EJPLT
ISSN 2704-8012

The right to privacy v. public safety. Covid-19 contact tracing applications

HELENA KORDASIEWICZ
Student, University of Warsaw

Abstract
During the COVID-19 pandemic many countries have created contact-tracing applications to protect the citizens' safety. This article discusses the rules for data processing in the context of a pandemic, especially considering said applications. Their source codes have been confronted with the laws and guidelines on data processing. The aim of the study is to evaluate whether the exceptions for processing of data in case of criminal threats and public health threats can be considered analogous.The analysis covers European Union laws, the Court of Justice of European Union case law. The conclusions provide insight on the permissibility of using analogies for establishing laws in this regard.

Durante la pandemia COVID-19 molti Paesi hanno creato applicazioni di tracciamento dei contatti per proteggere la sicurezza dei cittadini. Questo articolo discute le regole per il trattamento dei dati nel contesto di una pandemia, in particolare considerando tali applicazioni. I loro codici sorgenti sono stati confrontati con le leggi e le linee guida sul trattamento dei dati. L'obiettivo dello studio è valutare se le eccezioni per il trattamento dei dati in caso di minacce criminali e di minacce alla salute pubblica possano essere considerate analoghe. L'analisi riguarda le leggi dell'Unione europea e la giurisprudenza della Corte di giustizia dell'Unione europea. Le conclusioni forniscono indicazioni sull'ammissibilità dell'uso di analogie per la definizione di leggi in materia.

Keywords: contact-tracing; Court of Justice of the European Union; COVID-19;

Summary: Introduction. – 1.Privacy and public safety in the European legal framework. – 2. Balancing data protection and preventing crime in the case law of the Court of Justice of the European Union. – 3. Contact tracing in a pandemic. – 4. Data protection and public safety in criminal and health threats: a comparison. – 5. Conclusions.

Introduction.

The issue of balancing values in regard to public safety during the pandemic has been among the topic of focus of academics and legislators ever since the outbreak of SARS-CoV-2 virus in early 2020. The discussion falls not only on the line of balancing public safety with fundamental rights, such as liberty and the right to privacy, but also the mentioned fundamental rights with one another[1]. During the pandemic, among limited rights were the freedom of movement, freedom of assembly, right of access to healthcare (as most medical resources have been redirected towards mitigating the pandemic) and,

[1] Parker, M J, Fraser, C, Abeler-Dörner, L, Bonsall, D, *'Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic*' (2020) 46 Journal of Medical Ethics 427, 431.

the topic of this paper, the right to privacy. The emergence of the COVID-19 pandemic has created a concern surrounding it on an unprecedented scale. In attempts to contain the pandemic countries have introduced mask mandates, travel restrictions, mandatory remote work, lockdowns and implemented numerous tracking systems. During this pandemic, various policies, including contact tracing and providing information, have been implemented via smartphone applications, which highlights issues relating to health illiteracy, structural inequalities and data privacy[2]. Programs monitoring citizens' interactions, and in some cases even whereabouts, have become a crucial part of everyday life and using them was oftentimes inevitable.

The aim of the study is to evaluate whether the exceptions for processing of data in case of criminal threats and public health threats can be considered analogous. For this purpose, the similarities and differences between the data processing regimes for health and criminal threats are analysed. First part of the paper consists of a summary of the legal framework in which such solutions came to be introduced, ie laws provided by the European Union, guidelines and rules stemming from the Court of Justice of European Union (CJEU) case law. Later, cases predating the pandemic and regarding situations in which the threat to public safety was criminal are analysed as they provide important insight into how data ought to be processed in times of danger by introducing exceptions to the general data protection laws. As a proof of why this topic is worth researching, the efficacy and significance of contact tracing for mitigating the pandemic will be analysed. In order to comprehensively describe the rules for processing of data within contact tracing applications, guidelines for creating them, provided by both national and European bodies, have been scrutinized. For conducting a brief analysis of how the applications have complied with the guidelines, their source codes have been assessed. Finally, the rules applied to data processing with the purpose of guarding public safety, from threats of criminal or public health nature, have been compared to determine whether a legal solution, regulating both the scenarios on the level of the European Union, is feasible.

