COVID-19 and privacy in the European Union: A legal perspective on contact tracing

van Kolfschooten, H.; de Ruijter, A.

DOI
10.1080/13523260.2020.1771509

Publication date
2020

Document Version
Final published version

Published in
Contemporary Security Policy

CONTEMPORARY SECURITY POLICY
2020, VOL. 41, NO. 3, 478–491
https://doi.org/10.1080/13523260.2020.1771509

Routledge
Taylor & Francis Group

COVID-19 and privacy in the European Union: A legal perspective on contact tracing

Hannah van Kolfschooten and Anniek de Ruijter

Amsterdam Law School, University of Amsterdam, Amsterdam, The Netherlands

ABSTRACT

When disease becomes a threat to security, the balance between the need to fight the disease and obligation to protect the rights of individuals often changes. The COVID-19 crisis shows that the need for surveillance poses challenges to the right of privacy. We focus on the European Union (EU), which has a strong data protection regime yet requires its member states to exchange personal data gathered through contact tracing. While public authorities may limit the right to privacy in case of public health threats, the EU provides little guidance when such limitations are proportionate. To define standards, we analyze existing EU case law regarding national security measures. We conclude that on the proportionality of contact tracing in the EU it is difficult to reconcile public health measures and individual rights, but guidance can be taken from understandings of proportionality in the context of security, particularly in the current COVID-19 emergency.

KEYWORDS COVID-19; privacy; health threats; health law; pandemics; health security

Information for early detection of health emergencies can save lives (World Health Organization, 2018). In the COVID-19 crisis, we see that national governments in the European Union (EU) turn to widespread surveillance and contact tracing in order to gather information on the spreading and risks of the virus. While these surveillance measures can focus on groups of people, contact tracing often directly affects individuals. In light of this difficult conundrum, the European Commission has published a toolbox for contact tracing and the interoperability between member states (Commission, 2020a, 2020b). In this guidance privacy is a key concern, including the use of contract tracing in a proportionate manner. Yet there is no guidance as to what proportionality might mean and how we should go about assessing this.

CONTACT Hannah van Kolfschooten h.b.vankolfschooten@uva.nl Amsterdam Law School, University of Amsterdam, Postbus 15859, Amsterdam, NJ 1001, The Netherlands

Contact tracing is the tracing of individuals and their contacts, who have been exposed to a pathogen that can cause a serious (cross-border) threat to health, and who are in danger of developing or have developed a disease. In the EU, member states are required to share information of these contact-tracing findings when it pertains to serious cross-border threats to health via an electronic information system: the Early Warning and Response System (EWRS). This may include personal data and health data for the purpose of contact tracing (Decision 1082/2013/EU, 2013; General Data Protection Regulation, Article 9). This cooperation on contact tracing between member states increases the impact on the right to data protection and exacerbates the risks for individual's right to privacy in case of the outbreak of a pandemic.

In serious EU cross-border threats to health, public authorities may limit individual freedoms to a large degree (Elbe, 2006; Hanrieder & Kreuder-Sonnen, 2014). In the COVID-19 crisis, we have seen that the interest of public health in many member states outweighs the protection of individual privacy. Even when the right to privacy is strongly protected in EU fundamental rights instruments as well as national constitutions (ECHR, Article 8; CFREU, Articles 7 and 8). Moreover, since 2018, the EU has the strictest data protection regime in the world under the General Data Protection Regulation (GDPR). However, as COVID-19 exemplifies, privacy is not an absolute right and can be limited under special circumstances, such as a health security threat (ECHR, Article 8(2); CFREU, Article 52).

In case a public health threat rises to the level of a threat to security, public health interventions start to resemble security interventions. The COVID-19 threat certainly enters this realm of threat. In this regard, an emerging trend is identified in the EU contexts of "securitizing" of public health, which leads to an integration of policies on public health and public security (Dijkstra & de Ruijter, 2017). Public health policy and national security policy have in common that they require the balancing of the rights of the public against the rights of the individual (Dijkstra & de Ruijter, 2017). Furthermore, often public health, like national security, can only effectively be protected when individuals sacrifice some of their freedom (Eckmanns et al., 2019; Sinha, 2013). In this regard, whether we like it or not, the character of the measure of contact tracing is strongly reminiscent of surveillance actions taken in light of national security issues: The privacy of individuals is limited for the purpose of the protection of a greater part of the population (van Kolfschooten, 2019).

