art. 9(1); PIPL 2021, Art. 28(1).
36. EDPB, based in Brussels, was established under the GDPR as an independent European body contributing to the consistent application of data protection rules throughout the EU, and promoting cooperation between the EU's data protection authorities.
37. European Data Protection Board, 2020.
38. Cong, W., 2021.
39. Trestian, R., Celeste, E., Xie, G., Lohar, P., Bendechache, M., Brennan, R. and Ta, I., 2022.
40. Zhang, Z., 2022; Gasser, U., Ienca, M., Scheibner, J., Sleigh, J. and Vayena, E., 2020.
41. Hernández-Orallo, E., Manzoni, P., Calafate, C.T. and Cano, J.C., 2022.
42. Alshawi, A., Al-Razgan, M., AlKallas, F.H., Suhaim, R.A.B., Al-Tamimi, R., Alharbi, N. and AlSaif, S.O., 2022.
43. GDPR 2018, Art. 4(1); PIPL 2021, Art. 4(1).
44. Cristani, F.. 2021.
45. Civil Liberties Union for Europe. 2021.
46. Euronews. 2021(B).
47. Euronews. 2021(A).
48. Blade, T. 2022.
49. Euronews. 2022.
50. Civil Liberties Union for Europe. 2021.
51. Mandatory means use by everyone living in China unless they were too young or too old to access mobile devices.
52. Kostka, G. and Habich-Sobiegalla, S., 2022.
53. Zhou, S.L., Jia, X., Skinner, S.P., Yang, W. and Claude, I., 2021.

54. Gambarelli, G. and Gangemi, A., 2022.
55. GDPR 2018, Art. 9(1).
56. Ohm, P., 2014.
57. PIPL 2021, Art. 28.
58. Quinn, P. and Malgieri, G., 2021.
59. GDPR 2018, Art. 9; PIPL 2021, Art. 28.
60. Quinn, P. and Malgieri, G., 2021.
61. GDPR 2018, Art. 9(1).
62. PIPL 2021, Art. 28(1).
63. Matic, S., Iordanou, C., Smaragdakis, G. and Laoutaris, N., 2020.
64. Eisenstadt, M., Ramachandran, M., Chowdhury, N., Third, A. and Domingue, J., 2020.
65. Zuo, Y.T. and Wang, T.Y., 2021.
66. Zhang, X., 2022.
67. Wang, B., 2023.
68. GDPR 2018, Art. 1; PIPL 2021, Art. 1.
69. Data Protection Act (DPA, 2018), Art.6(1)(b).
70. GDPR 2018, Art. 6(1)(e).
71. PIPL 2021, Art. 13(4).
72. Agarwal, P., Swami, S. and Malhotra, S.K., 2022.
73. Information Commissioner's Office, 2022.
74. GDPR 2018, Art. 4(1); PIPL 2021, Art. 4.
75. Yang, C., 2022.
76. Nageshwaran, G., Harris, R.C. and Guerche-Seblain, C.E., 2021.
77. Spector-Bagdady, K., 2021.
78. Ho, K.K., Chiu, D.K. and Sayama, K.L., 2023.
79. Hamza, M., Khan, A.A. and Akbar, M.A., 2022.
80. ECHR 2013, Art. 8(2).
81. Civil Liberties Union for Europe. 2021.
82. Ungoed-Thomas, J. 2022.
83. The State Information Center and the National Health Commission of China.
84. Zhang, Z., 2022.
85. Zhu, L. and Demircioglu, M.A., 2022.
86. Yang, F., Heemsbergen, L. and Fordyce, R., 2021.
87. Li, V.Q., Ma, L. and Wu, X., 2022.
88. Davidson, H., 2022.
89. Liu, J. and Zhao, H., 2021.
90. Greenleaf, G., 2022.
91. GDPR 2018, Art. 17(1)(a).
92. PIPL 2021, Art. 47(1).
93. Baidu, China's Google equivalent, the largest and most widely used search engine in Mainland China.
94. 'Ren Jiayu v. Beijing Baidu Netcom Technology Co., Ltd.', 2015.