1. PRIVACY AND PUBLIC SAFETY in THE EUROPEAN LEGAL FRAMEWORK.

The European Union's data protection regime is among the strongest in the world[3]. The EU General Data Protection Regulation, further referred to as the GDPR[4], is the primary source of rules. As the name suggests, the GDPR describes general rules for processing of data in the European Union, provides numerous definitions and obliges member states of the EU to adjust their legal systems to its provisions and create or modify control institutions. The GDPR doesn't cover all of the instances in which data is being processed, other legislative texts compliment the system with specific guidelines. Among them, the

[2] Pandit, J A, Radin, J M, Quer, G, et al. *'Smartphone apps in the COVID-19 pandemic'* (2022) 40 Nat Biotechnol 1013–1022. https://doi.org/10.1038/s41587-022-01350-x

[3] Dijkstra, H, De Ruijter, A, '*The Health-Security Nexus and the European Union: Toward a Research Agenda*' (2017) 8(4) European Journal of Risk Regulation 613, 625.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard 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

Health Threats Directive[5], the Directive on privacy and electronic communications[6], and the Police Directive[7] are the most important in regard to measures used to mitigate the pandemic. Those legislative acts provide more precise guidelines and possible exemptions from adhering to the GDPR, but only in justified public interest.

The cornerstone of the GDPR framework is the principle of legality; data processing has to lawful, fair and transparent and when it is automated, partially automated or to be part of a data set has to fulfil the requirements of legality, proper documentation, being performed on minimal necessary amounts of data and not without regard to the data subject. Those rules are far from self-explanatory and the Court of Justice of the European Union is faced with hundreds of cases surrounding this topic each year[8].

When substantial public interest is demonstrated rights of individuals stemming from those regulations may be subject to limitations, within the principle of proportionality. However, guidance on how to measure proportionality in this context is not sufficient and interpretation of existing rules differs from country to country[9]. Moreover each Member State has national acts and provisions on data protection. Due to the high level of integration between countries within the European Union a common legislative solution for them all appears desirable, but is yet to be achieved.

Partly due to the differences in legal systems, during the pandemic Member States have developed their own contact tracing applications which were not synchronised with one another. When the so called covid-passports were created, after the introduction of vaccines, they weren't initially valid between countries, which further demonstrates the insufficient cooperation in this regard. Had a contact tracing application been developed on a European level, citizens lives would have been easier and, arguably, the pandemic could have been mitigated more effectively.

2. BALANCING DATA PROTECTION AND PREVENTING CRIME IN THE CASE LAW OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

Judgments of the Court of Justice of the European Union with signatures joined C-511/18, C-512/18 and C-520/18 (further referred to as the La Quadrature du Net case)[10], C-623/17 (further referred to as the Privacy International case)[11] and C-207/16 (further referred to as the Ministerio Fiscal case)[12] have been analysed with the purpose demonstrating

[5] Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293.
[6] 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 the electronic communications sector OJ L 201.
[7] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119.
[8] data from https://curia.europa.eu/jcms/jcms/j_6/en/
[9] Van Kolfschooten, H, De Ruijter, A, '*COVID-19 and privacy in the European Union: A legal perspective on contact tracing*' (2020) 41(3) Contemporary Security Policy 478, 491.
[10] Judgment of 6 October 2020, *La Quadrature du Net,* C-511/18, C-512/18 and C-520/18, [Text rectified by order of 16 November 2020], ECLI:EU:C:2020:791
[11] Judgment of 6 October 2020, *Privacy International,* C-623/17, ECLI:EU:C:2020:790
[12] Judgment of 2 October 2018, *Ministerio Fiscal ,* C-207/16, ECLI:EU:C:2018:788

privacy and data protection measures applicable when processing data is in exception to the GDPR on the basis of guarding public safety by preventing and prosecuting crime. The judgements concern processing data in criminal procedures and when a threat to national security of Member States related to terrorism occurs. Conclusions from them can be relevant to processing personal data during a pandemic as both situations regard the exemptions from following general data protection rules in order to avoid danger to public safety. While the COVID-19 pandemic is unprecedented in modern-day Europe, threats of criminal or terrorist type have always been present, hence the selection of guidelines is vastly broader for the criminal risks and that may even necessitate applying analogies.

In the La Quadrature du Net judgement, CJEU has highlighted that GDPR provisions may be subject to limitations to safeguard, *inter alia*, national security, defence and public safety. French courts posed preliminary questions on whether Member States were allowed to introduce national legislations which would impose a requirement of general and indiscriminate retention of traffic and location data in light of Article 15(1) of the ePrivacy Directive. The CJEU has answered that such legislations are precluded, as well as legislation which would require providers of communications services to grant competent national authorities access to that data, reason being that such data can indirectly reveal other information, including sensitive information such as 'sexual orientation, political opinions, religious, political, societal or other beliefs and state of health'[13]. It meant, that a national legislation which labels such data as not being identifiable does not necessarily prevent it from being classified as personal data, if the *de facto* state of data requires so.