Contact tracing of individuals across the EU in the context of COVID-19 therefore raises the question how privacy can be protected when a disease rises to the level of a threat to security? In 2013, the EU has been given a larger role in pandemic responses, as formalized in the Health Threats Decision (de Ruijter, 2017). As a consequence, contact tracing is now no longer a primarily

national issue responsibility as information is exchanged at EU level. In the COVID-19 crisis, the practice of exchanging personal (health) data between the member states for the purpose of contact tracing gains importance. However, in the field of EU health law there is only limited guidance as to how public health can be safeguarded in a proportional manner (Bastos & De Ruijter, 2019).

In this article, we analyze EU case law in the field of security to give us guidance as to determine proportionality of limitations on privacy in light of a public health threat. Proportionality in this regard implies that the measures–in this case contact tracing–do not go further than what is needed in light of the public policy aims. In the case of COVID-19 the aim of protecting public health has risen to a level of threat that it can also be seen as a risk to security (Fidler, 2016; Fidler & Gostin, 2007). However, important differences are also noteworthy and caution against a simple one to one comparison with security and public health. In the field of security policy makers are working often within a friend-enemy dichotomy, whereas in the field of public health the patient is seen as vulnerable and in need of assistance rather than as the enemy (Aldis, 2008; Collier & Lakoff, 2010, 2015).

In this article, we first critically examine the realignment of individual rights with public objectives in the context of *public health* as compared to *security policy* as observed in the literature. Secondly, we outline what the EU is currently doing, or capable of doing, in the field of contact tracing and how this can affect individual privacy as protected under EU law. In a last step we compare the current impact of contact tracing with the tracing and monitoring of suspected criminals threatening national security. This comparison can be used to inform proportionate limiting of the individual right to privacy in the context of health security and function as a benchmark for the protection of privacy in situations threatening security.

When public health threats become security issues

Security and public health policies are interconnected in certain instances. The World Economic Forum states that pandemics still pose one of the biggest threats to international security (Thomson, 2016). Pandemics weaken societies, political systems, economies, and can cause conflicts (Elbe, 2010). Vice versa, security threats also affect health. Biological and chemical warfare poses severe threats to public health (World Health Organization, 2003). Pandemics are more likely to occur in areas of civil war (Duff-Brown, 2017). In this line, an emerging policy practice at the EU level is identified, leading to increasing nexus of public health and security (Dijkstra & de Ruijter, 2017).

Indeed, over the past two decades, the EU's health emergency response has shifted from a "public health response model" toward a "preparedness model," building on the policy advice of security experts instead of solely health experts (de Ruijter, 2017). The 9/11 attacks in United States in 2001 and subsequent bio-terrorism with Anthrax put public health on the political agenda in the EU and was a strong driver for the securitization of EU public health (Greer et al., 2019). These attacks and the EU's lack of preparedness in the influenza A(H1N1) pandemic led to the adoption of decision 1082/2013/EU on serious cross-border threats to health in 2013. The main objective of this decision is to support cooperation and coordination between member states in the field of serious health threats (Decision No. 1082/2013/EU, article 1(2)).

The "Health Threats Decision" is a good example of the securitization of public health in the EU as it connects EU public health and security policy. It has a broad scope of application, taking an "all-hazards approach" by defining threats of biological origin (such as communicable diseases), threats of chemical origin, and threats of unknown origin all as "serious cross-border threats to health." The decision, in this regard, opens the door to bring communicable disease tools of contact tracing into the realm of security (Dijkstra & de Ruijter, 2017). Security and public health especially come together in the area of surveillance, such as border control and tracing of subjects (Purnhagen et al., 2020).

