Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.04

Received: 12.01.2021
Accepted: 10.04.2021

Patrycja Dąbrowska-Kłosińska
Queen's University Belfast, Northern Ireland
p.dabrowska@qub.ac.uk
ORCID ID: https://orcid.org/0000–0002-3581–3226

Agnieszka Grzelak
Kozminski University in Warsaw, Poland
agrzelak@kozminski.edu.pl
ORCID ID: https://orcid.org/0000–0002-5867–8135

Agnieszka Nimark
Cornell University, United States of America
Barcelona Centre for International Affairs (CIDOB), Spain
an355@cornell.edu

The Use of Covid-19 Digital Applications and Unavoidable Threats to the Protection of Health Data and Privacy[1]

Abstract: This paper starts with a dilemma. How to ensure the adequate protection of individual health data and privacy in a global pandemic, which has intensified the use of digital applications for the purposes of data sharing and contact-tracing? There is no simple answer to this question when choosing between the protection of public health and individual privacy. However, the history of the existing case-law regarding infectious diseases control, both Polish and European, teaches about numerous examples in which health data and privacy were not adequately protected, but, on the contrary, were misused leading to human rights infringements. In light of this case law and public health ethics, this paper argues radically that the use of digital applications to fight the Covid-19 pandemic has not been sufficiently justified at least in the Polish context. Especially, unconvincing benefits from the use of these

1 This research was in part supported by the project THEMIS (2018–2021; Principal Investigator: Patrycja Dąbrowska-Kłosińska) of the EU Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No. 746014, which is hereby acknowledged.

© 2021 Patrycja Dąbrowska-Kłosińska et al., published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

tools do not outweigh the likelihood of human rights infringements with far-reaching consequences for political, social and economic rights now and in the future. In its novelty, this article combines a historical-legal method with the concept of public health ethics and a human rights-based approach and to foster further research and discussion. The text also responds to the pressing need to analyze those human rights issues embedded in the Polish reality.
Keywords: COVID-19, digital applications, European Court of Human Rights, fundamental rights, global health threats, health data protection, privacy, surveillance

Introduction

The Covid-19 pandemic has drawn urgent attention to the known legal and ethical dilemma of how to ensure the adequate protection of individual privacy in times of "mass surveillance" technologies and global health threats of infectious diseases which require data sharing and contact-tracing.[2] Answers to this dilemma and the practical feasibility of ensuring an adequate level of protection in case of sensitive health data, particularly prone to infringements and misuse, have been challenged by the development of modern technologies of big data algorithms and artificial intelligence[3]. These issues have already been highlighted by scholars in surveillance and security, human and constitutional rights and public health law studies[4].

Yet, shortly after the coronavirus outbreak, many governments began employing digital tools, especially individual mobile phone applications (so-called:

2 Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 3.8.2018, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx (accessed 28.04.2021), pp. 5–8ff. See also for example: N. Ram, D. Gray, Mass surveillance in the age of COVID-19, 'Journal of Law and the Biosciences' 2020, vol. 7, no. 1, p. 1–17 and the sources provided there.

3 S.L. Roberts, Big Data, Algorithmic Governmentality and the Regulation of Pandemic Risk, "European Journal of Risk Regulation" 2019, vol. 10, Issue 1, pp. 94–115; cf. W.K. Mariner, Reconsidering Constitutional Protection for Health Information Privacy, 'Journal of Constitutional Law' 2016, vol. 18, no. 3, pp. 975–1054, in the U.S. context.

4 In the Polish scholarship, see e.g. K. Chałubińska-Jentkiewicz, M. Nowikowska, Bezpieczeństwo, tożsamość, prywatność – aspekty prawne, Warsaw 2020; K. Łakomiec, Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia, Warsaw 2020; K. Świtała, Interoperacyjność i bezpieczeństwo danych medycznych w systemach e-zdrowia i telemedycynie, (in:) I. Lipowicz, M. Świerczyński and G. Szpor (eds.), Telemedycyna i e-Zdrowie. Prawo i informatyka, Warsaw 2019; M. Rojszczak, Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warsaw 2019; P. Dąbrowska-Kłosińska Stosowanie unijnych przepisów o transgranicznych zagrożeniach dla zdrowia, a ochrona danych osobowych w UE, „Przegląd Prawa i Administracji Acta Universitatis Wratislaviensis" 2016, vol. 107, pp. 53–81; A. Grzelak, Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości, Warsaw 2015; W.R. Wiewiórowski, Profilowanie osób na podstawie ogólnodostępnych danych, (in:) A. Mednis (ed.), Prywatność a ekonomia: ochrona danych osobowych w obrocie gospodarczym, Warsaw 2013.

"Apps"), to fight the pandemic by controlling the way people move, collecting information about infected people and people with whom the infected had contact, and serving as communication tools. Consequently, a pressing need has emerged to re-examine the use of these applications for public health protection in the context of individual privacy. Specifically, crucial questions concern the purposes which these digital applications or systems really serve and their effectiveness; their possible violation of individual privacy in the public dimension while protecting the collective right to health; the justification of limiting the right to privacy especially in light of the proportionality analysis; and, finally, the implications for other human rights.

The development and use of digital tools caused the world-wide reaction of various actors and stakeholders. To begin with, the response by policy authorities and civil society shall be mentioned. A considerable number of documents was issued by the international organizations concerned with the use of these tools, data transfers and human rights protection in the context of fighting the pandemic: EU institutions[5], the Council of Europe[6] and the OECD[7]. Both civil society and private actors also published reports to emphasize the complexity of the issue[8].

5 See e.g. 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, C/2020/2523 (O.J. C 124I, 17.4.2020), pp. 1–9; European Data Protection Supervisor (EDPS), EU Digital Solidarity: a call for a pan-European approach against the pandemic, 6.4.2020, https://edps.europa.eu/sites/edp/files/publication/2020–04-06_eu_digital_solidarity_covid19_en.pdf (accessed 28.4.2021); Joined statement on the right to data protection in the context of the COVID-19 pandemic by A. Pierucci and J.-P. Walter, 30.3.2020 https://rm.coe.int/covid19-joint-statement/16809e09f4 (accessed 28.4.2021); European Data Protection Board (EDPB), Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21.4.2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (accessed 28.4.2021); Fundamental Rights Agency (later: FRA), Coronavirus Pandemic in the EU – fundamental rights implications: with a focus on contact-tracing apps, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf (accessed 28.4.2021).

6 Protection of health-related data – Recommendation CM/Rec(2019)2 adopted by the Committee of Ministers of the Council of Europe, 27.3.2019.

7 OECD Policy Responses to Coronavirus (COVID-19), Ensuring data privacy as we battle COVID-19, 14.4.2020 http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19–36c2f31e/#section-d1e690 (accessed 28.4.2021).

8 Privacy leaders, https://iapp.org/resources/article/privacy-leaders-views-impact-of-covid19-on-privacy-priorities-practices-programs/ (accessed 28.4.2021); Deloitte Report, Privacy and Data Protection in the age of COVID-19, https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf (accessed 28.4.2021).

Next, the state of the art in the scholarship needs to be outlined. The *problematique* has been extensively explored by the academia[9]. The debate has been inter-disciplinary and thematically and territorially wide-ranging. The ethical analyses have mushroomed, including those which offer guidelines to be respected by policy-makers[10]. The legal studies examine the protection of health data privacy in times of Covid-19 contact-tracing generally[11] and digital applications specifically[12], and they warn of threats from authoritarian regimes not aligning to the rule of law[13]. Several common threads can be identified in these analyses, namely: (i) they investigate whether and how the protection of ethical principles and human rights can be ensured when using digital tools/applications to fight the pandemic; (ii) they scrutinize the existing guarantees of the right to privacy and data protection provided by the present European legal system and/or the scope of lawful limitations of those rights; and (iii) they generally accept that the protection of public health may justify the use of digital tools. Further, to understand the limitations of the right to data protection, this scholarship usually refers to the digital environment case law and/or to security threats-related case law[14], neither of which is directly health-related, which may imply different protection standards. In other words, while fearing possible infringements, the majority of legal studies focus on *de lege lata* and *de lege ferenda* arguments using the method of deduction to infer opinions about the present (the Covid-19 applications and the relevant

9 M. Kędzior, The right to data protection and the COVID-19 pandemic: the European approach, „ERA Forum" 2021, no. 21, pp. 533–543; W.R. Wiewiórowski, Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią, „Europejski Przegląd Sądowy" 2020, no. 6, pp. 20–33.

10 C. Pagliari, The ethics and value of contact tracing apps: International insights and implications for Scotland's COVID-19 response, "Journal of Global Health" 2020, vol. 10; F. Lucivero, N. Hallowell, S. Johnson , B. Prainsack, G. Samuel and T. Sharon, COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale, "Journal of Bioethical Inquiry" 2020, no. 17, pp. 835–839.

11 H. van Kolfschooten, A. de Ruijter, COVID-19 and privacy in the European Union: A legal perspective on contact tracing, "Contemporary Security Policy" 2020, vol. 41, Issue 3, pp. 478–491.

12 See A. Michałowicz, Stosowanie aplikacji mobilnych podczas pandemii COVID-19 z perspektywy ochrony danych osobowych, "Europejski Przegląd Sądowy" 2020, no. 6, pp. 34–42; L. Bradford, M. Aboy and K. Liddell K., COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes, "Journal of Law and the Biosciences" 2020, vol. 7, no. 1, pp. 1–33; P.H. O'Neill, T. Ryan-Mosley and B. Johnson, A flood of coronavirus apps are tracking us. Now it's time to keep track of them, "MIT Technology Review", 7 May 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker (accessed 28.4.2021).

13 M. Rojszczak Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego, „Acta Universitatis Wratislaviensis - Studia nad Autorytaryzmem i Totalitaryzmem" 2020, vol. 42, no. 2, pp. 207–243.

14 *Ibidem*; H. van Kolfschooten, A. de Ruijter, COVID-19, *op.cit.*

legal and practical framework) and make recommendations for the future (about their potential safe use).

We appreciate the importance of the above-mentioned studies. However, this article takes a different point of departure. In its novelty, it combines a historical-legal method with the concept of public health ethics and a human rights-based approach to argue that digital applications likely cause human rights infringements and that legal guarantees are often disregarded.