The Court has also reinforced an obligation for data which has been automatically processed to be reassessed by non-automated means, due to the possible margin of error. A (national) court cannot apply national law allowing limits of temporal effects of a declaration of illegality, which it is bound to make under that law in regard to legislation imposing an obligation on providers of electronic communications services for 'general and indiscriminate retention of traffic and location'[14], hence stressing the importance of data protection even in the case of a criminal threat.

In the Privacy International case, a question whether the practices used by British security and intelligence to acquire and use bulk communications data, which have been made public, were legal was posed. CJEU assessed this within the legal framework of the ECHR[15] and European Union law. In this case, personal data such as biographical and travel information as well as communications data, which was liable to include information covered by professional secrecy and journalistic material were processed, notably using' unspecific, automated processing, with the aim of discovering unknown threats'[16]. The court has answered that Article 4(2) of the Treaty on European Union and Article 1(3) of the Police Directive have legislative measures which would require providers of electronic communications services to retain such data and grant 'competent national authorities'[17] access to said data. Notably, the court has said that such activity

[13] Judgment of 6 October 2020, *La Quadrature du Net,* C-511/18, C-512/18 and C-520/18, [Text rectified by order of 16 November 2020], ECLI:EU:C:2020:791
[14] ibid.
[15] European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950.
[16] Judgment of 6 October 2020, *Privacy International,* C-623/17, ECLI:EU:C:2020:790
[17] ibid.

cannot be regarded as activity characteristic of the State referred to Article 1(3) and creating a distinction based on the subject doing such processing is necessary[18].

In the third analyzed case, Ministerio Fiscal[19], the court was deliberating on what ought to be considered a metric of seriousness of crime. However, the facts of the case present an interesting perspective. Due to a complaint about a robbery of a mobile phone and a wallet, the Spanish Police has made a request to the Magistrate for access to phone numbers which have been contacted via the stolen phone and for personal information about owners of those numbers. CJEU has ruled that such a measure would not be in accordance with the principle of proportionality. This provides an insight into what the court deems acceptable in violations of data protection laws. As shown above, even in the case of protection of a right as fundamental as the right to property, data protection laws remain relevant and safeguarding property does not, on its own, legitimize making exceptions in measures of data protection.

3. CONTACT TRACING IN A PANDEMIC

Guidelines

Contact tracing on such a wide scale has only been introduced during the COVID-19 pandemic; most of the research about this topic is recent and related to combating the ongoing pandemic. Contact tracing is a crucial tool because, according to early research, around 50% of all infections have been transmitted via a person who was either pre-symptomatic or before the test could have been positive, often both[20]. Hence, only isolating individuals who have shown symptoms of the disease was not going to stop the spread of the virus. Generally speaking, transmission of infectious diseases can be divided into four categories: symptomatic, pre-symptomatic, asymptomatic and environmental[21]. Traditional, manual tracing of contacts of infected persons can be effective when transmissions are of the symptomatic type, but has proven itself to be insufficient in the light of COVID-19; it was not fast enough. However, the issue of its time efficiency can be eliminated via the use of a mobile app[22].

Works on developing the applications have begun almost immediately when the pandemic has started, but were conducted only on the national scale. In this light, the European Data Protection Board (EDPB) and the European Commission have developed guidelines.

EDPB guidelines on the use of location data and contact tracing tools, issued in April of 2020[23], is focused on ensuring compliance of such applications with data protection laws, as data-driven solutions were 'raising numerous privacy concerns'.[24]

[18] such distinction was not deemed necessary in the *La Quadrature du Net* case.
[19] Judgment of 2 October 2018, *Ministerio Fiscal* , C-207/16, ECLI:EU:C:2018:788
[20] Parker, M J, Fraser, C, Abeler-Dörner, L, et al, '*Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic*' (n 1)
[21] Ferretti, L, Wymant, C, Kendall, M, Zhao, L, Nurtay, A, Abeler-Dörner, L, Parker, M, Bonsall, D, Fraser, C, *'Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing'* (2020) 368(6491) Science 408, 412
[22] ibid.
[23] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Adopted on 21 April 2020, European Data Protection Board.
[24] ibid.

