Chapter 12
Data Protection Around the World:
Future Challenges

Elif Kiesow Cortez

Contents

12.1 An Overview of Future Challenges ............................................ 270
12.2 Automated Decision-Making and Artificial Intelligence ..................... 271
12.3 Face Recognition and Video Processing ......................................... 273
12.4 The COVID-19 Pandemic and Contact Tracing Apps ............................ 275
12.5 Upcoming Challenges ................................................................ 277
12.6 Concluding Remarks ................................................................... 277
References ...................................................................................... 278

Abstract As new technology becomes more integrated in daily tasks, new challenges to the right to the protection of personal data arise. GDPR aims to be technology neutral to make sure that the protection of the personal data does not depend on the techniques used in processing and is adoptable to the use of new technologies. This chapter will focus on European Data Protection Board guidelines and reports to highlight future GDPR compliance challenges to data protection and privacy in three prominent domains: (1) automated decision making, profiling and artificial intelligence, (2) face recognition technology and video processing, and (3) the newly emerged discussions on public health on the use of contact tracing apps with regards to the coronavirus pandemic and COVID-19. This chapter concludes by highlighting the importance of finding a balance between the right to protection of personal data without hindering the use and the development of innovative technologies in the EU.

Keywords Right to privacy · GDPR · Artificial intelligence · COVID-19 · Face recognition · Contact tracing · Corona apps

E. Kiesow Cortez (✉)
The Hague University of Applied Sciences, Johanna Westerdijkplein 75, 2521 EN The Hague, The Netherlands
e-mail: e.kiesowcortez@hhs.nl

© T.M.C. Asser Press and the authors 2021
E. Kiesow Cortez (ed.), Data Protection Around the World, Information Technology and Law Series 33, https://doi.org/10.1007/978-94-6265-407-5_12
12.1 An Overview of Future Challenges

Before the GDPR, within the EU, right to protection of personal data was legislated under the Data Protection Directive 95/46/EC of 1995. This legislation was a “directive” and not a “regulation” and therefore it required every EU member to transpose it into national legislation. This fragmented application of data protection rules therefore created problems both for the citizens and for the businesses willing to operate in or target their products and services to the EU market. For citizens, a fragmented approach might have led to unequal rights to the protection of personal data across member states. For companies, it meant that compliance was very costly due to the wide variation and need to track many different requirements.\(^1\) With the objective of creating a non-fragmented, uniform implementation of EU level data protection laws, the GDPR was adopted in 2016 after four years of strong negotiations.\(^2\)

The GDPR has been at the center of discussions regarding its extraterritorial applicability since it was in the draft stage.\(^3\) Research shows that at that point it was seen as controversial because it required any company, including international companies, that processes residents’ data to comply with the GDPR.\(^4\) The extraterritorial applicability might present as an effort to prevent data controllers from circumventing EU regulation by relocating to or contracting third parties from non-EU countries.\(^5\)

A communication by the European Commission reported that the GDPR was to create legislation in line with the EU Digital Single Market Strategy\(^6\) that would protect European citizens’ fundamental right to privacy. A European Commission survey from 2015 showed that 67% of the survey respondent EU citizens described themselves as concerned about having no control over the information they provide online as they did not know how this information could be used.\(^7\) A year after GDPR taking effect, in 2019, slightly less, 62%, indicated they were concerned about having partial or no control over the information they provide online.\(^8\) The same survey showed that some were trying to take control over their privacy settings, as 56% of social network users reported they had tried to change their default privacy settings on a social media platform.\(^9\) However, recent research shows that seemingly non-personal data variables such as location data or metadata based on the use of phone services can be used to extract personal data and that such attempts to control privacy provide little protection.\(^10\) Given such vulnerabilities, it is clear that new and emerging technologies pose a threat to individual privacy.

---

\(^1\) Albrecht 2016.

\(^2\) Voigt and von dem Bussche 2017.

\(^3\) Schwartz 2013.

\(^4\) Victor 2013.

