A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis

Maria Christofidou[1, 2], Nathan Lea[1], Pascal Coorevits[1, 2]
[1] The European Institute for Innovation Through Health Data (i-HD), Ghent, Belgium
[2] Ghent University, Faculty of Medicine and Health Sciences, Department of Public Health and Primary Care, Ghent, Belgium

Summary

Objective: This survey article presents a literature review of relevant publications aiming to explore whether the EU's General Data Protection Regulation (GDPR) has held true during a time of crisis and the implications that arose during the COVID-19 outbreak.

Method and Results: Based on the approach taken and the screening of the relevant articles, the results focus on three themes: a critique on GDPR; the ethics surrounding the use of digital health technologies, namely in the form of mobile applications; and the possibility of cross border transfers of said data outside of Europe. Within this context, the article reviews the arising themes, considers the use of data through mobile health applications, and discusses whether data protection may require a revision when balancing societal and personal interests.

Conclusions: In summary, although it is clear that the GDPR has been applied through a mixed and complex experience with data handling during the pandemic, the COVID-19 pandemic has indeed shown that it was a test the GDPR was designed and prepared to undertake. The article suggests that further review and research is needed to first ensure that an understanding of the state of the art in data protection during the pandemic is maintained and second to subsequently explore and carefully create a specific framework for the ethical considerations involved. The paper echoes the literature reviewed and calls for the creation of a unified and harmonised network or database to enable the secure data sharing across borders.

Keywords

COVID-19, data protection, ethics, privacy, public health

Yearb Med Inform 2021:226-32
http://dx.doi.org/10.1055/s-0041-1726512

1 Introduction

Late 2019 and early 2020 saw the arrival of the COVID-19 pandemic which resulted in a global health crisis and issues affecting countries worldwide. Through this past year, governments have expended great effort, in the form of both research as well as their overall healthcare systems, to better understand and contain the pandemic [1]. One of these efforts, in an attempt to gather information as quickly and efficiently as possible, has been the creation and operating of contact tracing applications and other digital health tools which enable the gathering of personal data and sensitive information [2]. These contact tracing applications have as their main objective to predominantly share knowledge about the virus and that, to be used across the majority if not the entirety of a population in order to be fruitful, retain data for research purposes or the secondary objectives of health authorities [3].

Within the European Union, the GDPR acts as the regulatory framework providing the necessary legal architecture by which the handling and processing of the personal data in this health crisis can be managed, particularly in the context of health mobile applications, in order to be lawful, fair, and reflecting the underpinning social and ethical values of the European Union. However, this begs the question as to the extent that the GDPR had to and can be applied when this particular type of data and information are needed for research under time pressure. As highlighted by academics, a guaranteed way by which this can be achieved is through collaboration and international health research efforts, with a vital source of information being the amount of digital health data that can be collected [3, 4]. However, this way in turn gives rise to questions surrounding the ethics of using citizens' data in a seemingly broad manner and places the public interest and the privacy of individuals on opposite ends of the scale. Consequently, this way also leaves room to question whether it is time to re-evaluate data protection overall when it comes to the privacy of citizens and whether it is time for the creation of a common COVID-19 database.

2 Objectives

This literature survey aims to identify and discuss the recurring themes surrounding the field of data protection and data sharing utilising the COVID-19 outbreak as a prime example on how this can be conducted at a time of crisis. It is due to this need for efficacy and efficiency that governments and organisations have deployed digital technologies in order to be able to obtain as much data as possible to comprehend and eventually adequately respond to the needs arising during the pandemic. Particular attention is therefore placed on both the implications of the GDPR with the rise of contact tracing applications and the ethical questions and dilemmas that come with the use of these technologies as described in the current literature.

3 Methods

To conduct this literature review, a search strategy was first developed to capture peer-reviewed publications related to the effect which COVID-19 had on the GDPR and how this is interconnected with mobile health applications. In order to ensure that coverage of the literature was as thorough as possible, a number of Medical Subject Headings (MeSH), terms used for indexing, cataloguing, and searching of biomedical and health-related information, and non-MeSH terms were selected and used as query terms, as illustrated in Table 1.