Using security tools such as critical infrastructure preparedness and other techniques for pandemic preparedness strategies may lead to greater capacities to deal with the effects of pandemics, based on the notion that "desperate times call for desperate measures" (Collier & Lakoff, 2008; Lo Yuk-ping & Thomas, 2010). However, reframing health as a security threat may have adverse effects for the protection of fundamental rights in health emergencies: The language of security can legitimate stricter measures by public authorities (Fidler, 2004; Upshur, 2005).

At the same time, public health policy and national security policy have in common that they often require the balancing of the rights of the public against the rights of the individual. Many public health measures require the constraining of individual rights and freedoms, such as the right to liberty and the right to privacy. This tension could become even more evident when public health is securitized, as the above legal instruments do. The "health security narrative" is then used by policymakers with the aim to justify extraordinary and limiting actions in response to health crises (Wenham, 2019).

The securitization of infectious diseases occasionally also leads to more involvement of state institutions such as the military and intelligence services. These institutions have more power to interfere with the individual's personal sphere (Elbe, 2006). Moreover, the securitization of health threats can lead to the declaration of the state of emergency or state of exception, allowing

governments and international institutions to take extraordinary measures which impact individual rights (Hanrieder & Kreuder-Sonnen, 2014). In sum, when a disease rises to the level of becoming a threat to security, security responses can sometimes impede on public health objectives and also change the balance between the need to fight the disease and protect the rights of patients, which makes it all the more important to provide guidance on the proportionality of these responses.

COVID-19: Contact tracing as a security measure

Contact tracing is a common measure to control infectious diseases. In the COVID-19 crisis, contact tracing also occupies an important position in the EU arsenal of measures. The aim is to identify and trace persons who have been exposed to the virus, and who are in danger of developing or have developed a disease (Decision 1082/2013/EU, Article 3(c)). Contact tracing is initially done by the member states (Decision 1082/2013/EU, Article 9). However, when member states notify an alert in reaction to a health emergency, they may be required to include personal data necessary for the purpose of contact tracing. That is, if this information (1) is available, (2) is in their possession, and (3) may be useful for coordinating the response (Decision 1082/2013/EU, Article 9(3)). Hence, the data that are collected in contact tracing are shared across the member states.

The personal data in question include travel information, but also information concerning health, such as information on the health status and the disease persons are possibly infected with (European Commission, 2017). Member states need to share the personal data via the electronic information sharing system EWRS (Decision 1082/2013/EU, Article 16). Sharing personal data may be useful for coordinating the response when the potentially infected person has traveled to another member state, or if the person has been in contact with persons staying in another member state (Dąbrowska-Kłosińska, 2017).

In the public health response to the COVID-19 crisis contact tracing plays an important role (World Health Organization, 2020b). In order to guide member states in the process of contact tracing, the ECDC has drawn up a document that outlines the key steps of contact tracing in the context of the COVID-19 response (ECDC, 2020a, 2020b). The ECDC defines a contact of a person infected with COVID-19 as "any person who has had contact with a COVID-19 case within a timeframe ranging from 48h before the onset of symptoms of the case to 14 days after the onset of symptoms." Confirmed COVID-19 patients are interviewed in order to identify their contacts. These contacts should be traced and phoned as soon as possible. Contact persons are then classified based on the level of exposure. For example, members of the patient's household and healthcare workers providing care

without protective equipment are considered close contacts with high-risk exposure. A fellow traveler in the train for less than 15min is classified as low-risk exposure.

The ECDC advises that high-risk exposure contacts are actively monitored by public health authorities and quarantined. Low-risk exposure contacts should self-monitor for symptoms and avoid close physical contact (ECDC, 2020a). As regards the means of contact tracing, member states can design their own strategies. However, the European Commission has issued a recommendation on a pan-European coordinated approach for the use of mobile applications (apps) for contact tracing (Commission Communication, 2020). There are currently multiple tracing apps in use in Europe. Privacy experts have repeatedly expressed concerns about the implications of these contact tracing apps for privacy of individuals in Europe.