\(^5\) Kuner 2010.

\(^6\) European Commission 2015a.

\(^7\) European Commission 2015b.

\(^8\) European Commission 2019.

\(^9\) Ibid.

\(^10\) Schneier 2015; Acquisti et al. 2016.
Recital 15 of the GDPR states that the regulation should be “technology neutral”\(^{11}\) to make sure that the protection of the personal data does not depend on the techniques used in processing. Therefore the European Commission and the European Data Protection Board (EDPB) regularly issue guidelines on how the GDPR applies to new and emerging technologies. In this chapter, we will focus on EU-level guidelines and reports on future challenges to data protection and privacy in three prominent domains: (1) automated decision making, profiling and artificial intelligence, (2) face recognition technology and video processing, and (3) the newly emerged discussions on public health with regards to the coronavirus pandemic and contact tracing apps.

### 12.2 Automated Decision-Making and Artificial Intelligence

Working Party 29 was established by Directive 95/46/EC\(^ {12}\) and was replaced by the EDPB to ensure the consistent application of the GDPR.\(^ {13}\) Working Party 29 adopted the latest version of the guidelines on automated decision making and profiling regarding GDPR in February 2018.\(^ {14}\) The EDPB endorsed these guidelines (hereinafter, the WP29 guidelines) during its first plenary meeting in 2018.\(^ {15}\) The guidelines explain that automated decision making brings about many advantages as it increases the accuracy of predictions as well as many risks regarding profiling given that individuals might end up being forced into existing profiles about themselves, which can lead to social segregation.\(^ {16}\)

Article 4.4 of the GDPR defines profiling as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.” The WP29 Guidelines break this down to the following key aspects: profiling consists of personal data processed through an automated manner with the aim of evaluating personal aspects of the data subject.\(^ {17}\) Individual’s right not to be subject to a decision based solely on

---

\(^{11}\) For an in-depth discussion on technology neutral law, see Hildebrandt and Tielemans 2013.

\(^{12}\) EU Directive 95/46: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

\(^{13}\) EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

\(^{14}\) Article 29 Data Protection Working Party 2018.

\(^{15}\) EDPB 2018.

\(^{16}\) Article 29 Data Protection Working Party 2018.

\(^{17}\) Ibid.
automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her is codified in Article 22 of the GDPR.

Data subjects are often unaware of the amount and the type of information collected about them as well as about how this information can be connected via artificial intelligence technologies to infer their characteristics. The key risk of this type of profiling is that users have no knowledge of or control over their categorization or how interconnected systems treat them based on this categorization.

The WP 29 Guidelines make a distinction between activities that are solely based on automated decision making and those that are based on profiling. By way of illustration, the guidelines explain that speed cameras on highways, which impose fines based on license plates, perform automated decision making but not profiling. But if these cameras were to monitor drivers’ behaviors and habits over time and the amount of fine was decided based on repeat of an offense or in light of other collected data about the individual, that would include profiling.

Artificial intelligence also presents a distinct challenge as an advanced form of automated decision making which facilitates profiling based on seemingly insignificant data. Article 9 and Recital 51 of the GDPR indicate that sexual orientation and ethnic origin are sensitive personal data. Kosinski et al. found that combining a list of things a Facebook user has liked with very limited information could be used to predict sexual orientation of the user with 88% accuracy and his or her ethnic origin with 95% accuracy. This study took place in 2013, and as artificial intelligence and data analytics continue to develop, accuracy as well as the range of extractable sensitive information may increase.

As the WP29 Guidelines refer to the fact that profiling can lead to social segregation, it is important to notice that data subjects’ profiles are interconnected and this might lead to targeting the data subject with the same personalized advertising and even information on different platforms. Research shows individuals may gain excessive confidence in their points of view because of such targeting of information and that this can lead to extremism and polarization in societies. Future research on data protection and privacy should focus on possible solutions to this problem.