First, methodologically, we refer to the past to understand the present and offer some lessons for the future. We thus employ the historical-legal method to trace past violations and unconstitutionalities in the context of health data protection case-law where infectious diseases were at issue. We use the examples of judicial decisions that established protection standards to show that unconvincing benefits from the use of digital applications for public health protection do not outweigh the likelihood of rights violations with far reaching consequences. By doing so, we follow the approaches that advocate the inquiries about the past in legal analyses of the health and human rights field[15]. The human and constitutional rights framework applicable in Poland offers the normative orientation for the text (the Polish Constitution, the EU Charter for Fundamental Rights "CFR", and the European Convention for Human Rights "ECHR").

Second, we take the concepts of George Annas and Wendy Mariner on the need for application of public health ethics to control government actions in health. They admit that it is hard "to define a set of ethical principles unique to public health", and they claim to link human and constitutional rights, health law and (medical) ethics to implement values such as equality, justice and non-discrimination[16]. They emphasize that "public health is a social endeavor"[17] and thus must be assessed within social and democratic institutions where governments are obliged to respect, protect and fulfil human rights, which means adhering to the rule of law more generally. They highlight that the *methods* of reaching public health goals as such can be ethically controversial (and not the aim as such) and claim that governments should show (burden of proof) that their public health policy is justifiable and necessary.

Third, we accept that the right to health data protection may need to be lawfully limited to implement contact-tracing procedures and infectious diseases control measures to fight the pandemic. However, we question the justification of limitations,

15 G.J. Annas, Worst Case Bioethics, Oxford/New York 2011; T. Murphy, Health and Human Rights' Past: Patinating Law's Contribution, "Health and Human Rights Journal" 21 November 2019. Cf. also P. Alston, Does the past matter? On the origins of human rights, "Harvard Law Review" 2013, vol. 126, no. 7, pp. 2043–2081.

16 See G.J. Annas and W. K. Mariner, (Public) Health and Human Rights in Practice, "Journal of Health Politics, Policy and Law" 2016, vol. 41, no. 1, pp. 129–133 for the explanation of the possible conceptualisation of public health ethics.

17 *Ibidem*, p. 130.

including their proportionality in case of digital tools, while looking at the seriousness of possible immediate consequences for human rights, including political, social and economic rights, and the rule of law. We also argue that the value of protecting health privacy should be prioritized in pandemics, because the chronic emergency situations may encourage loosening the basic principles of data protection, which in turn may lead to the abuse of these data.

Finally, the above method, frames and approach allow us to argue *radically* that there has not been sufficient justification for the use of individual mobile phones digital applications for contact-tracing and quarantine control to fight the Covid-19 pandemic, at least, currently, in Poland. To present the argument, the text proceeds as follows: section 2 describes the digital applications used in Poland during the Covid-19 pandemic; section 3 presents the past case-law regarding the health data protection and privacy, its limitations and infringements; and section 4 contains an appraisal in light of public health ethics. The last section offers conclusions.

1. The Polish Covid-19 Applications and Privacy Threats in Comparative Perspective

A wide variety of applications have been in use during the Covid-19 pandemic, which can be divided broadly in three types: 1) contact–tracing applications that make users aware of the interaction with the virus; 2) self-assessment applications that inform users about Covid-19 risks, symptoms and steps to follow when they emerge; and 3) quarantine-enforcement applications that report on quarantined people. The following sections present analytically the applications used in Poland to combat Covid-19 against the comparative background of other European states to highlight doubts around their design, mode of use and legal framework constituting threats to privacy rights[18].

1.1. The contact-tracing application: ProteGO Safe

From a public health perspective, the contact-tracing applications seem most promising to help governments manage the spread of diseases and complement traditional, in-person, contact-tracing. They are designed to inform users of their contact with a person who tested positive for Covid-19 and to upload data on the phone, after which the system sends a notification to phones of those who have been

18 See also: Theme 3: Covid-19, privacy rights and cyber security risks, "Covid-19 Resources", Pinciples for Responsible Investment, 7.9.2020, https://www.unpri.org/covid-19-resources/theme-3-covid-19-privacy-rights-and-cyber-security-risks/6343.article (accessed 28.4.2021).

in close contact with the person[19]. The applications rely on various technologies to track and store users' locations: either Bluetooth- (proximity data) or network- and/or GPS-based[20]. Bluetooth-based contact-tracing applications are more common; individuals download an application that detects other smartphones' Bluetooth signals. These applications follow "a decentralized model" (with users' data produced and stored locally on their devices), which better protects personal data as compared to "centralized models" (where users' data are stored and processed on some central servers).

"Trace Together" was one of the first contact-tracing applications introduced in the world (Singapore)[21]. In the EU, the applications were either available (Austria, Bulgaria, Cyprus, Czech Republic, Lithuania, Spain, and Poland) or under development by the end of April 2020 in most states (including Belgium, Germany or Denmark)[22]. As analyzed by the Fundamental Rights Agency ("FRA"), the majority of these applications were Bluetooth-based and relied on "a decentralized approach" following the recommendations of the European Commission and the European Data Protection Board[23].

The Polish Ministry of Digital Affairs designed an application called STOP COVID –ProteGO Safe[24]. It was developed to track the location and health data of users, disseminate personalized guidance in case of contact with an infected person, transmit relevant information directly to the Chief Sanitary Inspector (data controller) and provide users with verified medical advice. The risk-assessment was supplemented with a self-diagnostic monitoring tool and a dedicated helpline[25]. The ProteGO thus combined contact-tracing and self-assessment (see below). The application used Bluetooth-based technology to record data on the proximity to other users with the application installed on their devices. As the use of the application was

19 For technical details see: E. Kusat Kaya, Safety and privacy in the time of covid-19: contact tracing applications, Centre of Economics and Foreign Policy Studies, https://www.jstor.org/stable/resrep26089?seq=1#metadata_info_tab_contents (accessed 28.4.2021).

20 Cf. Norwegian Infection Stop, 20 April 2020, Privacy International, https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps (accessed 28.4.2021).

21 In line with: eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States, 15.4.2020, p. 9, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf (accessed 28.4.2021).

22 FRA, Coronavirus pandemic, *op. cit.*, pp. 52–53.

23 EDPB, Guidelines 04/2020, *op. cit.*

24 Personal data is processed on the basis of Art. 6, Sec. 1, letters c) and e) GDPR in connection with the performance of a task in the public interest, resulting from Art. 1, 2, 3, 6 and 81, Sec. 1, 4 and 5 of the Act of 14 March 1985 on the State Sanitary Inspection (consolidated text Journal of Laws 2019, item 59). See Regulation (EU) No. 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 (O.J. L 119, 4.5.2016), p. 1 ("GDPR").

25 eHealth Network, Mobile, *op. cit.,* p. 10.

voluntary, only 1.9% of the Polish population downloaded the application between June-September 2020. That was one of the lowest take-up levels in Europe, which affected the effectiveness of the costly system[26]. ProteGO Safe was also criticized for flaws in privacy protection and functionality[27].

Following the claims that the system was not effective, the Ministry held a consultation with the number of the Polish non-governmental organizations (NGOs), appointed a ProteGO Safe expert team, and finally prepared and published a set of documents: a privacy policy, a risk analysis for personal data protection, a FAQ document and a security audit report. As a result, the NGOs' evaluation of the application was positive, in principle, regarding data protection safety and compliance with the principles of applications' good design[28]. The application neither monitors the location nor collects any redundant data; it ensures encryption of transmitted messages (keys) and anonymity, and it guarantees data security.

Notwithstanding these measures, the doubt about the possibility of health data misuse remains regarding the practical use of the application. We will return to the analysis of the measures in section 4 below.

1.2. Self-assessment applications

The second type of developed applications serves information providing and gathering purposes. People wishing to know more about Covid-19, possible treatment and their health can assess either prognoses about the likelihood of infection or information about the outbreak. They allow users voluntarily to upload their anonymized data and symptoms to help governments to map the spread of the disease. While these applications typically neither ask for individual, identifiable data nor transfer them to third parties, some of the applications still do.

These tools preceded the pandemic and were offered by private companies before[29]. However, during the pandemic, state governments became involved in using them. The health reporting applications and websites exist in many EU states[30]; likewise, the World Health Organization has been involved in developing an

26 B. Koschalka, Uptake of Covid contact tracing app under 2% in Poland, among the lowest rates in Europe, 11.9.2020, Notes from Poland, https://notesfrompoland.com/2020/09/11/uptake-of-covid-contact-tracing-app-under-2-in-poland-among-the-lowest-rates-in-europe/ (accessed 28.4.2021).

27 See: Coronavirus contact tracing reignites Polish privacy debate, 'Deutsche Welle', https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913 (accessed 28.4.2021).

28 A. Obem, ProteGO Safe: instalować czy nie?, 3.8.2020, https://panoptykon.org/czy-instalowac-protego-safe and links on this webpage (accessed 28.4.2021).

29 See for example in Canada: https://preworkscreen.com/ (accessed 28.4.2021).

30 Coronavirus Pandemic In The EU – Fundamental Rights Implications: With A Focus On Contact-Tracing Apps, 21 March – 30 April 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf, p. 53 (accessed 28.4.2021).

application that provides medically-approved information and advice to users based on their symptoms[31]. In some countries, the contact-tracing and self-assessment applications are developed together as a one integrated system (e.g., the ProteGO Safe).

1.3. The Kwarantanna domowa application

The third type of Covid-19 applications is comprised of tools that track people in quarantine to control their compliance with isolation orders. These applications are required to be used by visitors and travelers in some states[32], while in others[33], they have been used by public authorities to communicate Covid-19 information and quarantine guidelines and to prevent violations of self-quarantine orders.

Similarly, in Poland, the application Kwarantanna domowa (in English: "home quarantine") was introduced for the individuals subjected to mandatory house quarantine, after possible Covid-19 exposure, to control whether they respected the quarantine orders[34]. The application uses geo-location and face recognition technology and obliges concerned individuals to upload their location and photo for identity verification upon request by the police. The application collects the following data: citizen ID – technical identifier of the citizen, first name, surname, phone number, declared residence address, photo, location of the citizen and the end date of quarantine. Compliance is mandatory unless one declares: (i) non-subscription/non-use of the telecommunications network; (ii) non-possession of an adequate mobile device to install the software; or (iii) a visual impairment (blind or partially sighted)[35].