Privacy limitations of contact tracing

In pandemics, the public health is to be balanced against the protection of individual rights. International human rights law considers health a human right: The highest attainable standard of health is a fundamental right of every human being (ICESCR, Article 12(1)). This imposes the legal obligation on governments to take steps to protect the health of the public, which includes the control of epidemic diseases. In order for the government to fulfill its duty to protect the right to health, it is sometimes necessary to restrict other individual rights and freedoms (CESCR, 2000). This means that under certain circumstances, the protection of public health conflicts with the protection of individual rights.

In the COVID-19 crisis, member states and the EU have indeed turned to freedom-limiting measures in the interest of the protection of public health. Some member states have even declared the state of emergency over the corona virus outbreak in order to adopt extraordinary measures and temporarily suspend specific individual rights with the aim of fighting the pandemic (Greene, n.d.). The processing and sharing of health data for the purpose of contact tracing limits the individual right to privacy of the persons involved: Member states process and share very sensitive data, without permission of the patient and on the basis of the sole suspicion of infection. The rights to privacy and health data are protected at the European level in the European Convention of Human Rights (*Z v. Finland*, 2010), the European Charter of Fundamental Rights (CFREU), and the General Data Protection Regulation (GDPR, Article 9).

The right to privacy is however not absolute; it can be limited when this is in accordance with the law, in the interest of a legitimate aim, necessary and proportional (ECHR, Article 8(2); CFREU, Article 52). Protection of public health is considered a legitimate aim and therefore legitimizes the limitation

of the right to privacy and protection of health data. Moreover, both the ECHR and the CFREU allow for derogation from fundamental rights in case of public emergencies "threatening the life of the nation" (ECHR, Article 15; CFREU, Article 52). The GDPR also provides for the possibility to derogate from the stricter data protection regime for health data in the event of serious cross-border threats to health (GDPR, Article 9(2)(h)).

Nonetheless, even in times of public health crises, limitations must meet the requirements of necessity and proportionality. Therefore, the question remains under what circumstances contact tracing is necessary and proportional in the case of public health emergencies such as the COVID-19 crisis. Member states may be required under the Health Threats Decision to share personal data necessary for the purpose of contact tracing. However, the Health Threats Decision offers limited guidance on proportionate implementation of the measure of contact tracing: the definition, aim and scope are unclear, it does not contain criteria to determine under what circumstances the sharing of health data is necessary and proportionate, it does not distinguish between different types of health threats and it does not specify how involved persons will be informed about the processing of their personal data (European Data Protection Supervisor, 2012).

The Health Threats Decision only provides for certain safeguards with regard to personal data protection in Article 16: Member states should take appropriate technical and organizational security measures, only share personal data through the selective communication channel with specified authorities and report incorrect processed personal data through the EWRS. Furthermore, personal data are automatically removed from the EWRS after twelve months (Dąbrowska-Kłosińska, 2017).

Whether contact tracing is proportionate to the health emergency at stake, therefore depends on the implementation on the national level by individual member states. This proportionality test basically comes down to the balancing of competing interests. In the case of contact tracing, these are on the one hand the right to privacy of the individual whose personal data is processed, and on the other hand the public interest of prevention and response to health threats. The positive obligations of the government with regard to the protection of public health are also relevant in this regard (*VO v. France*, 2004). Because of the limited guidance the Health Threats Decision offers in conducting this proportionality test and the lack of relevant case law, we offer to compare the current situation of tracing the contacts of COVID-19 patients with that of persons that are considered security threats.

How to draw the line on limiting the right to privacy

Contact tracing in the interest of combatting health threats shows relevant similarities to the tracing of individuals in the context of security policy.

The securitization of public health has introduced more enhanced surveillance techniques into infectious disease responses (Eckmanns et al., 2019). The Health Threats Decision is an example of this as it bridges the policy fields of health and security.