---

18 For a discussion on informational identity, see Floridi 2011.
19 Ibid.
20 Article 29 Data Protection Working Party 2018.
21 For suggestions on how legislation should be combined with technology design, see Hildebrandt 2008.
22 Kosinski et al. 2013.
23 For a thorough discussion on these risks, see Sunstein 2001.
24 See Helberger et al. 2018 for a detailed analysis of diversity-sensitive design.
12.3 Face Recognition and Video Processing

The EDPB adopted guidelines on processing of personal data through video devices on 29 January 2020. Thus, guidelines issued by the EDPB can be examined for insights on GDPR compliant practices in processing of personal data through video devices.

Scholarly discussions in personal data protection gave special attention to processing of facial recognition data collected through video devices. Under the GDPR, personal data refers to any information relating to an identified or identifiable natural person. The guidelines highlight that the frequent use of systematic automated monitoring of areas by audio-visual means increases the possibility of identifying the data subjects that use the monitored areas.

In the guidelines, the EDPB first defines the scope of applicability of the GDPR by demonstrating possible scenarios. For example, it states that a person using a personal device or an action camera attached to sports equipment to record activities when on holiday might be protected under the household exemption of the GDPR Article 2(2) (c) even if third parties have been recorded in the background. However, there is specific emphasis that the exemption applies to cases where the recording is shown to friends and family. The guidelines refer to a 2003 decision of the European Court of Justice and states that uploading the video on the internet and making the data available “to an indefinite number of people” does not benefit from household exemption.

Purpose specification is one of the principles of personal data processing under the GDPR Article 5(b). Regarding processing of personal data through surveillance cameras, the EDPB asserts that the purpose of the monitoring should be specified and documented for each surveillance camera. The guidelines also explain that “video surveillance for safety” on its own would not be seen as a sufficiently specific purpose. On the other hand, they state that, according to Article 6(1) (c), where national law requires video surveillance doing so cannot be a violation of the guidelines.

The guidelines describe when a shop owner could install a video surveillance system assuming no national law demands this action and therefore the shop owner would like to use the “legitimate interest” ground under the GDPR Article 6(1) (f) as the legal basis for posting the camera. To establish a legitimate interest in installing the system to avoid vandalism, the shop owner must prove that statistics show that vandalism is an actual threat in the relevant neighborhood; a general threat in the nation of vandalism does not suffice. The guidelines do say that banks and jewelers do not necessarily have to supply neighborhood-specific risk justification to post a camera.

25Ringrose 2019.
26EDPB 2020, p. 7.
27European Court of Justice, Judgment in Case C-101/01, Bodil Lindqvist case, 6 November 2003, para 47.
28EDPB 2020, pp. 9–10.
The guidelines state data controllers must balance the interests and fundamental rights of the data subjects and their legitimate interests. The EDPB list some of the balancing factors as the size of the area that is under video surveillance, the type of information that is gathered, and the number of data subjects. According to Recital 47 of the GDPR, when data subjects do not reasonably expect their data are being processed, it is likely that the interests and fundamental rights of the data subject would override the interests of the data controller.

The guidelines emphasize that data subjects can reasonably expect that they are monitored by video surveillance at a bank or ATM but not, for example, in their private garden, in fitness facilities, or in publicly accessible areas dedicated to regeneration or leisure. The EDPB guidelines also state that signs that inform the data subjects of video surveillance are not relevant in objectively assessing reasonable expectations of privacy. Thus, posting a sign saying the area is under video surveillance does not override an individual’s reasonable expectation of privacy.

Consent is one of the legal bases for processing an individual’s personal data. This might pose problems for entities that want to conduct video surveillance, given the challenges of collecting consent from every data subject who enters the area. Simply entering a marked area would not constitute valid consent on its own unless it is compliant with the criteria of Article 4 and 7.