The Kwarantanna domowa raised concerns about the possible violation of users' rights to personal data protection. These concerns were raised by both public institutions and academia. First, the Polish Commissioner for Human Rights ("the Polish CHR") asked the President of the Office for Personal Data Protection and the Prime Minister for an opinion on the matter[36]. These governmental authorities

31 See: COVID-19 App, https://worldhealthorganization.github.io/app/ (accessed 28.4.2021).

32 E.g. Russia and Hong Kong, see: There's an app for that: Coronavirus apps, 20.4.2020, https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps (accessed 28.4.2021).

33 Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics, 23.4.2020, https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/ (accessed 23.4.2020) (The South Korean Self-quarantine Safety App).

34 J. Van Zeben and B.A. Kamphorst, Tracking and Nudging through Smartphone Apps: Public Health and Decisional Privacy in a European Health Union, "European Journal of Risk Regulation" 2020, vol. 11, Issue 4, p. 838.

35 Art. 7e of the Act of 2 March 2020 on special solutions related to the prevention, counteraction and combating of COVID-19, other infectious diseases and the crisis situations caused by them (consolidated text Journal of Laws 2020, item 1842).

36 Aplikacja „Kwarantanna domowa" budzi wątpliwości obywateli. Rzecznik pisze do premiera, 13.11.2020, https://www.rpo.gov.pl/pl/content/rpo-do-premiera-aplikacja-kwarantanna-domowa-

obviously declared that appropriate encryption methods had been used and that the data processing model complied with the requirements set out in the General Data Protection Regulation ("GDPR")[37]. Second, two specific allegations against the application's solutions from the perspective of data protection were enumerated in the scholarship[38]: (i) for unknown reasons, the data stored on centralized servers will be kept for 6 years, except for theoretically deleted images when the user deactivates the account, if a user does so; (ii) for unknown purposes, the number of actors granted access by law to the data processed in the application and the system is unjustifiably large, including the Police Forces Headquarters, the Provincial Police Headquarters, the voivodes (the governmental organs of regional administration), e-Health Center, the National Research Institute, as well as the third parties: companies Take Task S.A. and Tide Software Sp. z o.o. (entities that support the technical side of the application).

Before proceeding to a further assessment, the objective of the next section is to show the breadth of possible implications for individual human and constitutional rights of the health data access by public and private actors, including for legitimate purposes, and to claim that the sensitivity of the data and often the fear of disease both create an additional temptation for the misuse.

2. The Infringements of the Right to Health Data Protection and Privacy: Lessons from the European and Polish Case-law Histories

To begin with, several matters merit explanation.

First, we follow the approach of the courts, both the Polish Constitutional Tribunal (pre-2015, "CT") and the EU Court of Justice ("CJEU") and refer to both rights together: the right to respect for private (and family) life and the right to the protection of personal data[39]. Both rights are closely related, protect similar values (the autonomy and human dignity of individuals) and are quintessential for the exercise of other fundamental freedoms. Second, we treat the normative framework applicable to the protection of individual rights, within which the relevant case-law has developed, as a joint matrix of the Polish (the Constitution and laws) and European provisions (CFR and ECHR) with the GDPR (a directly applicable EU secondary law) as a key reference for data protection in the EU. Third, the subsequent

budzi-watpliwosci (accessed 28.4.2021).

37 MC zapewnia: aplikacja mobilna „Kwarantanna Domowa" zgodna z wymogami RODO, 30.11.2020, https://www.rpo.gov.pl/pl/content/mc-zapewnia-rpo-aplikacja-kwarantanna-domowa-zgodna-z-rodo (accessed 28.4.2021).

38 A. Michałowicz, Stosowanie, *op. cit.*, pp. 34–42.

39 Judgment of the Constitutional Tribunal of 18 December 2014, K 33/13, OTK-A 2014, no. 11, item 120, point 4.4; Judgment of the CJEU of 9 November 2010 on joined cases of Volker and Markus Schecke GbR and Hartmut Eifert v Land Hessen, C-92/09 and C-93/09, point 52.

sections depict the lessons from known infringements of the right to health privacy through the lens of case-law histories in judicial proceedings in both Polish and European courts. The text does not aspire to present a systematic history of the jurisprudence on judicial standards for personal health data protection. The cases were purposefully selected to show health data misuse in various contexts important for persons' lives: work environment, judicial proceedings, media and international mobility. Specifically, we wish to show how particularly damaging health data misuse can be for individuals concerned and their human rights in the social and economic context *notwithstanding* the extensive legal guarantees to ensure the protection of individual health data privacy and its value. This connects to the initial ethical dilemma of this text and the known history of human rights violations in the name of public interests, including public health (understood broadly). Lastly, the first part of the section explains the normative framework for the lawful limitation of health privacy rights.

2.1. The right to health data protection and privacy and their limitations

The following norms apply to possible limitations of the right to health privacy.

The Polish Constitution protects both the right to health privacy (Art. 47) and the right to the protection of health data (Art. 51)[40]. These rights can be lawfully limited in accordance with Art. 31(3) of the Constitution, which requires compliance with basic conditions of legality and proportionality *sensu largo*. That is, the restriction must be: (i) based on law; (ii) necessary in a democratic state for one of the enumerated purposes; and (iii) respectful of the core of rights, i.e., proportionality *sensu stricto*[41]. The public health is among the legitimate reasons for limitation, and it corresponds to the state obligation to prevent and combat epidemic diseases provided by Article 68 of the Constitution[42].

Further, the Constitution does not define "health data" explicitly[43], but a broad definition is included in the GDPR (Art. 4, point 15), which also states that personal "data concerning health" belong to the category of sensitive data the processing of which is prohibited generally unless specific exceptions apply (Art. 9(1) "special

40 Judgment of the Constitutional Court in the already mentioned case K 33/13 and of 19 February 2002 in case U 3/01.

41 P. Tuleja, Komentarz do art. 31 Konstytucji RP, (in:) P. Tuleja (ed.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warsaw 2020, p. 114–119; L. Garlicki and M. Zubik (eds.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Tom I, Warsaw 2016; M. Safjan and L. Bosek (eds.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Warsaw 2016.

42 T. Sroka, Ograniczenia praw i wolności konstytucyjnych oraz praw pacjenta w związku z wystąpieniem zagrożenia epidemicznego, 'Palestra' 2020, no. 6, pp. 75–98 and sources cited therein.

43 M. Florczak-Wątor, Komentarz do art. 51 Konstytucji, (in:) P. Tuleja (ed.), Konstytucja, *op. cit.*, pp. 178–179. See also generally M. Safjan and L. Bosek (eds.), Instytucje Prawa Medycznego. System Prawa Medycznego. Tom 1, Warsaw 2017.

category of data" and Article 9(2)(a-j) "exceptions")[44]. The relevant exceptions may, for example, concern an explicit consent of a person (a); or processing required for "establishment, exercise or defense of legal claims" (f); "for reasons of substantial public interest" (g); "the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee (…)" provided it is undertaken by professionals obliged to professional secrecy (h); "for reasons of public interest in the area of public health", for example, protecting against serious cross-border threats to health (i); and scientific and historical research and statistical purposes (j)[45]. Further conditions, including limitations, with regard to the processing of health data can be introduced by national law.

Certainly, the GDPR enumerated exceptions to health privacy need to be situated and interpreted against the national law systems. In Poland, for example, health data confidentiality is further regulated and protected through various acts. Accordingly, it can also be limited, for example, pursuant to the applicable health laws (in case of patients)[46] or civil and criminal judicial procedures' laws (in case of participants in proceedings)[47].

Further, we can relate the GDPR general prohibition of sensitive data processing to Article 51(2) of the Constitution, which establishes a prohibition of the Polish citizens' data processing by public authorities unless necessary in a democratic society. This requirement functions similarly to the proportionality principle, which brings us back to the point that the constitutionality/lawfulness of a health privacy limitation on the basis of any given exception will still need to meet the conditions of Article 31(3) of the Constitution (see above)[48], and, if the matter falls within the scope of the EU law, the CFR.

---

44 FRA and Council for Europe, Handbook on European Data Protection Law, Luxembourg 2018, pp. 42–45; and P. Dąbrowska-Kłosińska, 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" 2017, vol. 8, no. 4, pp. 707–710.

45 E.g., Commission Implementing Decision amending Implementing Decision (EU) 2017/253 as regards alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through Passenger Locator Forms, 25.03.2021, no ref. yet.

46 E.g., M. Wałachowska, Ochrona danych osobowych w prawie cywilnym i medycznym, Toruń 2008; M. Jackowski, Ochrona danych medycznych, Warsaw 2011.

47 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 (O.J. L 119, 4.5.2016). See also A. Grzelak (ed.), Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Warsaw 2019.

48 M. Florczak-Wątor, Komentarz, *op.cit.*, p. 179.

Accordingly, Articles 7 and 8 of the CFR constitute right to privacy and data protection respectively in the EU, and a lawful limitation of the rights needs to respect Article 52(1) CFR, including in the context of public health[49]. Consequently, every transfer of health information by a public authority may be justified only if: (i) it is "in accordance with the law"; (ii) it pursues an objective which is exhaustively listed; and (iii) it is "strictly necessary" and proportional to achieve that objective[50]. In addition, since the CJEU makes direct references to the European Court of Human Rights' ("ECtHR") privacy case-law while considering data protection issues, the limitations which may lawfully be imposed on the right to protection of health privacy in the EU correspond to those accepted under Article 8 ECHR (the right to respect for private and family life)[51], which also stems from Article 52(3) CFR[52].