The two primary purposes of the app would be to access the *effet utile* of confinement measures (using location) and interrupting contamination chains as early as possible (using contact-tracing, based on proximity). The main conclusions from the guidelines are that the technology should be centred on proximity to other users, and not tracing location or movement of individuals. The EDBP has recommended establishing a controller for such data, ie a national health authority and defining the purposes, which are to be the legal basis for processing data, specific enough to prevent further processing of said data. The Guideline also suggests the data to be deleted or at least further anonymised once the pandemic comes to an end. Another important part of the document is proposing the applications to be open-source.

The European Commission, in turn, has underlined the importance of voluntary character of the applications[25], as they come with a high level of intrusiveness; not mandating using them should lead to higher trust, and in turn to higher compliance. Of course, the Guidance mentions the classic principles of data processing. Among them, data minimisation, which is to be achieved by choosing to use proximity measured with the use of Bluetooth Low Energy solution, rather than collecting location data of the users. This method has also been described as more precise, hence more effective for the purposes of contact tracing. The Commission recommends all of the information to be stored in a decentralised way, meaning that identifiers of people with whom the user has been in contact with should be stored on the mobile device itself, in a form of encrypted identifiers; the encryption ought to be 'state-of-the-art'. After the initial debate on the effectiveness and legal compliance of the centralised and decentralised approach[26], most of the introduced applications have been designed in the latter format. The Guidance also contains a requirement of limiting data storage — all of the proximity data should be deleted within a month or after an individual has tested negative for COVID-19.

Reality

The following part will demonstrate how Spain and the United Kingdom have developed their applications and compare the source code with guidelines. The choice of countries was dictated by their efforts into research on the effectiveness of the applications. While the UK is no longer in the European Union, it is included it in the analysis, as its regulation on data protection after having left the EU is analogous to the GDPR as well as due to the close economic and cultural ties between this country and the European Union.

The first part of the analysed studies on the effectiveness of contact tracing have limited applicability to the current state of the pandemic, as they have been conducted before vaccination has become available to the general public. Multiple frameworks have been proposed to assess the effectiveness of the applications, however the precise definition of their success is still to be created, as the field of digital epidemiology further develops[27]. Moreover, it has been shown that various factors influence the spread of the

[25] Communication from the Commission - '*Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protectio*n' 2020/C 124 I/01, C/2020/2523, OJ C 124l.
[26] White, L, Van Basshuysen, P, '*Privacy versus Public Health? A Reassessment of Centralised and Decentralised Digital Contact Tracing*' (2021) 27(2) Science and Engineering Ethics. https://doi.org/10.1007/s11948-021-00301-0
[27] Hernández-Orallo, E, Manzoni, P, Calafate, C T, et al, 'A methodology for evaluating digital contact tracing apps based on the COVID-19 experience' (2022) 12 Sci Rep 12728. https://doi.org/10.1038/s41598-022-17024-2

pandemic (not all of them being strictly related to sole contact with the virus) including the socio-economic background of the data subjects[28].

Naturally, national entities have also been working on guidelines. A report to the NHSX[29] based on a model of 1 million individuals, that is a representation of a catchment area of a single NHS trust, includes a description of measuring the probability of transmission. The calculations take into account the stage of infection, the network within which a contact has occurred and two aspects dependent on age of the persons: infectiousness of the transmitter and the susceptibility of the recipient.

Because the report above has demonstrated that 'digital tracing has the potential to make a substantial impact in suppressing the SARS-CoV-2 epidemic' an app was in fact developed; the code has been made publicly available[30]. The repository, along with the application code, contains a 'Architecture guidebook', which in the point 'Principles' once again states that the app is to be in compliance with data protection laws and focus on data storage minimisation.

However, there are a few objects within the code which have not been described in the basis for processing or anywhere else in descriptions of functioning of the application. There are some unexpected differences in analysis of the data for England and Wales, some of which are irrelevant in the context of data protection laws, such as the 'indexCaseSinceSelfDiagnosisUnknownOnset' field which describes the behaviour of the system when user did not input a start date of symptoms having a different amount of days for the two regions.

What is more relevant, the repository contains items processing of which has no legal basis. Processing of data, *ex definitione* includes storing data. Because of that, in spite of the CSV files mentioned below seemingly not being actively used, the sole fact of their existence poses a question. Those include files containing information on the ethnicity of local authorities, religion of local authorities and their placement has neither a legal nor a logical explanation. This part of the repository[31] also stores data about the demographic of the region and the IMD rank (an index of local deprivation), which however without a legal basis, do have a scientific justification of possibly influencing the local spread of the virus.