GDPR Article 9 and the EDPB guidelines provide somewhat contradictory information about the possibility that video surveillance produces health data. According to GDPR Article 9, revealing that a person is using a wheelchair could be seen as health data and therefore fall under special categories of data (sensitive data). However, the EDPB guidelines state that video footage showing health circumstances are not always considered to be sensitive data. While a hospital monitoring a patient’s health condition through video camera would constitute processing of sensitive data, video footage showing that someone uses a wheelchair is not per se processing of sensitive data. The guidelines liken intentional monitoring of a patient’s health to using video surveillance to detect someone’s political opinions, such as union organizing.

The guidelines provide other examples to clarify restrictions. For example, they state that for a hotel to use video surveillance to identify automatically if a VIP guest has entered the property they would have to get explicit consent of every guest in order to scan their faces. However, the EDPB indicates that if a shop is scanning customers only to detect their gender and age, without generating biometric templates of individuals, no affirmative consent is required as this does not constitute sensitive personal data.

EDPB guidelines on processing of personal data through video devices provide several examples on ensuring GDPR compliance with data processing principles and with data subjects’ rights regarding the use of video devices. In so doing they indicate that additional measures and restrictions might become applicable in the short run for video surveillance practices. Some new measures suggested in the guidelines include a requirement for informative signs on video surveillance that communicate data subjects’ rights and the data’s retention period as a condition of video surveillance. The guidelines also include a list of organizational and technical measures to assist
GDPR compliance. As law enforcement\textsuperscript{29} and targeted advertising\textsuperscript{30} increasing use face recognition technologies, the guidelines would serve to achieve a more uniform approach on processing of personal data through video devices within the EU.

### 12.4 The COVID-19 Pandemic and Contact Tracing Apps

During the first months of 2020, the coronavirus pandemic became a prominent topic in scholarly discussions about privacy and the right to protection of personal data. One of the main discussion points was contact tracing apps (also known as corona apps) that countries such as South Korea had adopted.\textsuperscript{31} In order to provide EU-level guidance to the discussion, the EDPB issued two guidelines regarding COVID-19 and privacy. The first guideline, on 21 April 2020, focuses on the processing of data for the purpose of scientific research in the context of the COVID-19 outbreak\textsuperscript{32} and the second guideline concerns the use of location data and contact tracing tools in the context of the COVID-19 outbreak.\textsuperscript{33}

This section will only focus on the second guideline regarding the contact tracing tools. The relevant EDPB guidelines refer to the fact that GDPR was designed as technology neutral and that the regulation is flexible enough to apply in the exceptional situation of the current COVID-19 outbreak. The guidelines underline that uses of individuals’ data should empower individuals and should be protected from any use that can stigmatize the data subjects. The guidelines highlight that contract tracing apps should be used to gather location data that would enable the experts to better predict the spread of the virus and the apps can also be used to notify the individuals who have been in close contact with an infected individual. The EDPB explains in these guidelines that the effectiveness of the contact tracing tools would depend on several factors such as the percentage of the citizens who would be using the app. They highlight that their position is to keep the use of these apps on a voluntary basis.

Some researchers explain that the use of contact tracing apps can be useful in containing the pandemic because the location data collected by the app would allow governments to track compliance with social distancing measures.\textsuperscript{34} Such timely feedback would provide vital information about the efficiency of messages and whether interventions are needed.\textsuperscript{35} However, metadata that seems unimportant such

\textsuperscript{29}Satariano A (2019) Police use of facial recognition is accepted by British court. \url{https://www.nytimes.com/2019/09/04/business/facial-recognition-uk-court.html}. Accessed 25 February 2020.

\textsuperscript{30}Kuligowski K (2019) Facial recognition advertising: the new way to target ads at consumers. \url{https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html}. Accessed 25 February 2020. Also see Lewinski et al. 2016.

\textsuperscript{31}Zastrow M (2020) Coronavirus contact-tracing apps: can they slow the spread of COVID-19? \url{https://www.nature.com/articles/d41586-020-01264-1}. Accessed 20 May 2020.

\textsuperscript{32}EDPB 2020b.

\textsuperscript{33}EDPB 2020c.

\textsuperscript{34}Buckee et al. 2020.