To put it simply, every judicial review of a possible rights' violation will need to establish: (i) the occurrence of interference with health privacy either with or without justification (i.e., adequate legal basis, legitimate aim/exception); and (ii) the necessity and proportionality of the applicable exception to health data processing prohibition (e.g., public health surveillance, serious health threat, etc.). In the context of a given claim in question, the scope and content of judicial review will depend on a court considering which specific legal framework will be applied as a source of human rights protection (that is, whether it shall be a constitutional or ECtHR standard). The court will also decide on a primary point of departure for the interpretation and construction of the standard of review for its ruling, including, e.g., a proportionality assessment.

Let us now turn to the relevant judicial practice.

---

49 Cf. also Judgment of CJEU of 8 April 2014 on joined cases of Digital Rights Ireland and Seitlinger and Others, C-293/12 and C-594/12, point 238.

50 Cf. Judgment of CJEU of 20 May 2003 on joined cases of *Österreichischer* Rundfunk, C-465/00, C-138/01 and C-139/01, points 73–75. See also Judgment of CJEU of 16 December 2008 on the case of Huber v. Germany, C-524/06, point 68.

51 See also Judgment of ECtHR of 29 April 2014 on the case of L.H. v. Latvia, application no. 52019/07; Judgment of ECtHR of 16 February 2000 on the case of Amann v. Switzerland, application no. 27798/95; Judgment of ECtHR of 4 May 2000 on the case of Rotaru v. Romania, application no. 28341/95.

52 Judgment of CJEU of 9 October 2009 on joined cases of Volker and Markus Schecke, C-92/09 and C-93/09, points 51–52, 57, 89. See also P. De Hert and S. Gutwirth, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, (in:) S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection?, Dordrecht 2009, p. 3.

2.2. Lesson 1: The health data disclosure without consent and freedom of expression

The opening example comes from the ECtHR and concerns press publication of personal health data without consent and its questionable justification through the protection of the freedom of expression and public interest[53].

In January 2001, Lithuania's biggest daily newspaper published a front-page article about the exposure of residents in villages of remote Lithuania to fear of death and the AIDS threat[54]. The text provided the name, private life extensive details and the health status (seropositive and tuberculosis) of Ms. Biriuk. The accuracy of the information was confirmed by the medical staff of a local hospital. National courts found the breach of her privacy, but the damages awarded were derisory. Moreover, the Lithuanian Supreme Court indicated that the personal safety of people living in proximity to those sick with AIDS and dangers from persons whose behavior does not always meet moral standards need to be taken into account as valid arguments[55].

The ECtHR did not agree that "the purported concerns of the local population for their safety were legitimate, either socially or scientifically" and did not justify a publication about the applicant's state of health and her life style. It established a violation of Article 8 ECHR and raised damages awarded to the applicant. Further, the ECtHR emphasized the fact that medical staff's confirmation of the published health data particularly undermined societal trust in the medical profession, and observed that lack of patient confidentiality, especially in case of infectious diseases, affects negatively the willingness of people to HIV-test voluntarily and seek appropriate treatment. The disclosures of health data endanger both individuals concerned and the society at large. The ECtHR also indicated that the state obligation to safeguard medical privacy must be effective and that the allegations about someone's health and personal life cannot be justified by a legitimate public interest and facts-reporting necessary for a debate in a democratic society (Article 10 freedom of expression). The Court explained that disclosure of health data may dramatically affect an individual's private and family life, as well as the individual's social and employment situation[56].

This case is illustrative for several reasons. The societal fear of disease pressures public authorities, including the judiciary, to accept the publication of health data of potentially "dangerous individuals", especially in cases of infectious diseases for the sake of the alleged protection of "public safety interest". As a result, those authorities often follow a paternalistic path, and their behavior leads to stigmatization and

53 Judgment of CJEU of 6 November 2003 on the case of Bodil Lindqvist, C-101/01.

54 Judgment of ECtHR of 25 November 2008 on the case of Biriuk v. Lithuania, application no. 23373/03 and Judgment of ECtHR of 25 November 2008 on the case of Armonienė v. Lithuania, application no. 36919/02.

55 ECtHR case *Biriuk v. Lithuania*, *op. cit*., points 1–10.

56 *Ibidem*, points 34–47.

shaming of individuals, which adversely affects their social lives considerably. Further, it prompts them and others similarly situated to hide their health condition and functions counter-productively to public health protection. Media broadcasters are tempted to publish such information to scandalize and increase sales or to manipulate public opinion and instigate fears. Finally, the ruling also highlights the centrality of consent in health data processing.

The next sections analyze the relevant aspects in the EU and Polish case-law concerning employment relations. These cases demonstrate the breadth of human rights' implications for individuals when their health data are transferred and/or misused in the area of occupational medicine, the right to work and the right to access public service.

2.3. Lesson 2: The misuse of health data, occupational medicine and the right to work

Mr. X took part in a recruitment procedure at the European Commission[57]. During the process, a specific blood test was carried out by a medical officer to establish indirectly his immune deficiency (AIDS), because he had explicitly refused to undergo HIV-antibodies testing. The test was thus carried out and communicated to Mr. X's general practitioner without his consent. As a result, Mr. X was denied employment due to "physical unfitness".

While referring to Article 8 ECHR, the CJEU stated that the right to personal privacy includes keeping secret the state of one's health. It also held that the legitimate interest of institutions in verifying the fitness of future employees (general public interest) can be justified as such, but medical tests cannot be performed against the person's will. It precludes any test which could establish the existence of an illness concerned. An unconsented medical test infringes the very substance of the protected right and constitutes disproportionate and intolerable interference.[58]

The second important case for consideration is that of Ms. F and concerned the transfer, without her consent and knowledge, of her medical file (containing personal health data) between EU institutions for the purposes of a recruitment process[59]. The CJEU referred to Article 8 ECHR again to scrutinize the lawfulness of the interference based on the legitimate aim of pre-recruitment medical examination and emphasized that exceptions must be constructed narrowly out of respect for the principle of

57 Judgment of the Court of 5 October 1994 on the case of X v Commission of the European Communities, C-404/92 P.

58 *Ibidem,* points 1–8, 17–25.

59 Judgment of the Civil Service Tribunal of the 5 July 2011 on the case of V v. European Parliament, F-46/09, points 112–113.

proportionality. The CJEU also cited the ECtHR's restricted margin of appreciation applicable to "extremely intimate and sensitive nature of medical data"[60].

While establishing the violation of the right, the CJEU stated that the right to privacy governs not only a patient's privacy (relating to medical ethics), but also the confidence (trust) in the medical profession and in the health services in general. It underlined that the sole institutional interest does not justify transfer of health data without consent, especially of those stored for another purpose (different recruitment); and that the secret practice of inter-institutional transfer of health data was not acceptable[61].

Finally in a national, Polish case, an inappropriate medical certificate and misconduct by the administrative personnel (who communicated the health data to the company chief) allowed the employer to learn about Mr. P.S.'s seropositive status. It resulted in his immediate dismissal without any grounds. The claim concerned damages, and, in 2019, the Polish Regional Court adjudicated high compensation based on discrimination in employment of the person concerned[62].

The cases show vividly the co-relation between the infringement upon privacy rights, the right to work and discrimination in access to employment by public and private actors. Discriminatory recruitment and redundancies resulting from disease stigma often occur because of unlawful health data transfer, fear among co-employees, but also lack of medical knowledge and ignorance of the actual health condition of persons concerned[63]. The philosophy of automatic dismissal of those affected by a disease is unfortunately not limited to discriminatory treatment, but can also be provided by law. The next section depicts this issue.

2.4. Lesson 3: The use of health data and access to public service and employment

The Polish CT's judgment (2009) concerned the provisions that regulated the fitness of the candidates to the Polish police forces and the respective powers of medical committees[64]. The applicable law mandated an automatic classification of seropositive persons serving in the police to the category of persons "entirely

60 *Ibidem,* points 122–3, 131, referring to judgment of ECtHR of 25 February 1997 on the case of Z v Finland, application no. 22009/03.

61 Judgment of the Civil Service Tribunal of the 5 July 2011 on the case of V v. European Parliament, F-46/09, points 128–140.

62 Judgment of the District Court in Warsaw of 14 May 2019, XXI Pa 106/19, http://www.ptpa.org.pl/site/assets/files/1855/sygn__akt__xxi_pa_106_19.pdf (accessed 29.04.2021).

63 Judgment of the Supreme Court of 2 October 2012, II PK 82/12, OSNP 2013, no. 17–18, item 202; Judgment of ECtHR of 3 October 2013 on the case of I.B. v. Greece, application no. 552/10; Judgment of the EU Court of First Instance of 9 June 1994 on the case of X v. Commission, T-94/92.

64 Judgment of the Constitutional Tribunal of 23 November 2009, P 61/08, OTK 2009, no. 10A, item 150.

incapable of service" and automatic dismissal from work. There was no exception to this rule and no possibility of its disapplication.

After an exemplary analysis of the proportionality of the restriction of the right to access public service (Articles 60 and 31(3) of the Constitution), the CT found that the objectives of ensuring the good health of police personnel and the public health protection from disease, which realize the state duty to combat epidemics under Article 68(4) of the Constitution, do not justify the automatism and restrictiveness of the legislative solution considered. The CT indicated that the law should aim to protect both public health *and* the right to access public service. It stated that the contested regulation infringed upon human dignity and led to a "mechanical" exclusion of HIV-infected persons despite the psychophysical conditions (service suitability), a state of health of an asymptomatic person, and circumstance of infection, which may be caused by the service itself, undertaken in the social interest. The CT also recognized that the relation between the HIV-status and the right to work/public service is an important social problem (disease stigma) and that the disproportionality of contested rules could be counterproductive and, in fact, lead to hiding infections and increased health threats. It supported its arguments by referring to the EU and US case-law and to the UN guidance on HIV and human rights, which recommend that no mandatory testing be conducted in recruitment processes, that the stability of employment be guaranteed as long as a person is able to work, and that the protection ensure against discrimination and stigmatization in the workplace.

The next case of Mr. P.T. concerns disclosure of his HIV-status in a certificate exempting him from military service, the presentation of which was obligatory upon renewing the identity documents and in job applications. The ECtHR held that there had been a violation of Article 8 ECHR, finding that the disclosure of seropositive status in the certificate concerned had breached the privacy rights. It noted that the Moldovan Government had not specified which "legitimate aim" of limitation of Article 8 ECHR had been pursued by revealing the illness and including sensitive information about the applicant in the certificate, which could be requested in a variety of situations, and where the medical condition was of no relevance. The ECHR found that such a serious interference with the right was disproportionate[65].