A contrario, the Spanish application, COVID-19 Radar contains and stores only the data strictly necessary for the purposes for which it has been developed[32]. What is important to note, they have not substantially differed in effectiveness, as described below.

Effectiveness

---

[28] Horton, R, *'Offline: COVID-19 is not a pandemic'* (2020) 396(10255) The Lancet 874. https://doi.org/10.1016/s0140-6736(20)32000-6

[29] Hinch, R, Probert, W, Nurtay, A, et al, *'Effective Configurations of a Digital Contact Tracing App: A report to NHSX'* (2020) Pathogen Dynamics Group, Big Data Institute, Nuffield Department of Medicine, University of Oxford; Wellcome Trust Centre for Ethics and the Humanities; faculty.ai; IBM UK; UCL/Alan Turing Institute.

[30] *NHS COVID-19 App source code:* nhs-covid19, August 13th 2020, covid19-app-system-public, https://github.com/nihp-public/covid19-app-system-public, accessed on April 27th 2022

[31] *NHS COVID-19 App source code,* covid19-app-system-public/src/static, 13 August 2020, https://github.com/nihp-public/covid19-app-system-public/tree/master/src/static, accessed on April 27th 2022

[32] COVID-19 RADAR App source code. GitHub. Accessed on 27 April 2022, at https://github.com/radarcovid

A study performed on the Spanish app[33] has identified seven Key Performance Indicators: adoption, adherence, compliance, turnaround time, follow-up, overall detection rate and hidden detection. The authors also highlight a crucial advantage of a digital contact tracing solution, which besides the turnaround time, turned out to be the hidden detection. Overall, the percentage of hidden close-contacts is around twenty-three to thirty-nine percent, and all of those contacts would have gone unnoticed had traditional, manual contact tracing been used. An aspect worth noting is the flexibility of the Spanish solution. Initially it has been set up to note interactions longer than fifteen minutes and closer than two metres, but those parameters can be adjusted as further research is conducted. In the testing stage, performed in La Gomera, around 33% of the population has downloaded the application and compliance has been high. The aftermath studies on the Spanish solution show, that for the effectiveness of TTI (Test-Trace-Isolate) approach, extensive work in the field of educating the public on the virus is necessary.[34] The NHS application has been downloaded by 28% of the population[35] and between September 24th and December 2020, 1.7 million notifications have been sent. The probability of infection in the notified person was between 5.96 and 6.09 percent. Later studies suggest, that the app could have prevented up to a million cases of COVID in a single year[36]. During its peak, the British app has been active for 38% of the population[37]. It is important to note, that promotion of the app[38] has stressed the privacy aspect of it — perceived compliance with data protection is an important factor for deciding whether to disclose personal data[39].

4. DATA PROTECTION AND PUBLIC SAFETY IN CRIMINAL AND HEALTH THREATS: A COMPARISON

Despite European Law not being imperceptive to the existence of a systemic connection between public health and security policies, exemplified by the Health Threats Directive[40], the plausible implication for the area of national public health of each state have not been 'considered in a truly comprehensive way'[41]. The issue of an insufficient legislative connection between the two concepts has also been raised in the literature[42]. Drivers for implementing a more comprehensive linkage have been identified as follows: systematic risks and management strategies, reactive event-driven policy-making, EU-

[33] Rodríguez, P, Graña, S, Alvarez-León, E, et al, *'A population-based controlled experiment assessing the epidemiological impact of digital contact tracing'* (2021) 12(1) Nature Communications
[34] De Nadai, M, Roomp, K, Lepri, B, et al, '*The impact of control and mitigation strategies during the second wave of coronavirus infections in Spain and Italy*' (2022) 12 Sci Rep 1073. https://doi.org/10.1038/s41598-022-05041-0
[35] Wymant, C, Ferretti, L, Tsallis, D, et al, *'The epidemiological impact of the NHS COVID-19 app'* (2021) 594(7863) Nature 408, 412.
[36] Kendall, M, Tsallis, D, Wymant, C, et al, '*Epidemiological impacts of the NHS COVID-19 app in England and Wales throughout its first year*' (2023) 14 Nat Commun 858. https://doi.org/10.1038/s41467-023-36495-z
[37] ibid.
[38] https://www.gov.uk/guidance/nhs-covid-19-app-your-data-and-privacy
[39] Dimodugno, M, Hallman, S, Plaisent, M, Bernard, P, '*The effect of privacy concerns, risk, control, and trust on individuals decisions to share personal information: A game theory-based approach*' (2021) 2090(1) Journal of Physics 012017. https://doi.org/10.1088/1742-6596/2090/1/012017
[40] Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293.
[41] Dijkstra, H, De Ruijter, A, '*The Health-Security Nexus and the European Union: Toward a Research Agenda*' (n 3)
[42] ibid.