Table 1 Search Terms

MeSH Terms	Non-MeSH terms
COVID-19	Novel coronavirus
Privacy	Pandemic
Telemedicine	eHealth
Ethics	Digital health
Confidentiality	mHealth
Medical device legislation	Medical Devices
	Transparency
	Public emergency
	Personal data
	Data protection
	Public interest
	GDPR

The reasoning behind the deviation in terms was predominantly due to the fact that, given the rapidly developing situation, not all MeSH terms were immediately applicable, and by extension and so as to not restrict the research results, these were not strictly followed.

Subsequently, the authors agreed to limit the review of articles published between October 2019 and up to December 2020, given that the topic of the COVID-19 outbreak was discussed more widely in Europe during this period. As indicated in the PRISMA chart [5] below, the selected search query terms were run through the PubMed, Mendeley and GoogleScholar databases. Some additional papers were also included as part of the literature review process using the snowballing method.

Novel insights covering online learning methods, mental health, surgical procedures, reviews of specific mobile and track-tracing applications, or home technologies were excluded following abstract screening. Further, publications that were not written in the English language or where an English translation was not provided were also excluded as were publications which did not discuss the European data protection legislation or national implementations of the GDPR. From the shortlisted articles, 77 were read and reviewed in depth with articles that provided a review or commentary on the features and functionalities or a particular contact tracing application and articles which were not discussing privacy, data protection or GDPR within the pandemic context were subsequently excluded. This ultimately left 25 articles which were agreed to be seen as relevant according to the research area in question. The authors then discussed the publications and agreed to have a thematic review by identifying the running themes and to form part of the immediate source material for the article.

4 Results

On reviewing the remaining literature, three broad themes were recurring throughout the reviewed publications:

1) Critiques of the GDPR;
2) Ethical considerations arising from the use of data during the pandemic; and
3) The possibility of cross border transfers of said data outside of Europe.

The shortlisted papers have therefore been split and placed under the three thematic groups which are then sub-divided in accordance with the underlying concepts that they discuss and highlight, as illustrated in Table 3. Duplications in Table 3 as to the referring selected publications occur given that several of these articles discuss various aspects of the subject.

5 Discussion

5.1 GDPR Critique

The COVID-19 outbreak has been described as a real test for how data protection and privacy frameworks, such as the GDPR, corresponds to research during the pandemic from two angles. One angle is through the exemptions used by the respective national health authorities and governing parties provided under Article 9(2) of the GDPR in order to enable health data to be used for research purposes and another angle is through the use of digital applications on devices aimed to track citizen's movements and health status [4, 7]. This has naturally given rise to critique and criticism over the adequacy, efficacy and efficiency of the GDPR, as well as other legal and regulatory mechanisms, which enable the use and sharing of European digital health data whether used for research or otherwise. Questions have been raised as to whether, and the extent to which, the GDPR provides an adequate framework [4, 6, 7, 14] when faced with the need to obtain securely data on the one hand and for this to be done so in a time critical manner on the other. Some of these criticisms are arguably justified to a certain extent. However, there are explicit mentions in the GDPR provisions (such as Recitals 46 and 52) which state that certain types of processing of special category data are allowed on grounds of serving both the public interest, as well as the interests of data subject, for the purposes of humanitarian actions and disease prevention. These examples therefore evidence that Regulation makes room for and provides leeway for national instruments and organisations to handle data in situations comparable to the pandemic at hand [7, 13, 21].

A review of commentary and literature also notes the issues of rushed innovation and decision for the adoption of pre-existing technologies which has been criticised for creating new vulnerabilities in privacy and data protection [17]. These remarks on fast innovation in time-sensitive situations however act as a double edged sword, as at times its necessary to waive high regulatory standards to address the need for a solution which may result in the rushed deployment of solutions which do not fully comply with the data protection principles, as would for

