CHAPTER 8

PRIVACY AND SECURITY: GERMAN PERSPECTIVES, EUROPEAN TRENDS AND ETHICAL IMPLICATIONS

Hartmut Aden

ABSTRACT

Since the European Union's (EU) Charter of Fundamental Rights became binding in 2009, data protection has attained the status of a fundamental right (Article 8) throughout the EU. This chapter discusses the relevance of data protection in the context of security. It shows that data protection has been of particular relevance in the German context – not only against the backdrop of rapidly evolving information technology, but also of the historical experiences with political regimes collecting information in order to oppress citizens.

Keywords: Germany; security; surveillance; transparency; privacy; social movements

INTRODUCTION – THE RELEVANCE OF PRIVACY IN GERMANY AND IN EUROPE

Over the past few decades, privacy has become an important issue in many countries, evolving in parallel with the rapid development of information technologies

Ethical Issues in Covert, Security and Surveillance Research
Advances in Research Ethics and Integrity, Volume 8, 119–129

ISSN: 2398-6018/doi:10.1108/S2398-601820210000008009

and the internet. This chapter discusses how historically unique and specifically German perspectives on privacy and data protection have shaped the relationship between privacy and security, and how privacy and data protection have gained relevance as fundamental rights and as ethical requirements in Europe. The chapter shows that the European Union's (EU) Charter of Fundamental Rights (CFR) and the recently introduced EU framework for data protection have contributed to the growing importance of data protection in everyday life, as well as for security agencies.

The EU's CFR became binding with the Treaty of Lisbon in 2009. In 2016, the General Data Protection Regulation (GDPR) 2016/679[1] and the Directive (EU) 2016/680[2] on data protection in the area of law enforcement (policing and criminal justice) laid down detailed rules on the implementation of data protection. When the CFR and the GDPR became directly binding, they established a solid legal framework for *privacy* and *data protection* everywhere in Europe. This includes binding rules for companies from outside the EU processing the personal data of individuals who are physically in the EU zone, as long as the processing activities are related to the monitoring of the individuals' behaviour or to the offering of goods or services (Art. 3(2) GDPR).

This chapter takes a trans-disciplinary historical-institutionalist perspective in discussing path dependencies between the misuse of knowledge about citizens by former German regimes, and the importance that many German citizens attribute to privacy in relation to the state's security agencies. These issues are related to the broader question about to what extent specific characteristics of a political system influence the relationship between security, ethics, and privacy.

The chapter uses the terms *data protection* and *privacy* not as synonyms, but rather as complementary aspects of the same right (see Tzanou, 2017, pp. 21–24 on the relationship between these terms). The term *privacy* is laid down in newer fundamental rights catalogues such as the EU's CFR. *Privacy* guarantees that private life is protected against attempts by state agencies and private parties to obtain and retain information related to an individual's private sphere. *Data protection* (guaranteed as a fundamental right by Article 8 CFR) is somewhat more broad. *Data protection* includes self-determination with respect to any information on individuals. Since *privacy* and *data protection* are complementary in relation to each other, courts tend to refer to both of them in conjunction.

GERMAN EXPERIENCES OF SECURITY AGENCIES COLLECTING EXCESSIVE INFORMATION ON CITIZENS

Over the last 90 years, German citizens have been confronted with two political regimes that based and enforced their abuse of power on information collected about their own citizens and, particularly, about their political opponents. The first of these was the *Geheime Staatspolizei* (commonly known as the *Gestapo* – Secret State Police) during the Nazi regime. The second was the *Ministerium für Staatssicherheit* (the *'Stasi'* – Ministry for State Security) in Eastern Germany. It is always a delicate exercise to compare these political regimes – they both

oppressed sections of their citizenry, however, they did so for very different reasons and to different extents. With this in mind, in the context of this chapter, it is relevant that both political regimes misused information collected by the *Gestapo* and the *Stasi* for further surveillance purposes. From a security ethics perspective, it is clear that these historical cases demonstrate the risks related to (mass) surveillance by powerful security agencies.

The *Gestapo*, established in 1933, quickly developed into one of the backbones of the Nazi's racist prosecution strategies. At that time, modern technological surveillance, as it is known today in the era of information technology, did not yet exist. The information collected about Jewish citizens, political opponents, and members of other groups targeted by racist prosecution mostly stemmed from denunciation – citizens providing evidence to security agencies for a variety of reasons knowing well that this would lead to prosecution, imprisonment and even murder – and other information provided by citizens (see Gellately, 1992).