\textsuperscript{35}Ibid.
as location data can give away information about an individual that would allow identification of them. \(^{36}\) Many news stories have described how infected individuals in South Korea whose data was shared anonymously were deanonymized and identified by other citizens. \(^{37}\)

Given that location data can be used to deanonymize individuals, the EDPB guidelines put special emphasis on the anonymization of data, providing three criteria to ensure contact tracing apps comply: (1) it should not be possible to single out the individual, (2) it should not be possible to link two or more data points about any surveilled individual, (3) inference with significant probability. EDPB guidelines express concern that the legitimate need to collect location data to fight the pandemic will cause a ratchet effect where infringement of privacy, once allowed, cannot be disallowed even when the pandemic passes.

The COVID-19 related tracking app rolled out in Germany in June 2020 attempts to accommodate privacy concerns through the adoption of the following design features. \(^{38}\) First, the real identities of the users are not exchanged, but only anonymized IDs that change several times an hour are exchanged between phones. Second, contact details are not stored centrally, but instead decentrally on the respective smartphones. Exclusively the list of anonymized IDs of the infected individuals is kept on a central server. The identification and matching of users that were close to an infected user for a sufficient amount of time takes place solely on the individual smartphones. Third, the app does not record names, addresses or telephone numbers of users. When a newly infected user chooses to insert that information in the app, the user attests the reliability of this information by scanning a QR code generated by the public health facility that performed the test. A second way to attest the truthfulness of the positive test result is through a phone hotline, through which the infected user obtains a code to be then inserted in the app. This second verification option can be criticized as problematic in terms of the degree of privacy protection, because the anonymization that is upheld with the QR code option cannot longer be guaranteed to the same extent when the infected user dials the hotline. \(^{39}\)

Currently researchers are working on centralized and decentralized models of gathering data \(^{40}\) and discussions are taking place regarding which model will protect individuals’ privacy while serving the public interest in data gathering to fight the disease.
pandemic. Further attention by privacy scholars might also be focused on the differences among the national contact tracing apps preferred by EU Member States, their compliance with the GDPR as well as their interoperability after border restrictions are lifted.

### 12.5 Upcoming Challenges

In addition to the selected technological and current developments that have been analyzed in this chapter, many scholars also paid special attention to how to further develop blockchain technology that is compliant with the GDPR. Blockchain technology gained wider popularity and wider use in the recent years. This also led to an increase in attention to regulatory frameworks that could be applicable for the use of blockchain technology. Some scholarly analysis focused on how or whether the blockchain technology should be regulated, a research question a study for the European Commission DG Communications, Networks, Content & Technology is currently exploring. Regulatory efforts are aiming to find a balance between creating legal certainty for users and investors of this technology without hindering innovation. Finding this delicate balance could lead to different regulatory approaches to blockchain technology emerging across the globe and would be a very fruitful and necessary domain for further research.

### 12.6 Concluding Remarks

Preserving the right to the protection of personal data in a world marked by increasing digitalization, innovation, and technology-reliant lifestyles constitutes the goal of the GDPR. It seems increasingly clear that this regulatory effort will frequently require additional clarifications and situation-specific refinements as circumstances evolve and change, as exemplified by AI-supported enhanced information gathering technologies or crises such as the current pandemic. Whether current efforts, like the GDPR, are likely to achieve the fine balance of adequate privacy protection without stifling innovation dynamics and without watering down the right to protection of personal data, will continue being an exciting area for legal and interdisciplinary research to tackle in the coming years.