Table 2 PRISMA Chart

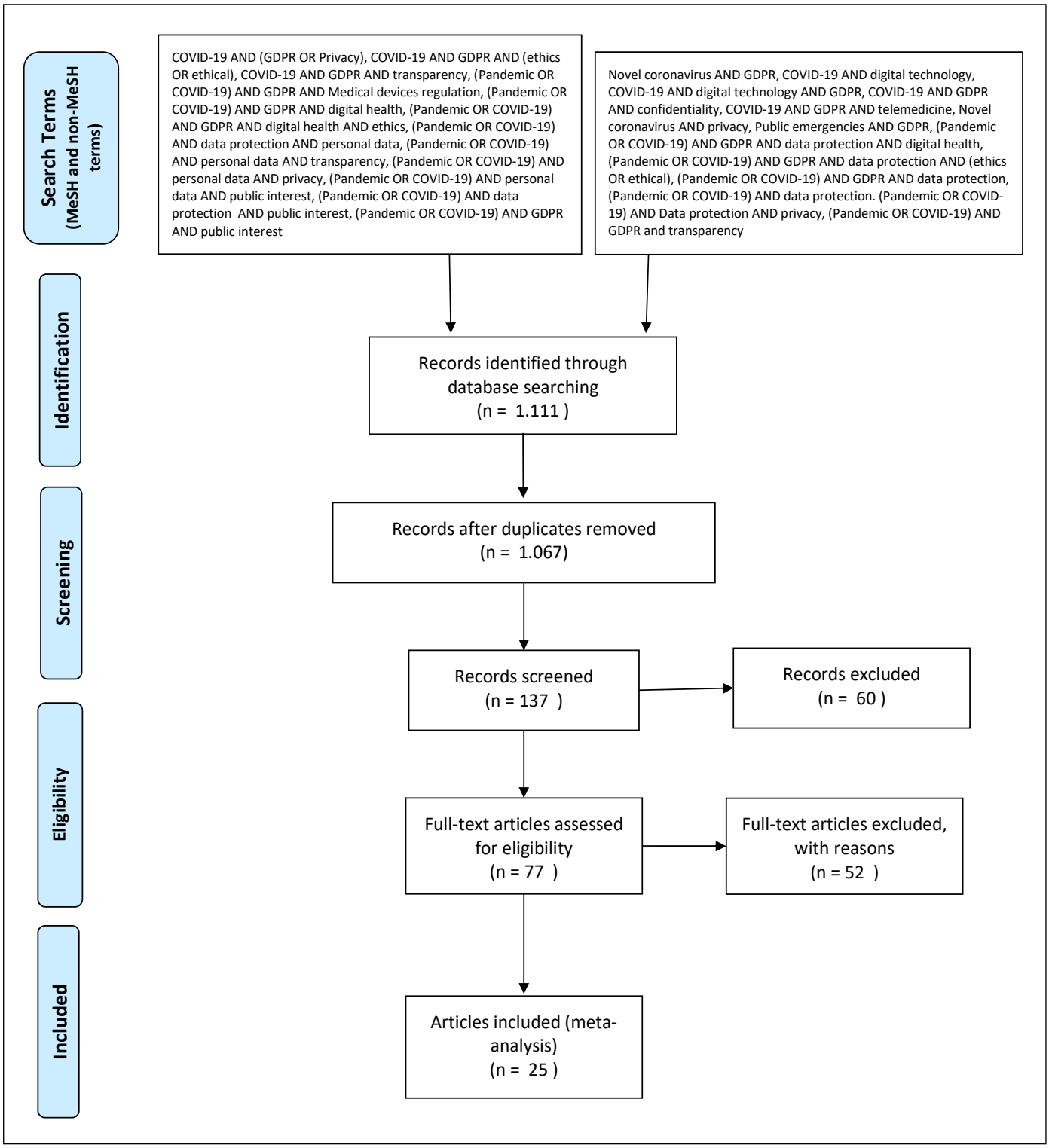

Table 3 Thematic review

1. GDPR critique
GDPR's operation for contact tracing apps, sharing tools and an analysis of how it applies [4,6-13] The authors overall discuss how the GDPR, being the key legal framework in data use and sharing, has been put to the test and the concerns arising which have made organisations to have a risk-averse approach in data sharing [4,6,7,11,12]. They analyse and assess how the legal grounds and guidance provided [6,7,12,13] and evaluate whether public interest basis may be more promising for research than a consent basis approach, given the high standards set out in the GDPR [12,13]. The literature also comments on the need for a proportional approach in data gathering which corresponds to the degree of emergency [9,12,13], how what seems to have risen is an inconsistent legal framework that impedes joint approaches [6,12,13] and how although these frameworks were not designed for AI surveillance, they have adapted to address concerns on privacy and human rights [10,13].
How and whether the GDPR and other data protection legislation is fit for purpose during a time of crisis such as COVID-19 [4,7,10-17] The authors analyse how and whether the GDPR and other data protection legislation and guidance is able to correspond during the current crisis by highlighting who is granted access to data [12,13,15,16] whether the removal of certain identifiers is sufficient to address privacy issues [23,25], the provisions which correspond to the research exemption [4], consent [14], public interest [12,17], and human rights [10,14,16]. It's stated and acknowledged that the GDPR makes explicit mentions of certain types of special categories of personal data processing on grounds of public interest, as well as serving the interests of data subject, for the purposes of humanitarian actions and disease prevention, which are comparable to the current situation, reflected in both Recital 46 and Recital 52 [7,13]. The issues as to whether the rushed decision for the adoption of pre-existing technologies and the regulatory aspect of rushed innovation are both discussed and criticised for leaving room for new vulnerabilities in privacy and data protection and the role and responsibilities attributed to the GDPR and to the national data protection authorities [17]. In this regard