The judgments show that inadequately and disproportionately implemented public health protection from contagious diseases can easily lead to unnecessary breaches of health confidentiality, the exclusion based on normative framework, and ultimately, discrimination based on health. Moreover, the fear of diseases and the temptation to exploit health data as a discriminating tool of exclusion and oppression appear also instructively in the histories of judicial proceedings where medical data

65 Judgment of ECtHR of 26 May 2020 on the case of P.T. v. the Republic of Moldova, application no. 1122/12. See also judgment of the Constitutional Tribunal of 19 June 2018, SK 19/17, OTK-A 2018, item 42.

were unnecessary disclosed during court trials with no connection to legal actions. Three cases illustrate the relevant matters.

2.5. Lesson 4: The disclosure of health data in judicial proceedings

In 1999, Mr. Panteleyenko faced criminal charges for alleged abuse of power and forgery of documents[66]. His office was searched as part of the investigation. During one of the proceedings, Mr. Panteleyenko denied having had mental health issues and produced a certificate from a psychiatric hospital supporting this assertion. The certificate was challenged, and the court requested his health records. As a result, his health record (explaining his treatment of mental illness) was provided by the hospital and read aloud at a public hearing.

The ECtHR found the violation of the applicant's right to privacy (Article 8 ECHR) due to the search of his office and the disclosure of his confidential health data in court, which was beyond what was necessary for the proceedings, as the information was not "important for an inquiry, pre-trial investigation or trial". The ECtHR explained that both the storing and use of information about an individual's private life by a public authority constitutes an interference with Article 8. Moreover, the ECtHR noted that the details at issue were irrelevant for the outcome of the litigation (i.e., establishing whether the alleged statement was made and assessing whether it was libelous) and that the domestic court's request for health information was redundant and unlawful according to the national law. This case highlights the problem of the disclosure and use of medical data that are ultimately irrelevant to a specific action.

A similar issue arose in the context of divorce proceedings of Mr. L.L. during which national courts used documents from his medical records without consent and any appointed medical expert[67]. The ECtHR again established a violation of Article 8 ECHR finding that the interference with the applicant's private life had not been justified in view of the fundamental importance of protecting personal data. It observed that the French courts had referred to the impugned medical report on a subsidiary basis to support their decisions, and, apparently, they could have reached the same conclusion without it.

Finally, in the case of Ms. Z, a Finnish national, the health data were included directly in the judgment[68]. Ms. Z and Mr. X (her husband) were both seropositive when X was convicted of rape. Ms. Z's confidential medical records disclosing her infection were seized by the prosecution and included in the investigation file without her prior consent. The City Court held the trial *in camera* and ordered the

66 Judgment of ECtHR of 29 June 2006 on the case of Panteleyenko v. Ukraine, application no. 11901/02.

67 Judgment of ECtHR of 10 October 2006 on the case of L.L. v. France, application no. 7508/02.

68 Judgment of the ECtHR of 25 February 1997 on the case of Z. v. Finland, application no. 22009/93.

ten-year confidentiality period of the case file, but Ms. Z's identity and health data (HIV-status) were published in the final judgment.

The ECtHR agreed that the seizure of the medical records in question and the orders requiring Ms. Z's medical advisers to give evidence in proceedings did not constitute a violation of Article 8 ECHR. However, the ECtHR noted that the national court was informed by X's lawyer about her confidentiality wishes and the lack of consent to the disclosure of information. Further, the ECtHR did not find any cogent reasons which would support the impugned publication of her health data in X's criminal conviction (irrespective of whether she had expressly requested the Court of Appeal not to disclose her identity and medical condition). Accordingly, the ECtHR established that the publication of the information concerned constituted the violation of the right to respect for private life under Article 8[69].

The above discussed cases help to demonstrate that health data processing and unjustified disclosure often take place against the individuals' will and may have irreversible adverse consequences. This kind of disclosure can happen notwithstanding appropriate procedural safeguards. The privacy breach is even more disturbing then, because individuals concerned have confidence that their rights will be respected.

Finally, discrimination based on health concerns both state citizens and foreigners. The ECtHR case-law shows the unequal treatment of migrants in the present context.

2.6. Lesson 5: The misuse of health data of and discrimination against migrants

Our last example concerns the Russian authorities' refusal to grant a residence permit to an Uzbek national because of a seropositive test, in response to which the ECtHR strongly condemned the stigmatization of people living with HIV[70]. Mr. Kiyutin challenged the decision as disruptive of his right to enjoy family life and disproportionate to the legitimate aim of public health protection. The ECtHR stated that the extremely intimate and sensitive nature of the information related to HIV-status calls for the most careful judicial scrutiny of any action taken by states, especially to communicate or disclose such information without consent. While eventually accepting that the impugned measure pursued the legitimate aim of protecting public health, it nevertheless established a violation of Article 14 (prohibition of discrimination) in conjunction with Article 8 ECHR. It also explained that health experts and international bodies recommend that any travel restrictions

69 See also A. Grzelak, Ochrona, *op. cit*., p. 111.

70 Judgment of ECtHR of 10 March 2011 on the case of Kiyutin v Russia, application no. 2700/10.

for seropositive persons cannot be justified by reference to public-health concerns[71]. In these migration cases, the ECtHR also acknowledged that the protection of personal data, including health information, is fundamentally important to the enjoyment of the right to respect for private life guaranteed by Article 8 and freedom from discrimination provided by Article 14 ECHR.

In sum, respect for health data confidentiality is a central aspect of personal privacy in the European human rights system and ought to constitute a vital principle in the legal systems of all members of the Council of Europe. It can be limited under the enumerated exceptions and strict conditions only[72].

Yet, the above-described jurisprudence also demonstrates that a high threshold of health data protection does not decrease the likelihood of disrespect of the existing protection guarantees and the resulting infringements of human rights. This legal-historical analysis serves as a crucial warning of the high temptation of all actors who have access to misuse health data, because health belongs to the most valuable and intimate aspect of human personality. The use of digital tools also prompts additional risks for health privacy[73]. Epidemics of infectious diseases also cause societal fear, which increases the probability of discrimination and stigmatizing practice. In such circumstances, overreactions are likely regardless of established laws.[74]

For these reasons, the regulation and use of Covid-19 applications require a very careful scrutiny of human rights arguments, rule of law principles, and ethical values (public health ethics) to verify whether their development and use can be justified in the aim of preventing disease spread (public health protection). We turn to these arguments in the next section.

3. Public Health Ethics and Covid-19 Digital Applications in Poland: Arguments Against

The analysis will now proceed to the examination of the regulation and exploitation of Covid-19 digital applications in the Polish context (section 2 above)

71 The ECtHR repeated these findings in the judgement of ECtHR of 15 March 2016 on the case of Novruk and others v. Russia, applications nos. 31039/11, 48511/11, 76810/12, 14618/13 and 13817/14.

72 Judgment of ECtHR of 17 January 2012 on the case of Varapnickaitė-Mažylienė v. Lithuania, application no. 20376/05, § 44.

73 Cf. also W.K. Mariner, Mission Creep: Public Health Surveillance and Medical Privacy, "Boston University Law Review" 2007, vol. 87, pp. 347–395, for the U.S. context.

74 See also W.K. Mariner, G.J. Annas and L.H. Glantz, Jacobson v Massachusetts: It's Not Your Great-Great-Grandfather's Public Health Law, "American Journal of Public Health" 2005, vol. 95, Issue 4, p. 587. Cf. C. McClain, Of Medicine, Race, and American law: The Bubonic Plague Outbreak of 1900, "Law and Social Inquiry" 1988, no. 13, pp. 447–513.

through the lens of public health ethics[75]. This lens prompts a closer look at the use of these applications *from the standpoint of three angles*: (i) the protection of human rights and other societal values; (ii) the respect for rule of law, including the focus on health and data protection laws; and (iii) the respect for some ethical principles. In this section, we present our arguments from these three perspectives and embedded in the current Polish reality.

3.1. The Human Rights-Based Arguments and Societal Values

Let us begin by considering the use of applications in Covid-19 prevention in Poland in light of the requirements of human and constitutional rights protection and the related threats of infringements.

First, the case-law histories regarding infectious diseases (see section 3, above) indicate that health data can be easily used without consent, transferred to other, public and private third parties, or misused in employment, administrative and judicial proceedings. Health data in the present context are prone to infringements, because they are predominantly sensitive, since they concern the lives of individuals endangered by a contagion. Further, the societal fear of Covid-19 infection can be simply amplified and lead to devastating social implications of discrimination and exclusion (e.g., children, migrants, and persons with disabilities). These phenomena also often target societal groups, who are already vulnerable, discriminated and/or excluded. As a result, "grey zones" of entire groups avoiding healthcare are likely to occur and lead to the counter-effectiveness of the measures.

Consequently, the protection of individual privacy *and* community public health interests requires recognition of two issues: (i) the vulnerability, caused by infection, of persons already experiencing a disease; and (ii) the devastating character of consequences of breaches of medical confidentiality, including stigmatization and the exposition to "*opprobrium and the risk of ostracism*"[76]. Otherwise, measures claimed to protect public health can become tools of oppression, which are counter-productive to public health protection[77]. It stems from the above-examined cases that courts often included the assessment of these issues in their proportionality analysis.

Second, respect for human (and constitutional) rights in the use of Covid-19 applications arguably requires inclusion of three related aspects of state obligations: respect of individual rights (e.g., privacy), protection from harm from external sources and third parties (standards including necessity and proportionality conditions), and

75 See fn. 15 above.

76 The ECtHR in cases Z v. Finland, *op.cit.*, points 95–96; Biriuk v. Lithuania, *op.cit*, point 36; and Judgment of ECtHR of 6 October 2009 on the case of C. C. v. Spain, application no. 1425/06, point 31.

