European Journal for Security Research (2020) 5:5–23
https://doi.org/10.1007/s41125-019-00062-9

ORIGINAL ARTICLE

Data, Data Banks and Security

Hans-Jörg Albrecht[1]

Received: 15 August 2019 / Accepted: 25 November 2019 / Published online: 25 February 2020

Abstract
The article discusses different examples of data-driven policing, its legal provisions and effects on a society's understanding of public security. It distinguishes between (a) the collection of classical data such as fingerprints or DNA, which serve to identify suspects and to collect evidence, (b) the processes and the impetus of big data, and (c) the networking of files from different security authorities. Discussing systematic forecasting tools, the article works out a significant difference between the prediction of incidents such as home burglary in the case of predictive policing, and the identification of individuals deemed to be at risk of involvement in various forms of crime in the case of risk control programs. Data and personality protection are interrelated issues.

Keywords Data-driven policing · Predictive policing · Risk control programs · Data retention policies

1 Introduction: Data, Risk and Security

Security policies and policing have always been based on systematic data collection and data banks. Taking of fingerprints, the production and retention of photographs of suspects, the systematic collection of crime and perpetrator information in comprehensive police files, and later the equally systematic collection and storage of DNA profiles refer to a line of data and data banks that are based on investigation of crime and criminal proceedings and are essentially built on the assumption that these data can contribute to the identification of suspects in current or future criminal cases. Another consideration is that the collection and retention of investigative data, in particular DNA profiles, can have a preventive effect by deterring those captured in data banks (Tegner Anker et al. 2018).

✉ Hans-Jörg Albrecht
h.j.albrecht@mpicc.de

[1] Max Planck Institute for Foreign and International Criminal Law, Günterstalstr. 73, 79100 Freiburg, Germany

Automated processing and digitization then made data retention and, above all, data analysis and matching of data easier from the 1990s onwards. At the same time, legislation on the protection of personal data is developing, leading to normative frameworks and conditions which have limiting effects in the form of deletion periods, reasons for data retention, etc. The main focus is here on the protection of personal data through minimizing the amount of retained data. This introduces a further perspective on security, namely the security of personal data and the protection of fundamental rights, above all the right to privacy and the right to self-determination with respect to personal data.

This first line in data collection and retention for law enforcement and security purposes, created during law enforcement, aims to improve the investigation of criminal offences by effectively identifying repeat offenders. Here, police themselves maintain databases in which personal data on known suspects or traces (DNA, fingerprints) of unknown suspects and other information on crime are entered and retained. This approach to data collection and resulting retention strategies are certainly convincing. Criminological research shows that in particular serious crime is committed predominantly by repeat offenders (or career offenders). In this respect, comprehensive data covering the group of repeat offenders is most likely to improve clearing up rates.

A second line of data collection and the use of retained data for security purposes arises from what is now known as "big data". The digitalization of communications and transactions leads to the extensive generation and storage of data that is generated during telecommunication, Internet surfing, financial transactions, travel information or reservations. The use of such data for security purposes takes various forms. The private sector is involved here in different ways, since most of these data is generated in the commercial sector. On the one hand, the police and secret services are granted the right of access to existing data files or data generated in an ongoing process (e.g. telecommunications providers) for the purpose of identifying and averting dangers or investigating and prosecuting suspects in individual cases. The retention of telecommunications traffic data must also be classified here. In addition, secret services generally have the authority to search data streams for suspicious transactions or suspicious communication using keywords (bulk surveillance). On the other hand, private individuals may be obliged to check data for suspected criminal offences and to pass these on to the police in the event of suspicion. Money laundering legislation has introduced such an obligation for banks, insurance companies and other commercial players (§43 Money Laundering Act). The obligation can also be aimed at handing over all data arising in a certain commercial area to state authorities. Such an obligation is introduced by the Passenger Data Act of 25 May 2018. Air carriers are obliged to transmit passenger data to the Federal Criminal Police Office (Passenger Information Unit) for flights within the European Union and to non-European countries. The analysis of the data and corresponding decisions on further retention, forwarding or further investigations will then be carried out by the police.