on the topic of 'explicit consent' for processing of health data and its adequacy, arguments are made that consent currently given online in emergency circumstances might be considered invalid [17]. A review of commentary and literature also notes that the duties of reporting and the scope of communications through the contact-warning apps, may be considerably expanded beyond what was originally foreseen in the relevant data protection guidelines [12] which in return has called for an ongoing evaluation of oversight by the relevant data protection bodies. Remarks are also made as to how in fast innovation where time is critical its sometimes necessary to waive high regulatory standards to address the need for a solution, which may in return prioritise functionality and usability over privacy [13,17].
Whether GDPR hinders or enables research and to what extend [4,7,10,13] The authors note that the general privacy principles do not prohibit the surveillance measures currently taken by governments, but on the contrary rather ensure the correct handling of the data once processed [13]. The literature analyses and assesses how the individual legal grounds and derogations support research [4,7] and comment on whether the GDPR's scope constitutes a hinderance or aids in advancing in conditions of uncertainty like the pandemic [7,10].
The connection between data protection, GDPR and fundamental rights [6,7,8,10,12-14,18,19] The authors analyse data protection and the GDPR through the lens of fundamental rights [18], discussing the principle-based approach contained in the framework and whether this is compatible and safeguards fundamental rights [6,7,8,10]. They look at the existing derogations and argue that the current data protection regimes do not mitigate concerns on this as their focus is not collective autonomy [14,13], and how these derogations and restrictions correspond to human rights [10,19].
The interpretation of GDPR on Member State level [6,8,12,13,20] Discussions are made as to the extent to which the GDPR leaves aspects of the public interest basis to be determined by individual Member States [6,8,12,13] and the aftermath that this has caused to a lack of uniformity [6,20].
GDPR and automated processing [10,15] Discusses how data protection and the GDPR falls within and can support automated processing [15], and the context this has in AI [10].