The *Stasi* was established in early 1950 soon after the eastern zone of Germany, occupied by the Soviet Union's forces at the end of World War II, became the *German Democratic Republic* (*Deutsche Demokratische Republik*, the DDR) in 1949. Until the end of the DDR regime in 1989, the *Stasi* employed more than 91,000 full time staff and a large number of informants in order to conduct surveillance of the country's 16 million inhabitants, with a particular focus on citizens suspected of being opposed to the DDR regime (see Macrakis, 2008).

Inferring a relationship between the *Gestapo* and the *Staatssicherheit (Stasi)* on one hand, and the specific sensitivity of German citizens towards privacy on the other, seems plausible; however, is difficult to prove based on the available empirical data. More than in most other countries, data collection by public administration and security agencies and more recently also by private companies has triggered powerful social movements in Germany that forced policy-makers to take privacy seriously. For example, a social movement successfully stopped the 1983 census before the German Constitutional Court (see Section 2). In 2008, more than 34,000 citizens signed a constitutional complaint against the retention of telecommunication meta data by security agencies for future criminal investigation – what was a step towards the annulment of the relevant EU Directive by the Court of Justice of the EU a few years later (cf. Aden, 2016, p. 56f.).

It should not be overlooked that, in any society, significant differences in the attitudes towards privacy exist and persist. Some citizens are worried about state agencies and private companies collecting their personal data, while others look at these practices in a more favourable manner. However, in all countries, opposition to excessive data collection by state agencies and private companies goes beyond specific small groups of civil liberties activists.

These issues, resituated to the current state of technology, are pertinent to the currently very high level of information on individuals now accessible to public security agencies as well as some private companies. In the cases of the *Gestapo* and the *Stasi*, this level of information would have made them incalculably more powerful; the abuse of state power would have become even more effective and broad.

With online communication and mobile devices such as smartphones and laptop computers becoming parts of everyday life, state agencies nowadays can

easily track current and past movements and communication. The mass-data collection practices of the US *National Security Agency* (NSA), disclosed by whistleblower Edward Snowden in 2013, and the surveillance system that the Chinese government established in order to supervise the behaviour of Chinese citizens, demonstrate that states are already able and willing to submit their citizens to a regime of mass surveillance and 24/7 monitoring if no solid ethical culture and rule of law framework prevent them from doing so.

DATA PROTECTION AND PRIVACY: THE 1983 GERMAN CENSUS CASE

In the specific German variant of a continental rule-of-law system, the recognition of privacy as a fundamental right means that any kind of data processing by a public authority needs an explicit and proportionate legal basis. Since the 1980s, this has significantly impacted the legal framework for data processing, initially by the former West German security agencies, and now for a united Germany.

The specific privacy regime that characterises the relationship between privacy and security in Germany goes back to a landmark judgement by the German constitutional court (*Bundesverfassungsgericht*, BVerfG). The BVerfG enjoys a strong position in the German political system, including the power to annul laws disproportionally encroaching upon the citizens' fundamental rights.

In 1983, the then West German government planned to renew the basis for statistical data collection in a general population census. The government intended to combine this census data collection with a renewal of the citizens' registers, in order to verify whether all citizens had correctly declared their residence to the local authorities – a legal obligation (*Meldepflicht*) under German law. However, West German civil liberties groups raised concerns, claiming that the combination of the census with updating the citizens' registers would lead to the existence of the 'transparent citizen' in West Germany. These concerns quickly spread outside the civil liberties groups. Protests developed into a social movement, and some lawyers involved in the growing movement brought a case before the BVerfG. This was possible because, similar to applications before the European Court of Human Rights, German citizens are able to bring fundamental rights cases directly before the BVerfG as constitutional complaints (*Verfassungsbeschwerden*). In exceptional cases, if serious harm to fundamental rights is seen as directly derived from a German law, citizens do not even have to go to the ordinary courts and through the stages of appeal before bringing a case to the BVerfG.

In response to the constitutional complaints brought before it, the BVerfG, in its judgement, annulled the 1983 census law. The reasons given by the court at that time now sound somewhat prophetic at a distance of almost 40 years, and several rounds of technological innovations later.