Given that the EWRS in the context of this Health Threats Decision creates an EU obligation to share data derived from contact tracing, EU case law regarding the protection of privacy and in the field of data protection and security is applicable to contact tracing (*Åklagaren v.Hans Åkerberg Fransson,* 2013). This includes the case law of the ECtHR for the EU institutions insofar as these cases correspond to similar rights in the CFREU and to the member states individually (CFREU, Article 52(3)). Hence this comparison can therefore provide guidance to the determination of proportionate implementation of contact tracing in context of health emergencies.

Security policy in practice teaches us that privacy limitations in the interest of security cannot take place at all costs. While the courts generally accept limitation of the individual's privacy in the interest of national security, limitations should be necessary and proportionate. Both the ECtHR and the CJEU have repeatedly ruled that measures limiting the right to privacy in the interest of national security were not proportionate to their aim. This is important guidance in the COVID-19 crisis, because many people seem to assume that "desperate times call for desperate measures" and allow for action beyond the scope of the law.

A proportionality review in this regard limits the possibility of public authorities in a number of ways. The ECtHR has expressed concern about inadequate safeguards for individual rights with regard to the collection of personal data by public authorities for the purpose of national security (*Rotaru v. Romania,* 2000). Here, the ECtHR has proposed several safeguards, such as specification of the categories of information to be collected, limitation of data processing to specific circumstances, maximum retention periods and an inspection procedure for data subjects. On maximum retention periods, the ECtHR stated that in the assessment of a proportional period, the nature of the personal data be taken into consideration (*Segerstedt-Wiberg and Others v. Sweden,* 2006). The CJEU clarified that retention periods should be established on the basis of objective criteria, and that a distinction should also be based on the usefulness of the data for its intended purpose (*Digital Rights Ireland*, 2014).

Furthermore, proportionality depends on the length of the privacy-limiting measure. The temporary character of contact tracing measures, especially ones with extensive impact on privacy such as contact tracing apps, is used as an argument in the proportionate balancing of individual rights and the public good. However, privacy experts are concerned that the extra technological possibilities created in the course of the COVID-19 pandemic will remain after the end of the pandemic, such as happened after the 9/11

attacks in the United States (Bloss, 2007; Levi & Wall, 2004; Sinha, 2013). Therefore, governments implementing contact tracing measures should ensure the temporary character of the measures in order for them to be proportionate to the aim.

Another aspect for assessing proportionality is transparency. Subjects of state surveillance should be informed about the surveillance afterwards. The CJEU has stated that failure to inform data subjects about the processing of their personal data increases the interference with privacy and data protection rights (*Digital Rights Ireland*, 2014). This also entails access to one's personal data, unless this entails an actual demonstrable threat to national security (*Dalea v. France*, 2010). Furthermore, the ECtHR held that not informing the subject of surveillance measures may only be proportional when the information affects the effectiveness of the measure for national security on the longer term (*Klass v. Germany,* 1978). Individuals should also be able to modify or delete their personal data. The ECtHR found the lack of provision for individuals to request the modification or deletion of stored personal data to be disproportionate in *Rotaru v. Romania (Rotaru v. Romania,* 2000). The CJEU also emphasized that the proportionality of the processing of personal data for the protection of national security may depend on the existence of appeals for data subjects to inspect, rectify or delete their personal data (*Schrems*, 2015).

Aforementioned case law may offer insights for proportionate tracing of individuals in health emergencies. Particularly also when it is possible that health information might become key as to people's reintegration into "normal society" after COVID-19. However, an important difference between the security case law and contact tracing is that the detection of persons in the context of national security is often less urgent, given that (potentially) infectious persons can cause a life-threatening epidemic in a short time. This may mean that, in contact tracing, the public interest outweighs individual rights. On the other hand, contact tracing processes health data more often, which is entitled to more protection than regular personal data. This can tip the balance to the other side.

For example, it follows from case law that member states must make the impact and duration of restrictive measures dependent on the magnitude of the risk. For contact tracing, this means that member states must specify under which circumstances they share which personal data via the EWRS, and with which authorities. This could include linking specific categories of personal data to the severity of the cross-border health threat, to be determined on the basis of the degree of infectivity, the severity of the health risks and the incubation period. Due to the major impact on privacy, health data could, for example, only be shared in the event of serious health threats. In addition, it should be laid down in which cases what authorities

receive the personal data, for example only if there is concrete evidence that the persons are located in those member states.