2. Ethical considerations
The balancing exercise and interplay between serving the public interest and state surveillance [3,9-13,17,21] The literature on this subject acknowledges that given the time-sensitivity of the issue, the rapid deployment and use of digital technologies such as contact-tracing applications has been proven useful [11,12,17]. The literature in this context discusses the approach countries have taken on the gathering and use of these data and discuss whether this is a slippery slope into surveillance or justified and proportionate in the name of the public interest [3,9,11,12,13,17,21]. Authors have commented on the concept of "ethical trade-offs". This has given rise to commentary stating that some limitations on liberty and privacy may be justified in the context of global health emergencies, although a tension may arise when these are placed on opposite ends of the scale [21]. The concept of "trade-offs" has also been discussed in the context of innovation and regulatory compliance, stating that at times foregoing high regulatory standards in order to rapidly address new demands at low cost is a worthy price to pay, which in return may result in privacy concerns [13,17]. Arguments are also made that, on the one hand the risks associated with personal data may evolve through new data collection tools are used, [12] whilst that the use of the applications, and the data gathered, can be autonomy enhancing [21]. Concerns are expressed as to whether this could be a threat to privacy [10,12,13] and whether these technologies were deployed with proper impact assessments, evaluations and adequate safeguards are in place to ensure that potential risks and privacy rights limitations are mitigated [12,13].
Privacy first v. data first approaches [3,10,12] The comparison between how various countries have taken an approach which either prioritise the privacy of its citizens [3,10,12] or the paramount role that the gathering of data, and therefore information, on the virus can benefit society [3,10].

Table 3 continued Thematic review

Prosocial motivations, transparency and solidarity [4,12,13,16,19]
The authors discuss the importance that the EU has placed on solidarity, which has been recognised and encouraged by its citizens through the use of their data, as well as the prosocial motivations that governments have which appear through the governance models they have adopted [4,13]. Discussions are made on the legitimacy of collecting this data and proposals are put forward on the need for transparency, verification and accountability to being the guiding principles [12,16], and the fulfilment of international obligations to collaborate and apply human rights [19].

Restriction of individual rights in the name of a public emergency [6,9,11-13,19]
The authors comment and discuss specific measures to safeguard the fundamental rights and the interests of the data subjects that are, or should be, taken into account and which are required when processing data [6,9,12,19]. Discussions are made as to whether an answer to whether restrictions on rights can be found through moral theories and the vital role of 'informational self-determination' [11]. Commentary is also made as to whether, in this context, the provisions of GDPR do not amount to a carte blanche [6].

Voluntary and mandatory use of mobile applications [3,12,15,20,21]
The authors describe the use of contact tracing applications and raise ethical concerns with regards to governments requiring their use or the voluntary basis and encouragement of this [3,15,20]. A discussion is also made as to whether this is feasible within Europe and constraints on privacy and liberty [20, 21].

Over-collection of data [3,9]
The authors discuss that on the one hand, the over-data collection can appear wasteful as it disposes of important amounts of data that could be of vital value in research, however it points out that privacy concerns are understandable given the nature of the date used and widespread adoption of the relevant applications is needed for the data to be of true value and size [3,9].

3. Cross border data transfers

Commentary on the differences and comparisons drawn between the EU and non-EEA countries [6,7,10,14,20]
The literature comments on the EU's mechanisms on data sharing and contrasts the GDPR and existing practices with how these operate when exchanging data with the US [6,14], given the narrower sector-specific US Acts [7] that leave gaps and the digital surveillance in Asia, the UAE, Singapore, Israel & South Korea [7,10,20].

Commentary on the existing tools and mechanisms in place to enable data transfers [6,16]
Authors discuss the existing limitations on data transfers across borders and analyse how these operate in practice such as the contractual agreements used by the EU institutions [6], with commentary made on the lack of protection against irresponsible technologies and suggestions on the relaxation of rules without having a necessary negative impact [16].

Proposals and calls for a harmonised approach and/or a common COVID-19 database [4,6,9,12,14,20]
The authors on the subject recognise that given the lack of integration and the various systems, there is an inconsistent framework that needs clarification and harmonisation [6]. This common database or framework has also been described as a cross-border and multisector collaboration that can either be based on existing partnerships [14, 20] or take the form of a newly created common COVID-19 database [4].
Proposals are made to the effect of ensuring that use and access must remain proportional to the degree of the emergency [9,12,14], such as the time frame limitation for the retention of the collected data, the need for transparency [9], and the inclusion of guiding principles and data practices [14].

example the processing of data for research and scientific purposes [13, 17]. This indeed has identified a gap in data protection rules and supports the argument for an ongoing evaluation of oversight by the relevant data protection bodies.