77 W.E. Parmet, Dangerous Perspectives. The Perils of Individualizing Public Health Problems, "Journal of Legal Medicine" 2009, vol. 30, no. 1, pp. 83–108.

fulfilling the health needs of the population[78]. This means that any possible limitation of health data privacy in the use of digital applications must effectively ensure the high threshold of both constitutional and human rights protection standards (CFR and ECHR), including narrowly interpreted exceptions applied (from the national health law/GDPR) *and* the burden of proof justifying the usefulness of solutions in light of scientific and epidemiological evidence. In light of the analyzed judgments, it would require proving that data collected via Covid-19 applications actually help to reduce the spread of disease effectively; and, further, explaining if, why, and under what conditions, and on what legal basis, they will be used for other purposes (e.g., statistical and research purposes), especially as the latter does not necessarily contribute to the aim of public health protection from the disease.

Third, the protection of collective public health through the use of applications is not the sole value to be defended. The public health ethics approach requires a parallel protection of human dignity and human rights but also of the principles of equality and non-discrimination.[79] The lack of adequate protection of any of these values affects individuals in all their circumstances, including family, social and employment situations. For example, the violation of health privacy can influence the freedom of movement and family reunion, the right to work (freedom of choice of one's profession and place of work), the right to access public service, and other social security rights. Either the denial of employment or redundancy, based solely on an asymptomatic infection by contagious disease, is a frequent consequence of an access to personal medical data by an employer, leading to discrimination (and stigma) in the work environment.

Forth, "public health" is often employed as a "label" for measures the actual objectives of which are different and endanger human rights and privacy. It concerns, for example, state surveillance of health data for security reasons and/or unknown reasons, including storing of data for an unspecified time. The use of security phrasing in the context of health ("war to fight Covid-19") helps to justify such measures.[80] That is why the access by applications to individual health data may provide powerful and easy tools of manipulation of the freedoms of expression and of the press. It can also allow for the politicization of threats/risk assessments, which means using societal fear of the Covid-19 threat to govern, justify disproportionate restrictions of individual rights, and exercise political control over individuals by

78 Cf. G.J. Annas, W. K. Mariner, (Public) Health and Human Rights, *op. cit*, pp. 132–135.

79 See also M. Domańska, People with Disabilities as a Vulnerable Group. The Concept of Protection of the Rights of Vulnerable Groups, "Białostockie Studia Prawnicze" 2018, Vol. 4, no. 23, pp. 25–34.

80 See C. O'Manique and P. Fourie, Security and Health in the Twenty-First Century (in:) M.D. Cavelty and V. Maure (eds.), The Routledge Handbook of Security Studies, Abingdon/New York 2010. Cf. also A Lakoff, Two Regimes of Global Health, "Humanity" 2010, vol. 1, no. 1, pp. 59–79.

portraying them as societal dangers[81]. An "accidental" broadcasting by the state TV of the Covid-19-test information of a leader of public protests against restrictions of reproductive rights in Poland offers a recent relevant example[82]. The Polish CHR has initiated courts' review of the case[83]. Hence, any health data stored through Covid-19 applications could possibly be misused, in a similar way, as indirectly indicated by the case-law histories.

Finally, a state is obliged to ensure health data protection in both horizontal and vertical relations[84]. The access to users' data by private providers of applications' protocols (Google and Apple) create risk to health privacy, which is impossible to assess at the moment. However, it may suggest that the cost of infrastructure for data protection which would be required to exclude any such possibility questions the very rationality of the investment and development of such digital systems. The related arguments return in the next section.

3.2. The Rule of Law Arguments

The consideration of the use of Covid-19 applications in light of the modern and dynamic concept of the rule of law[85] prompts the following observations. They indicate that the development and use of Covid-19 applications might not meet some of the required conditions.

The rule of law requires the limitation of any arbitrary political power, assurance of legal certainty and predictability, and protection of individual and collective human rights from arbitrary actions of public authorities. It also demands that the legal system guarantee a set of standards (mandatory elements): generality, clarity and publicity of norms, no retrospective effect, feasibility, stability, consistency and compliance with the principle of proportionality[86]. When applying these standards to Covid-19 applications in Poland, several significant problems can be identified.

---

81 W.E.Parmet, Dangerous Perspectives, *op. cit*.

82 Marta Lempart on leading Poland's abortion rights protests, 'Financial Times', 02.12.2020, https://www.ft.com/content/b6012449–0c11–419a-b439–6e3320f47e86 (accessed 29.04.2021).

83 Disclosure of the test for SARS-CoV–2 by Marta Lempart – complaint of the Polish Ombudsman to the Provincial Administrative Court, 18.2.2021, https://www.rpo.gov.pl/pl/content/sprawa-ujawnienia-przez-panstwo-testu-na-sars-cov-2-marty-lempart-skarga-rpo-do-wsa (accessed 29.04.2021).

84 Judgment of the Constitutional Tribunal of 19 February 2002, U 3/01, OTK 2002 no. 1A, item 3, para. 1 in fine.

85 See recently: T. Drinóczi and A. Bień-Kacała (eds.), Rule of Law, Common Values, and Illiberal Constitutionalism. Poland and Hungary within the European Union, Abingdon/New York 2020; among the vast literature on the topic; and also W.K. Mariner, G.J. Annas and W. Parmet, Pandemic Preparedness; A Return to the Rule of Law, "Drexel Law Review" 2009, vol. 1, no. 2, pp. 341–382.

86 As there is no opportunity to explain the concept of the rule of law here, one should refer to the documents of international organizations, including the Council of Europe, (2011), The Rule Of Law, adopted by the Venice Commission (CDL-AD(2011)003rev) or the European Commission,

Firstly, the laws establishing Covid-19 applications are not embedded in the Polish health law system in a coherent way. Both applications STOP COVID – ProteGO Safe and Kwarantanna domowa were based on emergency laws enacted in response to the pandemic, which affected their quality, predictability and certainty (see section 2, above).

Moreover, the scrutiny of the Polish applications in use during the pandemic against the requirements of the GDPR general principles deepens the doubts. Michałowicz claims that the terms and conditions of use of the Kwarantanna domowa application and the privacy policy of the ProteGO Safe application are equally not free from textual errors and inconsistencies. They either omit some information required by law or contain contradictory information. For example, these documents indicate that the user may exercise the right to object to the processing of personal data pursuant to Article 21 GDPR, but the exercise of this right is not applicable, because data processing is not based on an appropriate legal basis (arguably, it would need to be Article 6(1), letters e) and f) GDPR)[87]. It can thus be claimed that, because of the health data's sensitive character and the purpose of the applications, data processing in both Covid-19 applications should include a reference to the GDPR's two specific legal bases: Article 6(1), letters e) and f) [88] *and* Article 9(1), letter i) jointly[89]. The next question also arises whether the implementation of the transparency principle – as required by the GDPR – is adequate (Article 5(1), letter a) GDPR).

In summary, the doubts regarding the assessment of Covid-19 applications in light of the GDPR requirements regard data collection's legal basis and purpose (unclear, predetermined purpose for collection; it should be limited to the aim of "protecting against serious cross-border threats to health"[90]); data collection

(2014) Communication from the Commission to the European Parliament and the Council. A new EU Framework to strengthen the Rule of Law (COM(2014) 158 final), as well as the relevant jurisprudence of the Court of Justice (including recent cases C-619/18 *Commission v. Poland* or joined cases C-585/18, C-624/18 and C-625/18 A.K.).

87 A. Michałowicz, Stosowanie, *op. cit.*, p. 37.

88 Article 6(1) letter e) refers to the legal requirement – situation when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 6(1) letter f) refers to a legitimate interest – situation when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

89 Article 9(1) letter i) refers to the situation when processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

90 Cf. Art. 9, Section 1, letter i, GDPR.

scope (some collected data are redundant and unnecessary to achieve the goal set for a specific tool); data collection outcomes (a number of entities authorized to access the data whose activities are not related to the pursued goal); personal data retention time in Kwarantanna domowa (the six-year period of data storing since the application's deactivation, hardly justifiable as a time-limit for civil claims[91]) and in ProteGO (imprecise period of data storing, its privacy policy indicates that data will be "*stored no longer than the use of ProteGO Safe, and not longer than required by law and no longer than necessary to achieve the purpose of processing*"[92]).

There is also some disparity between the applications' technical design (which was assessed positively for ProteGO) and their practical functioning. Theoretically, applications cannot collect the geolocation or physical proximity data of the user (via Bluetooth) when the user chooses information and symptom verification functions only, but the contact-tracing function remains available. Yet, Michałowicz argues that the website, from which ProteGO can be downloaded, requires detailed permissions, including access to device location, Bluetooth settings, and network connections. This indicates that the actual scope of personal data processed in the application may actually be wider than the one declared in the privacy policy[93].

Secondly, the lack of a truly independent control over the system of data processing in case of Covid-19 applications causes concerns. The data transfer to an external server (e.g., managed by the Polish Sanitary Inspectorate) can take place only in strictly defined and justified cases (e.g., a confirmed incident of infection). Yet, it cannot be excluded that the Covid-19 applications will lead to the creation of new databases stored on public administration servers or that the applicable law will be modified to change the destination of the already collected data. Such processes are not impossible because they would be in accordance with, for example, the privacy policy of the ProteGO Safe application. It thus seems in this context that the GDPR-based control by the relevant Polish authority (President of the Personal Data Protection Office) is not sufficient to meet the relevant ECHR standards on the control of access to data by certain governmental services[94].

This is arguable, especially in light of the past experience with the actions of public authorities in Poland. There were some alerting signals before the pandemic

91 A. Michałowicz, Stosowanie, *op. cit.*, p. 40.

92 § 3 pkt 10 ProteGO SafePrivacy Policy, https://www.gov.pl/attachment/092a389f-0a09–438f-9532-b04b8c205c7e (accessed 29.4.2021).

93 A. Michałowicz, Stosowanie, *op.cit.*, s. 39.

94 Cf. Judgment of ECtHR of 23 July 2009 on the case of Hachette Filipacchi Associates v. France, application No. 12268/03, where the ECtHR afforded a margin of appreciation to the state requiring adequate protection to individuals against the arbitrariness of the authorities by ensuring judicial control or other independent control system of measures interfering with the rights of an individual (see also Judgment of ECtHR of 7 March 2017 on the case of Polyakova and Others v. Russia, applications Nos 35090/09 et al.

that some serious shortcomings in the data processing systems in Poland already existed[95]. The fact that the government demonstrated openness to the societal control during the development of the ProteGO Safe application[96], but not with the second one (Kwarantanna domowa), may exactly indicate the change of approach.