95. PIPL 2021, Art. 47(1).
96. GDPR 2018, Art. 17(1)(a).
97. GDPR 2018, Art. 4(8).
98. GDPR 2018, Art. 17(2).
99. GDPR 2018, Art. 17(3)(c).
100. Correia, M., Rego, G. and Nunes, R., 2021.
101. Rajczi, A., 2016.
102. Schünemann, W.J. and Windwehr, J., 2021.

8. REFERENCES

1. Agarwal, P., Swami, S. and Malhotra, S.K., 2022. Artificial intelligence adoption in the post COVID-19 new-normal and role of smart technologies in transforming business: a review. *Journal of Science and Technology Policy Management*.
2. Almeida, B.D.A., Doneda, D., Ichihara, M.Y., Barral-Netto, M., Matta, G.C., Rabello, E.T., Gouveia, F.C. and Barreto, M., 2020. Personal data usage and privacy considerations in the COVID-19 global pandemic. *Ciencia & saude coletiva*, 25, pp.2487-2492.
3. Alshawi, A., Al-Razgan, M., AlKallas, F.H., Suhaim, R.A.B., Al-Tamimi, R., Alharbi, N. and AlSaif, S.O., 2022. Data privacy during pandemics: A systematic literature review of COVID-19 smartphone applications. *PeerJ Computer Science*, *8*, p.e826.
4. Blade, T. 2022. *Tens of thousands protest COVID vaccine pass across France Access to the comments Comments*. [Online]. [Accessed 7 February 2023]. Available from: https://www.euronews.com/2022/01/09/tens-of-thousands-protest-covid-vaccine-pass-across-france.
5. Bond, J.W., 2009. The value of fingerprint evidence in detecting crime. *International Journal of Police Science & Management*, 11(1), pp.77-84.
6. Bradford, L., Aboy, M. and Liddell, K., 2020. COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. *Journal of Law and the Biosciences*, 7(1), p.lsaa034.
7. Civil Liberties Union for Europe. 2021. *COVID-19 Technology in the EU: A Bittersweet Victory for Human Rights?*. [Online]. [Accessed 5 February 2023]. Available from: https://dq4n3btxmr8c9.cloudfront.net/files/c-5f-T/Liberties_Research_EU_Covid19_Tracing_Apps.pdf.
8. Cong, W., 2021. From pandemic control to data-driven governance: The case of China's health code. *Frontiers in Political Science*, 3.
9. Correia, M., Rego, G. and Nunes, R., 2021. The right to be forgotten and COVID-19: Privacy versus public interest. *Acta Bioethica*, 27(1), pp.59-67.
10. Cristani, F.. 2021. *Protecting privacy and data while tracking COVID-19 in Europe: which cooperation? A focus on Italy and the Czech Republic*. 2021 Czernin Security Forum: Digital Transformation in Europe after 2020: Adaptation in Cyberspace, 20 November, Prague.
11. Data Protection Act (DPA, 2018).
12. Davidson, H., 2022. China scraps tracking app as zero-Covid policy is dismantled. *The Guardian*. [Online]. [Accessed 24 January 2023]. Available from: https://www.theguardian.com/world/2022/dec/12/china-scraps-tracking-app-amid-widespread-dismantling-of-zero-covid-policy.
13. do Carmo Barriga, A., Martins, A.F., Simões, M.J. and Faustino, D., 2020. The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance?.

Social Sciences & Humanities Open, 2(1), p.100096.
14. Eisenstadt, M., Ramachandran, M., Chowdhury, N., Third, A. and Domingue, J., 2020. COVID-19 antibody test/vaccination certification: there's an app for that. *IEEE Open Journal of Engineering in Medicine and Biology*, 1, pp.148-155.
15. Euronews. 2021(A). *France: Tens of thousands protest against COVID pass, vaccination*. [Online]. [Accessed 7 February 2023]. Available from: https://www.euronews.com/my-europe/2021/07/17/france-tens-of-thousands-protest-against-covid-pass-vaccination.
16. Euronews. 2021(B). *Protesters march against COVID-19 health pass in Barcelona*. [Online]. [Accessed 7 February 2023]. Available from: https://www.euronews.com/2021/12/11/protesters-march-against-covid-19-health-pass-in-barcelona.
17. Euronews. 2022. *COVID-19 vaccine passport protests in Europe draw thousands of people*. [Online]. [Accessed 7 February 2023]. Available from: https://www.euronews.com/2022/01/22/covid-19-vaccine-passport-protests-in-europe-draw-thousands-of-peopl.
18. European Centre for Disease Prevention and Control. 2018. *Early Warning and Response System of the European Union (EWRS)*. [Online]. [Accessed 4 February 2023]. Available from: https://www.ecdc.europa.eu/en/publications-data/early-warning-and-response-system-european-union-ewrs.