Another example that has given rise to critiques focuses on the use of 'consent' as a lawful basis in the reuse of sensitive health data, which can arguably be seen as challenging and even impractical [6]. This would be due to the multiple elements that this would entail to meet [22] as well as the fact that in reality, consent would entirely depend on the unlikely practicability of re-contacting all data subjects should the original purpose of their data collection not be the same as the re-use. In this regard on the topic of 'explicit consent' for processing of health data and its adequacy, arguments are made that consent currently given online in emergency circumstances might be considered invalid [17]. Though 'consent' is not the sole lawful basis that can be used for the reuse of data, the public interest' basis has also received criticism due to the lack of a uniform application and interpretation that exists on a national level [6].

It is important however to note that this lack of uniformity is, in part, due to the fact that each Member State has a margin of appreciation when it comes to fully implementing EU legislation. This is in order to ensure that this adoption of the GDPR on national levels is compatible with other data protection rules and mechanisms which the relevant derogations provide flexibility for in the application of the law. In the present case, this is conducted in order to ensure that the GDPR, which purely as a legal framework which favours innovation and allows for the introduction of technologies that process personal data to the market [13], is implemented in Member State law and operated in harmony with national data protection regulations as well as to allow room for draft secondary legislation on national levels. Therefore, though the additional levels of legislature or the powers conferred under the GDPR on Member States to pass additional restrictions on the processing of health and genetic data may seem additional hurdles to overcome or

potential divergence, this process allows space for interoperability and for each country to apply data protection correctly and as best suited in the jurisdiction. Further, as cited by literature and the European Data Protection Board ('EDPB'), "data protection rules like the GDPR don't hinder measures taken in this fight" but rather aid in advancing it [7,23]. European funded projects, such as the Helical Innovative Training Network [24], highlight that though sites of a consortium may be based in different parts of Europe and have their own national data protection rules, the GDPR is a means of enabling research and an effort towards European harmonisation. In addition, from a policy perspective it is important to bear in mind that healthcare is overall a Member State competency.

5.2 Ethical Considerations

The results of a European research study which concluded that many citizens would accept the secondary use of their data for health-related research under the research exemption of the GDPR based on prosocial motivations such as solidarity [4] arguably indicates that many trust the means by which governments gather their data through the use of contact tracing/warning applications and devices (whether this be due to the mechanisms that enable data protection or faith in their government). The literature considering the ethical implications of the subject has identified the diverging views and approaches taken in data collection and distinguishes between the "privacy-first" and the "data-first" approach [3]. While the former has at the forefront to protect citizens' data at the cost of extremely limited access for public health authorities and researchers, the latter aims to store large amounts of data which may come at the expense of citizens' privacy [3].

Fears have been expressed over a "surveillance state", which may be justified given that the data gathered by the contact tracing applications are 'the most personal and intimate data a government has ever sought to gather about its own citizens' [3], it is important to consider that perhaps in reality these fears may have little foundation. The use of contact tracing applications as indicated in literature and the mass media is conducted on a voluntary basis in Europe, a different approach taken than non-EEA countries such as China, India and Qatar all of which have legally mandated the use of the applications [15, 20].

The concept of "ethical trade-offs", which arguably is a central feature in the discussions of data protection and priority setting during the global health emergency, further highlights and even provides a somewhat acceptable middle ground solution when choosing between innovation that enables to better understand and face the challenges posed by the pandemic and regulatory compliance [13,17]. Although this solution evidences a shift which has been observed towards protecting public health over privacy across many levels, this is always done so long as it adheres to the principles of purpose limitation, proportionality and transparency [26]. As clearly stated in communication between the European Data Protection Board (EDPB) and the European Commission [27], an enactment of national laws which would result in the temporary limitation of individuals' rights in case of an emergency is not a blanket policy as stipulated under the GDPR. In such an event, a solid legal framework needs to be implemented which defines in detail the scope, the limited duration of the use of mobile phone information, disabling of tracking systems and deletion of the gathered data once the crisis is over. Further, the mere existence of data protection impact assessments, mandatory under GDPR (Articles 35, 36 and Recitals 89 - 96), as well as data protection authorities and data protection supervisory bodies should provide solace in that the protection of citizens' privacy interests is paramount and protected [10]. Given the sensitivity of the subject and the complex nature of ethics in the use of personal sensitive data, a comprehensive review of the ethical standards is needed.