Furthermore, member states should inform data subjects about the processing of their personal data, unless this affects the effectiveness of the measure for its intended purpose. In the case of contact tracing, it is not obvious that informing data subjects is harmful to the protection of public health. Member states are therefore obliged to inform data subjects about the processing of their health data. The same applies to the possibility of access to their own personal data. This means that there must be procedures to enable data subjects to request rectification or deletion of their personal data. This must be done in consultation with the member states with which the health data is shared, so that the health data is corrected or deleted in both the EWRS and in the other member states.

Moreover, a general and undifferentiated retention period is not proportional. Although the decision sets a general maximum retention period of 12 months for personal data in the EWRS system, member states will have to make the retention period dependent on the nature of the data and the nature and timeliness of the health threat. This means that member states should distinguish between categories of data, for example travel data and health data, and make the retention period dependent on the specific health threat, for example, based on the incubation period. In addition, it follows from the Health Threats Decision and general data protection provisions that for proportional implementation of contact tracing, member states must also ensure that health data is not processed for purposes other than the specific health threat and is only shared through the selective communication channel of the EWRS. In addition, they must take appropriate technical and organizational security measures.

EU guidance on proportionate contact tracing

Contact tracing illustrates the complex tension between the individual's right to privacy and protection of public health. The measure is implemented by health authorities at the national level, but the actual balancing of interests between privacy and public health is also performed at the EU level. By including the obligation for member states to share health data for the purpose of contact tracing in the Health Threats Decision, the European Commission has implicitly decided that the protection of public health outweighs the importance of the right to privacy in case of serious cross-border threats to health. However, the decision on the degree of restriction of rights is left to the individual member states. The comparison with national security measures shows that health surveillance conducted in the event of serious cross-border threats to health, such as the COVID-19 crisis, does not legitimize a diminished standard of privacy protection for EU individuals.

Member states collecting and sharing health data for the purpose of contact tracing should ensure that the limitation of the right to privacy is proportionate to the aim of public health. However, in the case of novel infectious diseases, it is difficult for national health authorities to determine the proportionality of the measures. In other emergency situations such as national security threats, it is often easier to adjust individual freedom limiting measures to the nature and severity of the threat. In the context of the COVID-19 outbreak in Europe, shortage of testing kits, uncertainty about the timeline of the disease and possible vaccines, and other knowledge gaps may lead to uninformed decisions with regard to the need for the limitation of individual rights and freedoms via the implementation of measures such as contact tracing. Whether the individual right to privacy was disproportionately limited by national authorities may only be fully evaluated in retrospect.

Since contact tracing is usually performed under pressure of time, it may lack a deliberate and well-informed balancing of interests. In addition, the COVID-19 crisis shows us that the protection of the right to privacy might differ a great deal across member states. Therefore, the EU should further clarify the member states' responsibilities with regard to public health surveillance and contact tracing in the Health Threats Decision. Specific criteria for proportional implementation of contact tracing are not included in the latest two guidance's from the Commission (2020a, 2020b). Also, the GDPR guidance by the European Data Protection Board gives little guidance as to ensuring the proportionality of the limitation of the right to privacy in light of the implementation of contact tracing across Europe. The lack of clarity for this complex proportionality test hinders a consistent and high level of protection of individual fundamental rights in the EU.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by Nederlandse Organisatie voor Wetenschappelijk Onderzoek [grant number 451-17-019].

Notes on contributors

Hannah van Kolfschooten is a lecturer in International and European health law and Ph.D. researcher in the field of EU regulation of health artificial intelligence and patients' rights.

Anniek de Ruijter is Associate Professor of health law, focusing on global and European legal sources of health law at the Amsterdam Law School.