The problem with the legal basis for the transfer of data by state authorities has also emerged in several specific situations. For example, in Poland in 2020, presidential elections were to be organized by postal ballots because of the pandemic. Despite the lack of legal acts regulating it, the Minister of Digital Affairs decided to transfer to Poczta Polska (the Polish Post, which was potentially responsible for sending election packages) the data of all citizens entitled to vote. The unlawfulness of the data transfer was confirmed by the Provincial Administrative Court[97]. Second, the governmental actions of pandemic management, based on the Prime Minister's orders solely[98] and the adoption of normative acts of a sub-statutory rank in place of law statutes[99], did not help to overcome the distrust of the digital measures. Given the doubts surrounding the applications against the GDPR requirements outlined above, it is therefore hard to trust and ascertain that the data collected via Covid-19 applications will be used solely for the purposes declared by the authorities.

Lastly, the requirement for the social acceptance of norms belongs to the rule of law conceptualization[100]. Thus, the consideration of three facts is needed in the present context: the high polarization of the Polish society; the overwhelming lack of trust in the government; and the conviction of part of the society that the authorities are moving towards an authoritarian regime[101]. It is not our goal to determine their actuality and extent, but such social beliefs may result in a very low level of acceptance of any solutions that rely on gathering information about society, which

95 Expert team of the Polish CHR, "Osiodłać pegaza" report, September 2019, https://www.rpo.gov.pl/pl/content/osodlac-pegaza-inwigilacja-propozycja-niezalezna-instytucje-do-nadzoru-sluzb-specjalnych (accessed 29.4.2021).

96 Report from the audits of the ProteGO Safe, https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport (accessed 29.4.2021). There is no such report in relation to "Kwarantanna domowa".

97 Judgment of the Provincial Administrative Court in Warsaw of 26 February 2021, IV SA / Wa 1817/20, Lex no. 3150569.

98 Koronawrius. Czy premier nakazał telekomom przekazywanie danych lokalizacyjnych osób chorych i w kwarantannie, 17.4.2020, https://www.rpo.gov.pl/pl/content/koronawrius-rpo-czy-premier-nakazal-przekazywanie-danych-lokalizacyjnych or Do rządu popłynął strumień danych o lokalizacji osób poddanych kwarantannie, 16.4.2020, https://www.rp.pl/Koronawirus-SARS-CoV–2/200419545-Do-rzadu-poplynal-strumien-danych-o-lokalizacji-osob-poddanych-kwarantannie.html (accessed 29.4.2021).

99 For example, the law ordering the wearing of masks was adopted only on October 28, 2020, prior to which this obligation resulted from the provisions of the Regulation of the Council of Ministers only.

100 See note 82 above.

101 W. Sadurski, Poland's Constitutional Breakdown, Oxford 2019.

clearly affects the utility of any such tools. This brings us to the ethical arguments against the applications.

3.3. The Ethical Arguments

Finally, reflecting on the ethical principles and the use of Covid-19 applications provokes several remarks.

The ethical scholarship usually emphasizes that the following principles need to be respected in the use of digital applications in response to the Covid-19 pandemic: autonomy, utility, voluntarism, and equality. The principle of autonomy requires prioritization of individual consent and the citizens' first approach in data protection. In light of the preceding analysis, it is not convincing that both Covid-19 applications respect these principles. Although, theoretically, all grounds of processing personal data are equal, this does not mean that they can be used freely, since different consequences are linked to various legal bases[102]. Imposing a legal basis in the form of a legal obligation would be an expression of the authority and would ignore the ethical aspect and the necessity to take into account the citizens' first approach. In this sense, consent should be a priority for data processing in situations such as those discussed in this text.

Next, the Polish applications can also be questioned from the perspective of the utility principle given the very low number of participants in the ProteGO Safe application, while, in case of Kwarantanna domowa, the relevant data are unknown (see section 2, above). The utility of the tools is doubtful, because usually at least a sixty percent uptake is needed for their effectiveness. Thus, the public usage of mobile applications depends not only on the perfection of technical solutions used in the development of such applications (or potential compatibility of measures with the human rights and constitutional standards, for that matter), but also on the level of social trust and acceptance of far-reaching digitalization to reduce the pandemic (reflected in the number of people using a specific application).

In addition, the Kwarantanna domowa application has not respected the ethical principle of voluntarism entirely. It seems to follow a paternalistic approach in heath law, which should instigate a broader debate that links (public health) ethics and law. Otherwise, the risk of an uncritical acceptance of solutions unjustifiably limiting individual rights increases.

Finally, although the vast majority of the population owns a smartphone, the actual realization of the equal access principle can be questioned. Many persons can encounter the problems with inadequate operation systems on their phones, which do not allow for the applications to be downloaded or encounter difficulties handling them (the elderly, people with disabilities).

102 W. Kotschy, Comment on Article 6, in: Ch. Kuner, L. A. Bygrave and Ch. Docksey (eds.), The EU General Data Protection Regulation (GDPR). A commentary, Oxford 2020, p. 339.

To sum up, in light of the three perspectives applied in this section to examine the design, use and regulation of Covid-19 applications in Poland, it is difficult to conclude that their regulation and use meet fully the requirements of public health ethics based on the protection of human rights, the respect for the rule of law and ethical principles.

Conclusions

This article scrutinizes the normative framework and use of Covid-19 digital applications in Poland and arrives at the conclusion that the implementation of these solutions has not been sufficiently justified. To determine this conclusion, we analytically examine the technical and legal features of the applications; explore the case-law history concerning the potential conflict between the protection of the right to health privacy and public health with the implications for diverse human/constitutional rights; and inspect the applications against the human rights-based standards, ethical principles and the rule of law arguments (the conceptualization of the public health ethics). The article questions the use of these digital tools as such amidst the doubts surrounding them, and, therefore, departs from the approach employed by many existent scholarly works offering analyses of lawful usage of public health surveillance technologies, including coronavirus applications, but usually not questioning the developed solutions[103].

It needs to be emphasized strongly that we do not question the necessity of contact-tracing measures employed by public health authorities during health emergencies/pandemics to identify sources of contagion, inform people about their possible exposure to infection, and impose quarantines to limit the spread of diseases and protect populations' health. The employment of the public health measures can then lead to limiting human/constitutional rights on the condition that at minimum they are lawful and proportionate. However, after scrutinizing the Covid-19 applications in the present text, we see no sufficient safeguards that promise that these conditions will be always fulfilled and individual human rights and data protection will be respected; that third parties will not misuse the data; that the government will actually fulfil its obligations to ensure that no violations occur; or that ethical principles will be followed. Accordingly, we argue that the *digital methods* employed to achieve public health goals must always be examined very carefully, because their justification in terms of a useful prevention of disease spread can likely be unsatisfactory.[104]

103 Cf. S. Sekalala, S. Dagron, L. Forman and B.M. Meier, Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis, "Health and Human Rights Journal" 2020, vol. 22, no. 2, pp. 7–20.

104 Cf. W.K. Mariner, Reconsidering Constitutional Protection, *op. cit.*, p. 1052.

We also think that the purely legal standpoint and analyses are not sufficient to adequately assess the justification of digital applications used for public health purposes. That is why, the application of the critical lens of public health ethics is helpful. It allows for the presentation of a broader picture from the wide-ranging perspectives and the development of a complete and coherent argument around the use of these applications in response to pandemics. In light of the applied lens, our extensive analysis of the Covid-19 applications developed in Poland prompts the recommendation that there is no convincing justification for their use in the present circumstances.

The number of actual threats to the protection of individual rights, including the health privacy, legal reservations and ethical doubts highlighting societal resistance, which *de facto* cannot be feasibly eliminated, do not convincingly outweigh any potential benefit from the use of the applications, at least in light of the analyzed examples. Finally, digital tools can be developed for public health protection, but the key question must always be asked critically: what is their justification?

REFERENCES

Alston P., Does the past matter? On the origins of human rights, "Harvard Law Review" 2013, vol. 126, no. 7.

Annas G.J. and Mariner W.K., (Public) Health and Human Rights in Practice, "Journal of Health Politics, Policy and Law" 2016, vol. 41, no. 1.

Annas G.J., Worst Case Bioethics, Oxford/New York 2011.

Aplikacja „Kwarantanna domowa" budzi wątpliwości obywateli. Rzecznik pisze do premiera, 13.11.2020, https://www.rpo.gov.pl/pl/content/rpo-do-premiera-aplikacja-kwarantanna-domowa-budzi-watpliwosci.

Bradford L. Aboy M. and Liddell K., COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes, "Journal of Law and the Biosciences" 2020, vol. 7, no. 1.

Chałubińska-Jentkiewicz K. and Nowikowska M., Bezpieczeństwo, tożsamość, prywatność – aspekty prawne, Warsaw 2020.

Commission Implementing Decision amending Implementing Decision (EU) 2017/253 as regards alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through Passenger Locator Forms, 25.03.2021, no ref. yet.

Communication from the Commission to the European Parliament and the Council. A new EU Framework to strengthen the Rule of Law (COM(2014) 158 final).

Coronavirus contact tracing reignites Polish privacy debate, "Deutsche Welle", https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913.

Coronavirus Pandemic In The EU – Fundamental Rights Implications: With A Focus On Contact-Tracing Apps, 21 March – 30 April 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf.

COVID-19 App, https://worldhealthorganization.github.io/app.

Dąbrowska-Kłosińska P., Stosowanie unijnych przepisów o transgranicznych zagrożeniach dla zdrowia, a ochrona danych osobowych w UE, „Przegląd Prawa i Administracji Acta Universitatis Wratislaviensis" 2016, vol. 107.

Dąbrowska-Kłosińska P., 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' 2017, vol. 8, no. 4.

De Hert P. and Gutwirth S., Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, (in:) S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection?, Dordrecht 2009.