5.3 Cross Border Data Transfers

The transfer of data, and specifically the cross-border transfer of European data outside of the Union, has been a subject that has received meticulous criticism. The literature has commented on the complex mechanisms and existing safeguards which either hinder or make the transfer particularly difficult to be achieved in practice [14]. Namely, the literature reviewed and commented on the limitations which exist on data sharing, either due to the need to inform the data subject about the particular transfers, the lack of practicability of standard contractual clauses provided by the European Commission, given that the inability of the US to consent to these and the administrative procedures which result in delays should alternative means be sought [14]. Further, the lack of a global consensus on best practices for contact tracing and the varying approaches taken by countries has been identified as issues which, although collectively generating vast amount of data which would be seen as useful, result in scarce efforts given the lack of integration [7]. The reviewed literature commenting on reform has been unanimous in calling for the creation of integration and collaboration. As highlighted, one of the lessons learned from the pandemic has been the evident need for cross-border domain co-operation that supports stakeholders and, in particular, policy makers with responsibilities in the areas of public health [1]. Whether it is through the use of existing networks or the creation of multidisciplinary partnerships, there is a call for a platform which enables the safe exchange of available data.

5.4 Future Research Directions

The unusual nature of the pandemic and commentary to date suggests that the views surrounding the impact of the GDPR, the implications of retaining rapidly collected personal data at scale and the societal and ethical treatises are likely to evolve. The area is one which overall requires further research and a recommendation for further work and follow-up in the following 8-12 months post publication of this paper is needed when taking into consideration the fast-developing nature of policy, such as the proposal for Digital Green Certificates [27], the deployment of technology for the gathering of data and data protection concerns that arise and how these are addressed, such as the Right to be Forgotten or the Right to be Informed. Moreover, in similar context, further research is recommended to explore and understand the patient community views and outlook on whether the GDPR practically corresponds to their expectations in

circumstances of time sensitivity as well as the potential mechanisms that would enable the betterment of cross border data transfers. This can also be conducted, in addition to the means used in the present paper, through a review of legal databases as well as through interviews of stakeholders.

6 Conclusions

The reviewed publications discuss how COVID-19 has acted as a prime case example of an urgent need to collect data from citizens on both their exposure and health experience during a public health emergency. The outbreak has also clearly indicated the ability of governments, health authorities and researchers to harvest this data efficiently and securely in order to reliably learn from it. Through this experience, the GDPR has been tested and put under pressure to indicate whether it can indeed in practice deliver in both efficacy and efficiency. Though certain data protection rules can have very specific derogations, the overall system may be a difficult one to implement in practice when it comes to data transfers lacking concrete definitions and requiring very specific circumstances and high thresholds to meet. This article echoes that given the lessons learned, there is a clear and distinct need for a harmonised and collective effort and approach to global research. The authors therefore recommend further review and research to firstly ensure that an understanding of the state of the art in data protection during the pandemic is maintained and secondly support the call that has been expressed for a common multinational database that would support a GDPR and data protection compliant effort into global research.

Acknowledgments

This work has been performed as part of the HELICAL Innovative Training Network, a European Commission funded project under the Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 813545.