19. European Convention on Human Rights (ECHR, 2013).
20. European Council. 2023. *EU digital COVID certificate: how it works*. [Online]. [Accessed 14 February 2023]. Available from: https://www.consilium.europa.eu/en/policies/coronavirus/eu-digital-covid-certificate/.
21. European Data Protection Board, 2020, Statement on the processing of personal data in the context of the COVID-19 outbreak.
22. European General Data Protection Regulation (GDPR, 2018).
23. Forman, R. and Mossialos, E., The EU Response to COVID—19: From Reactive Policies to Strategic Decision—Making, *Journal of Common Market Studies* (2021).
24. Gambarelli, G. and Gangemi, A., 2022. PRIVAFRAME: A Frame-Based Knowledge Graph for Sensitive Personal Data. *Big Data and Cognitive Computing*, 6(3), p.90.
25. Gasser, U., Ienca, M., Scheibner, J., Sleigh, J. and Vayena, E., 2020. Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. *The Lancet, Digital Health*, 2(8), pp.e425-e434.
26. Greenleaf, G., 2022. Now 157 Countries: Twelve Data Privacy Laws in 2021/22. *Privacy Laws & Business International Report*, 17(6), pp.3-8.
27. Guglielmetti, P., Coulombier, D., Thinus, G., Van Loock, F. and Schreck, S., 2006. The early warning and response system for communicable diseases in the EU: an overview from 1999 to 2005. *Eurosurveillance*, 11(12), pp.7-8.
28. Guo, Y., Chen, J. and Liu, Z., 2022. Government responsiveness and public acceptance of big-data technology in urban governance: Evidence from China during the COVID-19 pandemic. *Cities*, 122, p.103536.
29. Gvili, Y., 2020. Security analysis of the COVID-19 contact tracing specifications by Apple Inc. and Google Inc. *Cryptology ePrint Archive*.
30. Hamza, M., Khan, A.A. and Akbar, M.A., 2022, June. Toward a secure global contact tracing app for COVID-19. In Proceedings of the International Conference on Evaluation and Assessment in Software, pp. 453-460.
31. Hernández-Orallo, E., Manzoni, P., Calafate, C.T. and Cano, J.C., 2022. A methodology for evaluating digital contact tracing apps based on the COVID-19 experience. *Scientific Reports*, 12(1), p.12728.
32. Ho, K.K., Chiu, D.K. and Sayama, K.L., 2023. When privacy, distrust, and misinformation cause worry about using COVID-19 contact-tracing apps. *IEEE Internet Computing* (Preprint).
33. Huang, J.J., 2020. Applicable law to transnational personal data: trends and dynamics. *Cambridge German Law Journal*, 21(6), pp.1283-1308.
34. Ienca, M. and Vayena, E., 2020. On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature medicine*, *26*(4), pp.463-464.
35. Information Commissioner's Office, 2022. What is personal data? [Online]. [Accessed 9 February 2023]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what -is-personal-data/.
36. Kędzior, M., 2021, January. The right to data protection and the COVID-19 pandemic: the European approach. In *ERA forum* (Vol. 21, No. 4, pp. 533-543). Berlin/Heidelberg: Springer Berlin Heidelberg.
37. Kostka, G. and Habich-Sobiegalla, S., 2022. In times of crisis: Public perceptions toward COVID-19 contact tracing apps in China, Germany, and the United States. *New Media & Society*, p.14614448221083285.
38. Lanzing, M., Lievevrouw, E. and Siffels, L., 2022. It takes two to techno-tango: an analysis of a close embrace between Google/Apple and the EU in fighting the pandemic through contact tracing apps. *Science as Culture*, 31(1), pp.136-148.
39. Latemore, G., 2021. COVID and the common good. *Philosophy of Management*, *20*(3), pp.257-269.
40. Li, V.Q., Ma, L. and Wu, X., 2022. COVID-19, policy change, and post-pandemic data governance: a case analysis of contact tracing applications in East Asia. *Policy and Society*, *41*(1), pp.129-142.
41. Liu, J. and Zhao, H., 2021. Privacy lost: Appropriating

surveillance technology in China's fight against COVID-19. *Business Horizons*, 64(6), pp.743-756.