> 1. In the context of modern data processing, the general right of personality [*Allgemeines Persönlichkeitsrecht*] under Article 2.1 in conjunction with Article 1.1 [Human Dignity – *Menschenwürde*] of the Basic Law encompasses the protection of the individual against unlimited collection, storage, use and sharing of personal data. The fundamental right guarantees the

> authority conferred on the individual to, in principle, decide themselves on the disclosure and use of their personal data.
>
> 2. Limitations of this right to 'informational self-determination' are only permissible if there is an overriding public interest. They require a statutory basis that must be constitutional itself and comply with the principle of legal clarity under the rule of law. The legislator must furthermore observe the principle of proportionality. It must also put in place organisational and procedural safeguards that counter the risk of violating the general right of personality.[3]

Essentially, the BVerfG judgement established a new fundamental right through the interpretation of two already existing rights. Since then, this new fundamental right has had a significant impact upon the way in which public authorities and private entities process personal data. In the security sector, federal laws governing criminal procedure, the federal police agencies, and the federal intelligence services had to be adapted to this new fundamental right. As policing is one of the core tasks of the 16 States (*Länder*) in the German federal system, the *Länder* had to include data processing rules in their policing laws (cf. Aden & Fährmann, 2019).

In 2008, the BVerfG even established an additional fundamental right: the *guarantee of the confidentiality and integrity of information technology systems*,[4] again, equally deduced from Articles 2.1 and 1.1 of the German constitution (*Grundgesetz*). The establishment of this new fundamental right in Germany recognises the relevance of the essential role of personal electronic devices as they are used today and the potential threat to privacy if state surveillance is not effectively limited through legislation. This has become even more relevant since then. People use their smartphones and computers all day long, and therefore these devices 'know' much about their users, in many cases including information on the core of private life, such as communication between family members.

PRIVACY AND THE CURRENT STATE OF TECHNOLOGICAL DEVELOPMENT

The rapid development of information technology during the past decades (cf. Aden, 2019; Nogala, 1989, 2019) creates additional challenges for the relationship between privacy and security as well as for security ethics.

The Internet, since the 1990s, has facilitated information sharing and communication worldwide – it has also enabled security agencies to intercept and retain detailed information on every citizen. In one sense, this approach is understandable from the perspective of requirements of state agencies to protect their citizens, and, indeed, to avoid criticisms of not doing so. Accordingly, in reaction to the terrorist attacks in New York City and Washington DC on 11 September 2001, many state security agencies developed mass surveillance strategies. In 2013, whistleblower Edward Snowden revealed the extent to which the US NSA retained huge quantities of data, not justifiably related to any specific security purpose. Although Snowden's revelations led to a controversial debate on the legitimacy of mass surveillance, and, in some jurisdictions, to certain legal limitations, untargeted surveillance by security agencies was not substantially restricted (see Lyon, 2015).

Rapid technological advances have contributed to making mass surveillance even more intrusive and in contention with fundamental rights. Carrying a smartphone in everyday life means that users produce passive data that security agencies and private parties, such as providers of smartphone applications, can easily access. Smartphones therefore have become auto-surveillance tools enabling security agencies to monitor individuals and to track their movements. German security agencies frequently use stealth pings ('stille SMS') in order to secretly detect the location of a device and its user. They also use their legal authority to claim data on all mobile devices (and their owners) present in a specific area at a given time from mobile communication providers in order to find potential suspects following a crime (see Fährmann, Aden, & Bosch, 2020, p. 141; Monroy, 2019).

The growing relevance of other devices connected to the internet in everyday life ('internet of things' or IoT) is likely to make mass surveillance even easier for security agencies. Security research is developing new search and identification technology, mostly based on the use of biometric data such as fingerprints and facial recognition, often combined with automated searches of large quantities of data (see Kühne & Schlepper, 2018 for a critique).

During police stops, biometric data stored in ID cards and passports enable police officers to use newly introduced mobile devices to compare the personal data of the legitimate holder to the data of the individual present at the stop – in order to be sure that the passport is not counterfeit or stolen. In German state and federal police laws, the legal requirements for background checks in police databases tend to be low – mostly the only requirement is that the information is necessary to carry out a police task. German police officers therefore routinely carry out background checks in police databases: mobile devices enable them to collect fingerprints or photographs – they can use this biometric data to check if the stopped individual has entries in police databases (cf. Fährmann et al., 2020, p. 142f.). The quantity of data accessible in police databases is rapidly growing, accelerated not only by a new generation of technology, but also by recent initiatives to make the EU's policing and migration databases interoperable: the *Schengen Information System*, the *Visa Information System, Eurodac*, the newly established EU *Entry Exit System*, and other databases (cf. Aden, 2020 for a critique).