level entrepreneurship and securitisation across policy areas[43]. The reactive, event-driven policy-making has been especially prevalent in the aspect of attacks related to transportation, which included the 9/11 attacks in the United States in 2001, bombing in Lisbon and London in 2004 and 2005, attacks on the metro in Brussels in 2016. Those incidents have pushed the legislators to implement extensive regulation in regard to transport security and a similar approach could be taken in regard to health and security connection.

In the context of COVID-19 contact tracing applications, similarities between the topics include the analogy between the EDPB Guidelines and those stemming from CJEU case law in the cases described above. Both recommend specification of purpose, limitation of the scope and establishing national authorities to effectively monitor the processing of data.

One difference is how the EDPC and the CJEU approach (in the different scenarios) the possibility to further process the data. The guidelines about the app fiercely propose creating an obligation to delete the data as soon as possible and not allow any further processing. On the other hand, in the La Quadrature du Net judgement only limitations on such processing are imposed; they include description of time, purpose and scope. Despite characterising processing of data outside of the GDPR regime, after careful review a picture of rules governing processing of data in times of danger appears and it strikingly resembles the general principles of processing of data described in the GDPR (lawfulness, fairness, transparency). The La Quadrature du Net judgement establishes an obligation for every result of automated analysis to be subject to "individual re-examination by non-automated means before an individual measure adversely affecting the persons concerned is adopted". While the fact that the product of the application can have no binding legal effect remains true, the British application has introduced a functionality of automatically signing up the person who is suspected to have been infected to a COVID test. This solution appears to balance right at the middle between the two dangers stemming from ill-designed systems, one being complete ineffectiveness and the second, granting too much power to an algorithm. Similarly, the applications used within the European Union, unlike in Asian countries, have no binding effect on the individual. Requiring such double confirmation would completely deny the very nature of all of the works in regard to creating and implementing contact-tracing applications, ie furthering the efficiency and time to make the process of identifying individuals whose health is in danger. Luckily it has not been imposed. However, it is important to note that the applications itself cannot produce a legally binding result and operates based on users consent (consent in this context is in regard to using the app, and not in regard to the legal basis of data processing).

5. Conclusions

The applications used for contact tracing during the pandemic have been an important measure of combating the spread of the pandemic and in most instances it has remained possible to not expose users to substantial risk in regard to their data. The data collected and processed has been of bigger scope than in the usual state of a democratic society but since "protection of public health is considered a legitimate aim' it is regarded

[43] ibid.

to allow for limitations of the right to privacy to be imposed for the time being[44]. As mentioned in the beginning, the similarities between exceptions for processing of data in case of criminal threats and public health threats appear to be sufficient to propose establishing that a comprehensive legislation of both would be a sensible solution.

A different problem that creating a pan-European regulation would facilitate to solve is that of a government of a Member State having far-from-pure intentions when it comes to gathering citizens data. The connection between backsliding into authoritarianism and increasing surveillance has already been academically discussed[45] but not within the operational framework of the pandemic. A comprehensive regulation on data protection in times of 'danger' on the European level would prevent such governments from creating their own rules, which could be harmful to the citizens. Moreover, pan-European proceeding in cases where data processing is of common interest across Member States remains an issue to be legally designed, as approaches and laws related to this topic differ between countries, however in some instances, especially where common European interest is demonstrated, a common solution could strengthen the protection of citizens rights[46].

[44] Van Kolfschooten, H, De Ruijter, A, '*COVID-19 and privacy in the European Union: A legal perspective on contact tracing*' (n 9)
[45] Rojszczak M, '*Electronic Surveillance in a Time of Democratic Crisis*' (2022) Verfassungsblog. Accessed on 27 April 2022, at https://verfassungsblog.de/os6-dem-crisis-pl/
[46] see: Bastos, F. B., & Pałka, P. (2023). Is centralised general data protection regulation enforcement a constitutional necessity? *European Constitutional Law Review*, 1–31. https://doi.org/10.1017/s1574019623000202