ORCID

Hannah van Kolfschooten http://orcid.org/0000-0002-3342-0285
Anniek de Ruijter http://orcid.org/0000-0002-6140-8988

Reference list

Aldis, W. (2008). Health security as a public health concept: A critical analysis. *Health Policy and Planning*, *23*(6), 369–375. https://doi.org/10.1093/heapol/czn030

Bastos, F. B., & de Ruijter, A. (2019). Break or bend in case of emergency? Rule of law and state of emergency in European public health administration. *European Journal of Risk Regulation*, *10*(4), 610–634. https://doi.org/10.1017/err.2019.71

Bloss, W. (2007). Escalating U.S. police surveillance after 9/11: An examination of causes and effects. *Surveillance & Society*, *4*(3). https://doi.org/10.24908/ss.v4i3.3448

Collier, S. J., & Lakoff, A. (2008). The vulnerability of vital systems: How "critical infrastructure" became a security problem. In M. D. Cavelty & K. S. Kristensen (Eds.), *Securing 'the Homeland': Critical infrastructure, risk and Securitisation* (pp. 40–62). Routledge. http://www.abebooks.com/Politics-Securing-Homeland-Critical-Infrastructure-Risk/1113744040/bd

Collier, S. J., & Lakoff, A. (2010). Health security, and new biological threats: Reconfigurations of expertise. In C. E. Bird, P. Conrad, A. M. Fremont, & S. Timmermans (Eds.), *Handbook of medical sociology* (6th ed, pp. 363–379). Vanderbilt University Press.

Collier, S. J., & Lakoff, A. (2015). Vital systems security: Reflexive biopolitics and the government of emergency. *Theory, Culture & Society*, *32*(2), 19–51. https://doi.org/10.1177/0263276413510050

Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01, Pub. L. No. OJ C 124I (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)

Dąbrowska-Kłosińska, P. (2017). Tracing individuals under the EU regime on serious, cross-border health threats: An appraisal of the system of personal data protection. *European Journal of Risk Regulation*, *8*(4), 700–722. https://doi.org/10.1017/err.2017.60

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 Text with EEA relevance, Pub. L. No. OJ L 293 1/15 (2013).

de Ruijter, A. (2017). Mixing EU security and public health in the health threats decision. In A. de Ruijter & M. Weimer (Eds.), *EU risk regulation, expert and executive power* (pp. 101–120). Hart Publishing.

Dijkstra, H., & de Ruijter, A. D. (2017). The health-security nexus and the European Union: Toward a research agenda. *European Journal of Risk Regulation*, *8*(4), 613–625. https://doi.org/10.1017/err.2017.34

Duff-Brown, B. (2017, October 17). *The collision of civil war and threat of global pandemics*. Stanford Health Policy. https://healthpolicy.fsi.stanford.edu/news/civil-wars-and-global-threat-pandemics

Eckmanns, T., Füller, H., & Roberts, S. L. (2019). Digital epidemiology and global health security; an interdisciplinary conversation. *Life Sciences, Society and Policy*, *15*(1), https://doi.org/10.1186/s40504-019-0091-8

Elbe, S. (2006). Should HIV/AIDS be securitized? The ethical dilemmas of linking HIV/AIDS and security. *International Studies Quarterly*, *50*(1), 119–144. https://doi.org/10.1111/j.1468-2478.2006.00395.x

Elbe, S. (2010). *Security and global health*. Polity Press.

European Centre for Disease Prevention and Control. (2020a). *Contact tracing: Public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update, 31 March 2020*. ECDC.

European Centre for Disease Prevention and Control. (2020b). *Resource estimation for contact tracing, quarantine and monitoring activities for COVID-19 cases in the EU/EEA*. https://www.ecdc.europa.eu/en/publications-data/resource-estimation-contact-tracing-quarantine-and-monitoring-activities-covid-19

European Commission. (2017). *(EU) 2017/1140 of 23 June 2017 on personal data that may be exchanged through the Early Warning and Response System (EWRS) established pursuant to Decision No 1082/2013/EU of the European Parliament and of the Council for the purposes of the coordination of contact tracing measures in relation to serious cross-border threats to health (notified under document C(2017) 4197) [2017] OJ L 164/65*.