In the German rule of law system, state action that restricts the citizens' use of their fundamental rights requires a legal basis and proportionate safeguards in order to prevent excessive restrictions. Therefore, if German security agencies wish to use new technologies, for example, body-worn cameras or facial recognition, this requires a specific legal basis, defining the extent to which these technologies may restrict the right to data protection. Technological development can also lead to more performant technologies that make already existing legal bases more intrusive to fundamental rights. For example, video technology has rapidly become more performant over the past decades. With older video cameras, it was often impossible to identify individuals in a crowd on video footage. Recent technological development allows a comparatively high level of resolution, and individuals can be more easily detected. Therefore, laws authorising video surveillance (Closed Circuit

Television, CCTV) have become much more intrusive upon the citizens' right to data protection, even if the relevant laws have not been amended in their wording (see Fährmann et al., 2020, p. 143ff.).

The use of machine learning and artificial intelligence tools by security agencies is also likely to trigger further mass surveillance in the future (cf. Golla, 2020). As a result, the fast development of information technology that enables security agencies to potentially collect detailed information about all citizens including core aspects of their private life will require clear ethical standards and legal limitations that protect the individuals' fundamental rights.

TRANSPARENCY, ACCOUNTABILITY AND DATA PROTECTION

Data protection can only be effective if it is integrated into a solid accountability framework. The obligation to explain and justify conduct is a core element of accountability (Bovens, 2007, p. 450). As major parts of electronic data processing are invisible for the individuals concerned, independent data protection authorities play a crucial role as accountability forums (cf. Aden, 2021, p. 35f.).

In addition to independent oversight, transparency is another key factor involved in the accountability of data processing (cf. Raab, 2012, p. 24ff.). Transparency means, in this case, that only if citizens understand the purposes for which security agencies will use and process their data, they are able to decide if these purposes are acceptable to them. Article 5(1) GDPR mentions transparency as one of the core principles for data protection, along with principles such as the legality and fairness of data processing and purpose limitation. Directive 2016/680 on data protection for policing and criminal justice purposes does not explicitly mention transparency as a data protection principle (Article 4(1)). However, transparency is referenced as part of the fairness principle laid down in Article 4(1) (cf. Johannes & Weinhold, 2018, p. 65; Tzanou, 2017, p. 26). Transparency and fairness are closely connected. Only if the use and application of a technology is transparent, and therefore understandable for the citizens, may they perceive it as fair and legitimate – and therefore accept it.

In the digital era, the accountability of data processing and principles of fairness and transparency are confronted by new challenges. Even if citizens wish to understand how state agencies and private companies process their personal data, mounting quantities of data and complex technologies make this increasingly difficult. Both security agencies and private companies are not necessarily interested in making data processing transparent. In their eyes, transparency may lead to critical questions and unwanted monitoring and oversight. More generally, the availability of information leads to an asymmetric power relationship (cf. Aden, 2004, 2018). Power is based on access to and understanding of information and knowledge; power can be more easily exerted upon someone who does not understand the data landscape. In this respect, accountability of operators and transparency for citizens are crucial elements of lawful and ethical data processing.

PRIVACY AND SECURITY – NEW SYNERGIES?

In political debates, privacy and security are often framed in opposition to each other, with data protection preventing enforcement agencies from collecting, retaining, and analysing data necessary for combating criminal behaviour effectively.

However, political debates, and sometimes also arguments by security practitioners, tend to overestimate this conflict and to underestimate synergies between data protection and effective law enforcement. Collecting large quantities of data alone does not guarantee effective law enforcement. With increasing quantities and types of 'big data', quality management, in order to turn it into effective intelligence, becomes an ever more demanding task. False or outdated information may misguide law enforcement and lead to a loss of precious investigative time. Therefore, keeping databases and other information used by security agencies up-to-date is a major issue. In contrast to paper archives, electronic information nowadays needs very little space to be stored. Searches in databases have become easy and fast, even with vast quantities of data. Therefore, the instances of paper files or stacks being full and difficult to manage that forced security agencies to trash outdated information in the analogue world are not applicable in the digital age.