42. Matic, S., Iordanou, C., Smaragdakis, G. and Laoutaris, N., 2020, October. Identifying sensitive urls at web-scale. *Proceedings of the ACM Internet Measurement Conference*, pp. 619-633.
43. Moujahdi, C. and Assad, N., 2019. On the security of face recognition terminals at modern airports. *International Journal of Computing and Digital Systems*, 8(5), pp.470-476.
44. Nageshwaran, G., Harris, R.C. and Guerche-Seblain, C.E., 2021. Review of the role of big data and digital technologies in controlling COVID-19 in Asia: Public health interest vs. privacy. *Digital Health*, 7.
45. Ohm, P., 2014. Sensitive information. *Southern California Law Review*, 88, p.1125.
46. Quinn, P. and Malgieri, G., 2021. The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework. *German Law Journal*, 22(8), pp.1583-1612.
47. Rajczi, A., 2016. Liberalism and public health ethics. *Bioethics*, 30(2), pp.96-108.
48. Ram, N. and Gray, D., 2020. Mass surveillance in the age of COVID-19. *Journal of Law and the Biosciences*, *7*(1), p.lsaa023.
49. 'Ren Jiayu v. Beijing Baidu Netcom Technology Co., Ltd.', [2015] 09558, (Beijing's First Intermediate People's Court).
50. Schünemann, W.J. and Windwehr, J., 2021. Towards a 'gold standard for the world'? The European General Data Protection Regulation between supranational and national norm entrepreneurship. *Journal of European Integration*, 43(7), pp.859-874.
51. Schwartz, P.M., 2019. Global data privacy: The EU way. *NYUL Rev.*, 94, p.771.
52. Spector-Bagdady, K., 2021. Governing secondary research use of health data and specimens: the inequitable distribution of regulatory burden between federally funded and industry research. *Journal of Law and the Biosciences*, *8*(1), p.lsab008.
53. The General Data Protection Regulation (GDPR, 2018).
54. The Personal Information Protection Law of China 2021 (PIPL ,2021).
55. Trestian, R., Celeste, E., Xie, G., Lohar, P., Bendechache, M., Brennan, R. and Ta, I., 2022, June. The privacy paradox-investigating people's attitude towards privacy in a time of COVID-19. In *2022 14th International Conference on Communications (COMM)* (pp. 1-6). IEEE.
56. Ungoed-Thomas, J. 2022. *Controversial £360m NHS England data platform 'lined up' for Trump backer's firm*. [Online]. [Accessed 9 February 2023]. Available from: https://dq4n3btxmr8c9.cloudfront.net/files/c-5f-T/Liberties_Research_EU_Covid19_Tracing_Apps.pdf.
57. Wang, B. Celebrities' Photos, Other Info Leaked Due to Privacy Flaw in Beijing's Health Code. [Online]. [Accessed 17 February 2023]. Available from: https://en.pingwest.com/a/8168.
58. Warren, G.W. and Lofstedt, R., 2022. COVID-19 vaccine rollout management and communication in Europe: one year on. *Journal of Risk Research*, *25*(9), pp.1098-1117.
59. Yang, C., 2022. Digital contact tracing in the pandemic cities: Problematizing the regime of traceability in South Korea. *Big Data & Society*, 9(1).
60. Yang, F., Heemsbergen, L. and Fordyce, R., 2021. Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality?. *Media International Australia*, 178(1), pp.182-197.
61. Zhang, X., 2022. Decoding China's COVID-19 Health Code Apps: The Legal Challenges. *Healthcare*, 10, p. 1479.
62. Zhang, Z., 2022. Public Health vs. Personal Privacy During COVID-19 in China. In *Coping with COVID-19, the Mobile Way: Experience and Expertise from China* (pp. 169-185). Singapore: Springer Nature Singapore.
63. Zhou, S.L., Jia, X., Skinner, S.P., Yang, W. and Claude, I., 2021. Lessons on mobile apps for COVID-19 from China. *Journal of Safety Science and Resilience*, 2(2), pp.40-49.
64. Zhu, L. and Demircioglu, M.A., 2022. National approaches for citizen data management in response to COVID-19: An overview and implications of contact tracing apps in 21 countries. *Information Polity* (Preprint), pp.1-23.
65. Zuo, Y.T. and Wang, T.Y., 2021. Conflicts and solutions between the public's right to know and citizens' right to privacy [疫情背景下公众知情权与公民隐私权的冲突及解决]. *Journal of Western* [*西部学刊*], 16, pp.49-51.