---

41 Criddle C and Kelion L (2020) Coronavirus contact-tracing: world split between two types of app. https://www.bbc.com/news/technology-52355028. Accessed 20 May 2020.
42 Finck 2018.
43 Study on Blockchains: Legal, governance and interoperability aspects (SMART 2018/0038), Study on Blockchains (2020.0931), version 27 March 2020.
References

Acquisti A, Gross R, Stutzman FD (2014) Face recognition and privacy in the age of augmented reality. J Privacy and Confidentiality 6(2):1
Acquisti A, Taylor C, Wagman L (2016) The economics of privacy. J Econ Lit 54(2):442–492
Akerlof G (1970) The market for lemons: Qualitative uncertainty and the market mechanism. Q J Econ 84:488–500
Albrecht JP (2016) How the GDPR will change the world. Eur Data Prot L Rev 2:287
Bucke CO et al (2020) Aggregated mobility data could help fight COVID-19. Science (NY) 368(6487):145 https://science.sciencemag.org/content/368/6487/145.2
European Commission (2015a) Communication, “Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe”, COM (2015) 192
European Commission (2015b) Special Eurobarometer 431 (June 2015). http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf Accessed 16 January 2020
European Commission (2019) Special Eurobarometer 487a (June 2019). http://ec.europa.eu/public_opinion/archives/ebs/ebs_487_sum_en.pdf Accessed 16 January 2020.
European Data Protection Board (2018) Endorsement 1/2018. https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf Accessed 25 February 2020
European Data Protection Board (2020a) Guidelines 3/2019 on processing of personal data through video devices, Version 2.0 29 January 2020. https://edpb.europa.eu/our-work-tools/our-documements/guidelines/guidelines-32019-processing-personal-data-through-video_en Accessed 25 February 2020
European Data Protection Board (2020b) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, Version 1.1 30 April 2020. https://edpb.europa.eu/sites/edpb/files/files/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf Accessed 20 May 2020
European Data Protection Board (2020c) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020. https://edpb.europa.eu/sites/edpb/files/files/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf. Accessed 20 May 2020
Federal Government of the Federal Republic of Germany (2020), press release on the “Introduction of the Corona-Warning-App” https://www.bundesregierung.de/breg-de/themen/coronavirus/veroeffentlichung-der-corona-warn-app-1760892 Accessed 17 June 2020
Finck M (2018) Blockchains: regulating the unknown. German Law J 19(4): 665–692
Floridi L (2011) The informational nature of personal identity. Minds Mach 21(4):549–566
Hildebrandt M (2008) Profiling and the identity of the European citizen. In:Hildebrandt M, Gutwirth S (eds) Profiling the European citizen. Springer, Dordrecht, pp 303–343
Hildebrandt M, Tielmans L (2013) Data protection by design and technology neutral law. Comput Law Secur Rev 29(5):509–521
Kosinski M, Stillwell D, Graepel T (2013) Private traits and attributes are predictable from digital records of human behaviour. P Natl Acad Sci USAmerica 110(15):5802–5805
Kuner C (2010) Data protection law and international jurisdiction on the internet (part 1). Int J Law Inf Technol 18(2):176–193
Lewinski P, Trzaskowski J, Luzak J (2016) Face and emotion recognition on commercial property under EU data protection law. Psychol Marketing 33(9):729–746
Ringrose K (2019) Law enforcement’s pairing of facial recognition technology with body-worn cameras escalates privacy concerns. VA Law Rev Online 105:57
Schneier B (2015) Data and Goliath: The hidden battles to collect your data and control your world. WW Norton, New York
Schwartz P (2013) The EU-US privacy collision: a turn to institutions and procedures. Harvard Law Rev 126:1
Sunstein CR (2001) Republic.com. Princeton University Press, New Jersey
Victor JM (2013) The EU general data protection regulation: Toward a property regime for protecting data privacy. Yale Law J 123:513
Voigt P, von dem Bussche A (2017) The EU general data protection regulation (GDPR): A practical guide. Springer International Publishing, Cham
Wachter S (2018) Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR Comput Law Secur Rev 34(3):436–449
Welinder Y (2012) A face tells more than a thousand posts: Developing face recognition privacy in social networks Harv J Law Technol 26:165

**Dr. Elif Kiesow Cortez** is a senior lecturer and researcher in data protection and privacy regulation in the International and European Law Program at The Hague University of Applied Sciences (THUAS), the Netherlands.