Thus, one impact and result of privacy regulation can be more effective investigation and enforcement. Data protection laws prohibit the use of false or outdated personal data, in the interest of the individuals concerned, but also in the interest of the quality of investigations and effective management of resources. According to CFR Article 8 (2), 'everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'. False or outdated data may have far-reaching consequences for the individuals concerned; for example, an unjustified arrest. Therefore, developing effective tools to assure high quality data used for security purposes creates synergies between privacy and security. It follows that when privacy laws prevent security agencies from collecting a wide swath of data, they are forced to create and use a more focussed investigative strategy.

Privacy by design and by default, required by EU data protection law (Article 25 GDPR and Article 21 Directive 2016/680), also aims to ensure effective consideration of privacy issues at the development and implementation stages of new technologies. This is a strategy to prevent the dependency of effective data protection on the 'human factor' at the end user stage. Data protection solutions that depend upon their application by individual users are likely to be circumvented or simply forgotten by negligence. Designing technology in a way that only allows its use in a way that is data protection friendly is therefore a relevant strategy to create synergies between privacy, ethics, and security (see Aden & Fährmann, 2019, 2020 on the growing importance of *privacy by design* solutions). Data protection laws only define *privacy by design and by default* as a general obligation. Therefore, specific technological standards will have to be developed in order to implement *privacy by design and by default* for technology used by security agencies. Data protection impact assessments (as foreseen by

Article 35 GDPR and Article 27 Directive 2016/680) and trans-disciplinary cooperation between lawyers, engineers and social scientists can be adequate loci for the development of new technologies implementing the ideas of *privacy by design and by default* (cf. Aden & Fährmann, 2020).

TOWARDS EUROPEAN LEGAL AND ETHICAL STANDARDS FOR THE PROTECTION OF THE CITIZENS' PRIVACY?

In June 2020, two years after the GDPR (EU) 2016/679 entered into force, the European Commission drew a generally positive picture.

> In an economy increasingly based on the processing of data, including personal data, the GDPR is an essential tool to ensure that individuals have better control over their personal data and that these data are processed for a legitimate purpose, in a lawful, fair and transparent way. (European Commission, 2020, p. 1)

However, additional harmonisation efforts remain on the agenda with respect to GDPR rules requiring adaptation to specific issue areas, to opening clauses left to the member states' legislators and to the transposition of the data protection directive (EU) 2016/680 for law enforcement into the member states' laws.

This chapter has shown that Germany has been a forerunner for establishing data protection and privacy as fundamental rights. Bad experiences with political regimes that built their power on surveillance may have contributed to make this topic more relevant in Germany compared to other countries. Surveillance strategies by public authorities repeatedly triggered social movements that successfully forced policy-makers to take privacy seriously. Through the EU's CFR, binding since 2009, the GDPR and the law enforcement data protection directive, similar standards now govern the relationship between security and data protection in all EU countries. While most areas are covered by the directly binding GDPR, data protection standards for security agencies in the area of policing and criminal justice have been separately regulated in the law enforcement data protection directive – this means that the member states have to transpose the directive and establish binding standards in their own laws. However, the wording and the substantive data protection standards tend to be similar to those covered by the GDPR. Further standards that the European Data Protection Board – a coordinating body including the member states' Data Protection Authorities and the European Data Protection Supervisor – and upcoming judgments of the Court of Justice of the EU interpreting the GDPR and the directive are likely to influence data protection standards for law enforcement as well. Thus, it can be forecasted that even in Germany, where policing is one of the core authorities of the 16 *Länder*, improved European standards for data protection will influence the security sector as well.

Sociologists of law claim that law has an impact on the behaviour of most people (Friedman, 2016). In the digital era, data protection laws that establish ethical rules oriented towards the protection of fundamental rights can play a crucial

role for security ethics. In Germany, and the EU in general, the increasingly rapid development of information and surveillance technology continues to make the relationship between security and privacy an important issue for security ethics and for the protection of citizens' fundamental rights against exaggerated intrusion into private life for security purposes.

NOTES

1. 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 (GDPR), OJ EU L 119 of 4.5.2016, p. 1.
2. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ EU L 119 of 4.5.2016, p. 89.
3. BVerfG judgement of 15 December 1983 BVerfGE 65, 1; official English summary: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html;jsessionid=87B3C7425DE662A7E1A31F91729C4D70.2_cid377 (accessed 20.12.2020).
4. BVerfG, judgement of 27 February 2008, BVerfGE 120, 274; official English summary: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html (accessed 20.12.2020).