References

1. UK Government. UK Coronavirus Legislation and guidelines. 2020. Dec 1, [2020-12-18] https://www.legislation.gov.uk/coronavirus. BBC News. Oxford Covid vaccine: Regulator asked to assess jab. 2020. Nov 27 [20202-12-18] Available from: https://www.bbc.com/news/uk-55096434. Luxembourg government. Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. Journal officiel du Grand-Duché de Luxembourg. 2018. Aug 01, [2020-12-18] Available from: https://tinyurl.com/y442zgzz
2. European Commission. 2020 Mobile contact tracing apps in EU Member States. [2020-12-18] Available from: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en
3. Fahey RA, Hino A. COVID-19, digital privacy, and the social limits on data-focused public health responses. Int J Inf Manage 2020 Dec;55:102181.
4. McLennan S, Celi LA, Buyx A. COVID-19: Putting the General Data Protection Regulation to the Test. JMIR Public Health Surveill 2020 May 29;6(2):e19279
5. Moher D, Liberati A, Tetzlaff J, Altman DG, PRISMA Group. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. PLoS Med 2009;6(7):e1000097.
6. Becker R, Thorogood A, Ordish J, Beauvais MJS. COVID-19 Research: Navigating the European General Data Protection Regulation. J Med Internet Res 2020 Aug 27;22(8):e19799.
7. Bradford L, Aboy M, Liddell K. COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. J Law Biosci 2020 May 28;7(1):lsaa034.
8. Audrey Guinchard. Our digital footprint under Covid-19: should we fear the UK digital contact tracing app?, International Review of Law, Computers & Technology 2021;35:1:84-97.
9. Schneble CO, Elger BS, Martin Shaw D. Data protection during the coronavirus crisis. EMBO Rep 2020 Sep 3;21(9):e51362.
10. Shachar C, Gerke S, Adashi EY. AI Surveillance during Pandemics: Ethical Implementation Imperatives. Hastings Cent Rep 2020 May;50(3):18-21.
11. Stoeger K, Schmidhuber M. The use of data from electronic health records in times of a pandemic-a legal and ethical assessment. J Law Biosci 2020 Jun 16;7(1):lsaa041
12. Shabani M, Goffin T, Mertes H. Reporting, recording, and communication of COVID-19 cases in workplace: data protection as a moving target. J Law Biosci 2020 Apr 22;7(1):lsaa008.
13. Newlands M, Lutz C, Tamò-Larrieux A, Fosch Villaronga E, Harasgama R, Scheitlin G. Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. Bog Data & Society 2020;7:2. https://doi.org/10.1177/2053951720976680
14. Zwitter A, Gstrein OJ. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. Int J Humanitarian Action 2020;5(4). Available from: https://doi.org/10.1186/s41018-020-00072-6
15. Lucivero F, Hallowell N, Johnson S, Prainsack B, Samuel G, Sharon T. COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale. J Bioeth Inq 202;17(4)835-9.
16. Almeida BA, Doneda D, Ichihara MY, Barral-Netto M, Matta GC, Rabello ET, et al. Personal data usage and privacy considerations in the COVID-19 global pandemic. Cien Saude Colet 2020 Jun;25(-suppl 1):2487-92.
17. Harris M, Bhatti Y, Buckley J, Sharma D. Fast and frugal innovations in response to the Covid-19 pandemic. Nat Med 2020;26(6):814–7.
18. Alexopoulos AR, Hudson JG, Otenigbagbe O. The Use of Digital Applications and COVID-19. Community Ment Health J 2020 Oct;56(7):1202-3.
19. Sekalala S, Forman L, Habibi R, Meier BM. Health and human rights are inextricably linked in the COVID-19 response. BMJ Glob Health 2020 Sep;5(9):e003359.
20. Horgan D, Hackett J, Westphalen B, Kalra D, Richer E, Romao M, et al. Digitalisation and COVID-19: The Perfect Storm. Biomed Hub 2020;5(3):1341-63.
21. Parker MJ, Fraser C, Abeler-Dörner L, Bonsall D. Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. J Med Ethics 2020 Jul;46(7):427-31.
22. European Data Protection Board. EDPB Guidelines 05/2020 on consent under Regulation 2016/679 (Version 1.1) 2020. May 04, [2020-12-18]. Available from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
23. European Data Protection Board. Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak. 2020 Mar 16, [2020-12-18]. Available from : https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en
24. Helical Innovative Training Network, European Commission Project under the Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 813545.
25. European Commission. Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29
26. European Data Protection Board. EDPB Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic. 2020. Mar 19, [2020-12-18]. Available from: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-concerning-european-commissions-draft-guidance_en
27. European Commission. Communication "Coronavirus: Commission proposes a Digital Green Certificate". [2021-03-17] Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181

Correspondence to:
Maria Christofidou
E-mail: Maria.Christofidou@UGent.be