Deloitte, Privacy and Data Protection in the age of COVID-19, https://www2.deloitte.com/content/dam/Deloitte/be/ Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf.

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 (O.J. L 119, 4.5.2016).

Disclosure of the test for SARS-CoV–2 by Marta Lempart – complaint of the Polish Ombudsman to the Provincial Administrative Court, 18 February 2021, https://www.rpo.gov.pl/pl/content/sprawa-ujawnienia-przez-panstwo-testu-na-sars-cov-2-marty-lempart-skarga-rpo-do-wsa.

Do rządu popłynął strumień danych o lokalizacji osób poddanych kwarantannie, 16.4.2020, https://www.rp.pl/Koronawirus-SARS-CoV–2/200419545-Do-rzadu-poplynal-strumien-danych-o-lokalizacji-osob-poddanych-kwarantannie.html.

Domańska M., People with Disabilities as a Vulnerable Group. The Concept of Protection of the Rights of Vulnerable Groups, "Białostockie Studia Prawnicze" 2018, vol. 4, no. 23.

Drinóczi T., Bień-Kacała A. (eds.), Rule of Law, Common Values, and Illiberal Constitutionalism. Poland and Hungarywithin the European Union, Abingdon/New York 2020.

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

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, C/2020/2523 (O.J. C 124I, 17.4.2020).

European Data Protection Board (EDPB), Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21.4.2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

European Data Protection Supervisor (EDPS), EU Digital Solidarity: a call for a pan-European approach against the pandemic, 06.4.2020, https://edps.europa.eu/sites/edp/files/publication/2020–04-06_eu_digital_solidarity_covid19_en.pdf.

Expert team of the Polish CHR, "Osiodłać pegaza" report, September 2019, https://www.rpo.gov.pl/pl/content/osodlac-pegaza-inwigilacja-propozycja-niezalezna-instytucje-do-nadzoru-sluzb-specjalnych (accessed 29.4.2021).

Florczak-Wątor M., Komentarz do art. 51 Konstytucji, (in:) P. Tuleja (ed.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warsaw 2020.

FRA and Council for Europe, Handbook on European Data Protection Law, Luxembourg 2018.

Fundamental Rights Agency, Coronavirus Pandemic in the EU – fundamental rights implications: with a focus on contact-tracing apps, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf.

Garlicki L. and Zubik M. (eds.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Tom I, Warsaw 2016.

Grzelak A. (ed.), Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Warsaw 2019.

Grzelak A., Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości, Warsaw 2015.

Jackowski M., Ochrona danych medycznych, Warsaw 2011.

Joined statement on the right to data protection in the context of the COVID-19 pandemic by A. Pierucci and J.-P. Walter, 30.3.2020 https://rm.coe.int/covid19-joint-statement/16809e09f4.

Kędzior M., The right to data protection and the COVID-19 pandemic: the European approach, 'ERA Forum' 2021, no. 21.

Koronawrius. Czy premier nakazał telekomom przekazywanie danych lokalizacyjnych osób chorych i w kwarantannie, 17.4.2020, https://www.rpo.gov.pl/pl/content/koronawrius-rpo-czy-premier-nakazal-przekazywanie-danych-lokalizacyjnych.

Koschalka B., Uptake of Covid contact tracing app under 2% in Poland, among the lowest rates in Europe, 11.9.2020, https://notesfrompoland.com/2020/09/11/uptake-of-covid-contact-tracing-app-under-2-in-poland-among-the-lowest-rates-in-europe.

Kotschy W., Comment on Article 6, (in:) Ch. Kuner, L.A. Bygrave and Ch. Docksey (eds.), The EU General Data Protection Regulation (GDPR). A commentary, Oxford 2020.

Kusat Kaya E., Safety and privacy in the time of covid-19: contact tracing applications, https://www.jstor.org/stable/resrep26089?seq=1#metadata_info_tab_contents.

Lakoff A., Two Regimes of Global Health, "Humanity" 2010, vol. 1, no. 1.

Łakomiec K., Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia, Warsaw 2020.

Lucivero F., Hallowell N., Johnson S., Prainsack B., Samuel G. and Sharon T., COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale, "Journal of Bioethical Inquiry" 2020, no. 17.

Mariner W.K., Annas G.J. and Glantz L.H., Jacobson v Massachusetts: It's Not Your Great-Great-Grandfather's Public Health Law, "American Journal of Public Health" 2005, vol. 95, Issue 4.

Mariner W.K., Annas G.J. and Parmet W., Pandemic Preparedness; A Return to the Rule of Law, "Drexel Law Review" 2009, vol. 1, no. 2.

Mariner W.K., Mission Creep: Public Health Surveillance and Medical Privacy, "Boston University Law Review" 2007, vol. 87.

Mariner W.K., Reconsidering Constitutional Protection for Health Information Privacy, "Journal of Constitutional Law" 2016, vol. 18, no. 3.

Marta Lempart on leading Poland's abortion rights protests, "Financial Times", 02.12.2020, https://www.ft.com/content/b6012449–0c11–419a-b439–6e3320f47e86.

MC zapewnia: aplikacja mobilna „Kwarantanna Domowa" - zgodna z wymogami RODO, 30.11.2020, https://www.rpo.gov.pl/pl/content/mc-zapewnia-rpo-aplikacja-kwarantanna-domowa-zgodna-z-rodo.

McClain C., Of Medicine, Race, and American law: The Bubonic Plague Outbreak of 1900, "Law and Social Inquiry" 1988, no. 13.

Michałowicz A., Stosowanie aplikacji mobilnych podczas pandemii COVID-19 z perspektywy ochrony danych osobowych, „Europejski Przegląd Sądowy" 2020, no. 6.

Murphy T., Health and Human Rights' Past: Patinating Law's Contribution, "Health and Human Rights Journal" 21 November 2019.

Norwegian Infection Stop, https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps.

O'Manique C. and Fourie P., Security and Health in the Twenty-First Century (in:) M.D. Cavelty and V. Maure (eds.), The Routledge Handbook of Security Studies, Abingdon/New York 2010.

O'Neill P.H., Ryan-Mosley T. and Johnson B., A flood of coronavirus apps are tracking us. Now it's time to keep track of them, "MIT Technology Review", 7 May 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker.

Obem A., ProteGO Safe: instalować czy nie?, 3.8.2020, https://panoptykon.org/czy-instalowac-protego-safe.

OECD Policy Responses to Coronavirus (COVID-19), Ensuring data privacy as we battle COVID-19, 14.4.2020 http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19–36c2f31e/#section-d1e690.

Pagliari C., The ethics and value of contact tracing apps: International insights and implications for Scotland's COVID-19 response, "Journal of Global Health" 2020, vol. 10.

Parmet W.E., Dangerous Perspectives. The Perils of Individualizing Public Health Problems, "Journal of Legal Medicine" 2009, vol. 30, no. 1.

Privacy leaders, https://iapp.org/resources/article/privacy-leaders-views-impact-of-covid19-on-privacy-priorities-practices-programs.

Protection of health-related data – Recommendation CM/Rec(2019)2 adopted by the Committee of Ministers of the Council of Europe, 27.3.2019.

Ram N. and Gray D., Mass surveillance in the age of COVID-19, "Journal of Law and the Biosciences" 2020, vol. 7, no. 1.

Regulation (EU) No. 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 (O.J. L 119, 4.5.2016).

Report from the audits of the ProteGO Safe, https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport.

Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 3.8.2018, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

Report on the rule of law - Adopted by the Venice Commission at its 86th plenary session, Venice, 25–26 March 2011.

Roberts S.L., Big Data, Algorithmic Governmentality and the Regulation of Pandemic Risk, "European Journal of Risk Regulation" 2019, vol. 10, Issue 1.

Rojszczak M., Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego, „Acta Universitatis Wratislaviensis - Studia nad Autorytaryzmem i Totalitaryzmem" 2020, vol. 42, no. 2.

Rojszczak M., Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warsaw 2019.

Sadurski W., Poland's Constitutional Breakdown, Oxford 2019.

Safjan M., Bosek L. (eds.), Instytucje Prawa Medycznego. System Prawa Medycznego. Tom 1, Warsaw 2017.

Safjan M., Bosek L. (eds.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Warsaw 2016.

Sekala S., Dagron S., Forman L., and Meier B.M., Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis, "Health and Human Rights Journal" 2020, vol. 22, no. 2.

Sroka T., Ograniczenia praw i wolności konstytucyjnych oraz praw pacjenta w związku z wystąpieniem zagrożenia epidemicznego, „Palestra" 2020, no. 6.

Świtała K., Interoperacyjność i bezpieczeństwo danych medycznych w systemach e-zdrowia i telemedycynie, (in:) I. Lipowicz, M. Świerczyński and G. Szpor (eds.), Telemedycyna i e-Zdrowie. Prawo i informatyka, Warsaw 2019.

Theme 3: Covid-19, privacy rights and cyber security risks, 'Covid-19 Resources', Pinciples for Responsible Investment, 7.9.2020, https://www.unpri.org/covid-19-resources/theme-3-covid-19-privacy-rights-and-cyber-security-risks/6343.article.

There's an app for that: Coronavirus apps, 20.4.2020, https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps.

Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics, 23.4.2020, OECD, https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636.

Tuleja P., Komentarz do art. 31 Konstytucji RP, (in:) P. Tuleja (ed.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warsaw 2020.

Van Kolfschooten H. and de Ruijter A., COVID-19 and privacy in the European Union: A legal perspective on contact tracing, "Contemporary Security Policy" 2020, vol. 41, Issue 3.

Van Zeben J. and Kamphorst B.A., Tracking and Nudging through Smartphone Apps: Public Health and Decisional Privacy in a European Health Union, "European Journal of Risk Regulation" 2020, vol. 11, Issue 4.

Wałachowska M., Ochrona danych osobowych w prawie cywilnym i medycznym, Toruń 2008.

Wiewiórowski W.R., Profilowanie osób na podstawie ogólnodostępnych danych, (in:) A. Mednis (ed.), Prywatność a ekonomia: ochrona danych osobowych w obrocie gospodarczym, Warsaw 2013.

Wiewiórowski W.R., Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią, „Europejski Przegląd Sądowy" 2020, no. 6.