REFERENCES

Aden, H. (2004). Herrschaft und Wissen. In H. Aden (Ed.), *Herrschaftstheorien und Herrschaftsphänomene* (pp. 55–70). Wiesbaden: Verlag für Sozialwissenschaften.

Aden, H. (2016). Die Beteiligung von Bürgerrechtsverbänden an Gerichtsverfahren. Politisierung von Rechtsfragen oder Entpolitisierung durch Verrechtlichung?. In M. Plöse, T. Fritsche, M. Kuhn, & S. Lüders (Eds.), *„Worüber reden wir eigentlich?" Festgabe für Rosemarie Will* (pp. 556–565), Berlin: Humanistische Union.

Aden, H. (2018). Information sharing, secrecy and trust among law enforcement and secret service institutions in the European Union. *West European Politics (WEP)*, *41*(4), 981–1002.

Aden, H. (2019). Polizei und Technik zwischen Praxisanforderungen, Recht und Politik. *Vorgänge, no. 227*, *58*(3), 7–19.

Aden, H. (2020). Interoperability between EU policing and migration databases: Risks for privacy. *European Public Law*, *26*(1), 93–108.

Aden, H. (2021). Financial accountability in the broader framework of accountability studies. In P. Stephenson, M.-L. Sánchez-Barrueco, & H. Aden (Eds.), *Financial accountability in the European Union. Institutions, policy and practice* (pp. 25–40). London: Routledge.

Aden, H., & Fährmann, J. (2019). Defizite der Polizeirechtsentwicklung und Techniknutzung. *Zeitschrift für Rechtspolitik*, *52*(6), 175–178.

Aden, H., & Fährmann, J. (2020). Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung. Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie. *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, *29*(3), 24–29.

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, *13*(4), 447–468.

European Commission. (2020). Communication […]: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – Two years of application of the General Data Protection Regulation. COM(2020)264 final, Brussels.

Fährmann, J., Aden, H., & Bosch, A. (2020). Technologieentwicklung und Polizei: intensivere Grundrechtseingriffe auch ohne Gesetzesänderung. *Kriminologisches Journal*, *52*(2), 135–148.

Friedman, L. M. (2016). *Impact. How law affects behavior*. Cambridge, MA: Harvard University Press.

Gellately, R. (1992). *The Gestapo and German society: Enforcing racial policy, 1933–1945*. Oxford: Oxford University Press.

Golla, S. J. (2020). Lernfähige Systeme, lernfähiges Polizeirecht Regulierung von künstlicher Intelligenz am Beispiel von Videoüberwachung und Datenabgleich. *Kriminologisches Journal*, *52*(2), 149–161.

Johannes, P. C., & Weinhold, R. (2018). *Das neue Datenschutzrecht bei Polizei und Justiz*. *Europäisches Datenschutzrecht und deutsche Datenschutzgesetze*. Baden-Baden: Nomos.

Kühne, S., & Schlepper, C. (2018). Zur Politik der Sicherheitsversprechen. Die biometrische Verheißung. In J. Puschke & T. Singelnstein (Eds.), *Der Staat und die Sicherheitsgesellschaft* (pp. 79–99). Wiesbaden: Springer VS.

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge: Polity Press.

Macrakis, K. (2008). *Seduced by secrets: Inside the Stasi's Spy-tech World*. Cambridge: Cambridge University Press.

Monroy, M. (2019). Die Ortungswanze in der Hosentasche Maßnahmen nach §§ 100 StPO zum Ermitteln des Aufenthaltsorts und der Kennung von Mobiltelefonen. *Vorgänge, no. 227*, *58*(3), 85–93.

Nogala, D. (1989). *Polizei, avancierte Technik und soziale Kontrolle*. Pfaffenweiler: Centaurus.

Nogala, D. (2019). Polizei, avancierte Technik und soziale Kontrolle. Wie geht's dem Frosch heute? *Vorgänge, no. 227*, *58*(3), 21–30.

Raab, C. (2012). The meaning of 'accountability' in the information privacy context. In D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland, & H. Postigo (Eds.), *Managing privacy through accountability* (pp. 15–32). Basingstoke: Palgrave Macmillan.

Tzanou, M. (2017). *The fundamental right to data protection*. Oxford: Hart Publishing.