European Commission. (2020a). eHealth Network Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States Version 1.0 (2020) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

European Commission. (2020b). eHealth Network, Interoperability guidelines for approved contact tracing mobile applications in the EU. https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

European Data Protection Supervisor. (2012). *Opinion of the European Data Protection Supervisor on the proposal for a decision of the European Parliament and of the Council on serious cross-border threats to health (2012/C 197/05)*.

Fidler, D. (2016). A pathology of public health securitism: Approaching pandemics as security threats. In A. Cooper (Ed.), *Governing global health: Challenge, response, innovation* (pp. 41–64). Routledge.

Fidler, D. P. (2004). Germs, governance, and global public health in the wake of SARS. *The Journal of Clinical Investigation*, *113*(6), 799–804. https://doi.org/10.1172/JCI21328

Fidler, D., & Gostin, L. (2007). *Biosecurity in the global age: Biological weapons, public health, and the rule of law*. Stanford University Press.

Greene, A. (n.d.). State of emergency: How different countries are invoking extra powers to stop the coronavirus. *The Conversation*. Retrieved April 10, 2020, from http://theconversation.com/state-of-emergency-how-different-countries-are-invoking-extra-powers-to-stop-the-coronavirus-134495

Greer, S. L., Fahy, N., Rozenblum, S., Jarman, H., Palm, W., Elliott, H. A., & Wismar, M. (2019). *Everything you always wanted to know about European Union health policies but were afraid to ask* (2nd ed.). World Health Organization.

Hanrieder, T., & Kreuder-Sonnen, C. (2014). WHO decides on the exception? Securitization and emergency governance in global health. *Security Dialogue*, *45*, 331–348. https://doi.org/10.1177/0967010614535833

Levi, M., & Wall, D. S. (2004). Technologies, security, and privacy in the post-9/11 European information society. *Journal of Law and Society*, *31*(2), 194–220. https://doi.org/10.1111/j.1467-6478.2004.00287.x

Lo Yuk-ping, C., & Thomas, N. (2010). How is health a security issue? Politics, responses and issues. *Health Policy and Planning*, *25*(6), 447–453. https://doi.org/10.1093/heapol/czq063

Purnhagen, K. P., de Ruijter, A., Flear, M. L., Hervey, T. K., & Herwig, A. (2020). More competences than you knew? The web of health competences for Union action in response to the COVID-19 outbreak. *European Journal of Risk Regulation*, 1–17. https://doi.org/10.1017/err.2020.35

Sinha, G. A. (2013). NSA surveillance since 9/11 and the human right to privacy. *Loyola Law Review*, *59*(4), 861–946.

Thomson, S. (2016). *This is one of the biggest threats to international security – and it's not what you think*. World Economic Forum. https://www.weforum.org/agenda/2016/02/this-is-one-of-the-biggest-threats-to-international-security-and-its-not-what-you-think/

UN Committee on Economic, Social and Cultural Rights (CESCR). (2000, August 11). *General comment No. 14: The right to the highest attainable standard of health (Art. 12 of the Covenant) (E/C.12/2000/4)*. https://digitallibrary.un.org/record/425041?ln=en

Upshur, R. E. G. (2005). Enhancing the legitimacy of public health response in pandemic influenza planning: Lessons from SARS. *The Yale Journal of Biology and Medicine*, *78*(5), 335–342.

van Kolfschooten, H. (2019). 'Contact tracing' versus privacy bij ernstige grensoverschrijdende gezondheidsbedreigingen. *Privacy & Informatie*, *2*, 43–48.

Wenham, C. (2019). The oversecuritization of global health: Changing the terms of debate. *International Affairs*, *95*(5), 1093–1110. https://doi.org/10.1093/ia/iiz170

World Health Organization. (2003). *Public health response to biological and chemical weapons*.

World Health Organization. (2018). *Managing epidemics: Key facts about major deadly diseases*.

World Health Organization. (2020b). *Coronavirus disease 2019 (COVID-19) Situation Report—72*. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200401-sitrep-72-covid-19.pdf?sfvrsn=3dd8971b_2