Finally, a third line concerns the networking of files held by different security authorities. The anti-terror data bank provides an example of such networking. This third line also includes (international) data exchange, the associated issue

of interoperability and the development of transnational data systems such as the Schengen Information System or the European Travel Information and Authorisation System (ETIAS; see for a summary Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2019, pp. 31–32).

Data thus ultimately become the core of security policies. The European Strategy for Internal Security (European Commission 2010) already states that information is the key to effective internal security. Data and data exchange are also at the centre of European Union policies establishing a "Security Union" (European Commission 2016).

2 Security Agencies, Data and Security Strategies

Since the 1990s, strategies of "predictive policing" (or "smarter policing") have been developed, which are increasingly attracting international attention and which are complemented by police strategies falling under "community policing", "problem policing", "hot spot policing" and "zero tolerance". Common to these approaches is not only the claim to solve crime problems on the basis of empirical knowledge and empirical evidence (or to reduce crime and feelings of insecurity), but also the more or less strong reference to criminological and social science theories in the form of the theory of rational choice, the theory of routine activities, the theory of social disintegration and informal social control (broken windows) or theories of legitimacy (trust and cooperation). The practical prerequisites for the formation of a preventative police were created by the rapid development of information technology, reduced costs for hardware, increasing and effective networking and data transfer, the rapid growth of police information systems and databases as well as decentralized data collections driven by social media and IT corporations such as Google, Facebook or Apple, and finally by increasingly efficient data mining techniques, which also reflect the considerable progress in pattern recognition software and the integration of geographical data, texts or pictures. In designing predictive policing, however, there is now a movement away from a research—(and theory-led) towards a data-driven strategy (which, incidentally, is embedded in the general interest in stockpiling information and widening data collection and is described with great openness in a paper from the North Rhine-Westphalian Ministry of the Interior as a procedure that is "free of content-related and theoretical assumptions", Schürmann 2015, p. 4).

The concept of a predictive police in Germany has received special attention in recent years, initially in connection with burglaries (Landeskriminalamt NRW 2017). After a sharp increase in burglaries up to about 1993, there was an even more pronounced decline up to about 2006, after which the number of burglaries rose again by 2015, although the scale of burglaries in the years after the abolition of borders and the fall of the iron curtain in Europe and in the first half of the 1990s was not even close to reached. The presentation of German police crime statistics in 2016 then again showed a drastic decrease in burglaries compared to 2015 (from about 167,000 to ca. 151,000; cf. time series on www.bka.de; the decrease developed into a free fall in 2017: 116,540 burglaries were

registered in 2017). In 2018, the police crime statistics finally count 97,504 burglaries. The increasing number of burglaries since 2006, which is noticeable in view of the otherwise declining burden of conventional, also property-related, crime (Albrecht 2016), and which is particularly relevant for criminal policy because of the considerable effects it has on the victims' feelings of security and the notoriously low rate of investigations (Landeskriminalamt NRW 2017, p. 23f), some years ago encouraged some European and then above all German police authorities to use software first developed in the USA and finally offered by various companies in Europe, which promises accurate predictions of the occurrence of burglaries and effective solutions going beyond the burglary. However, IBM's offer already showed certain weaknesses not in the basic arithmetic operations, but in the determination of the problem, when for the year 2014 out of 152,123 burglaries (including 63,282 day time burglaries) by simple addition 215.405 burglaries and moreover forgetting to adequately consider attempted burglary crimes (which account for almost half of police-registered offences; http://www.935.ibm.com/services/multimedia/Smarter_Policing.pdf). An increasing number of enquiries in German state parliaments and the Bundestag since 2014 underline that predictive policing has gained great importance both politically and practically today. In any case, different software is now being used in different federal states with the aim of reducing the number of burglaries (Bayerisches Landeskriminalamt 2015; in summary www.heise.de/newsticker/meldung/Predictive-Policing-Die-deutsche-Polizei-zwischen-Cyber-CSI-und-Minority-Report-3685873.html).

Forward-looking and preventative policing is a matter of course. Averting dangers, preventing crime and dealing with threats are central tasks of police and are always based on prediction (and assessments). In this context, prevention is essentially about short-term prevention, i.e. pre-emption, which differs significantly from the more long-term forms of prevention developed in criminal law theory (positive general prevention and prevention through resocialization). If preventative police are concerned with the prevention or reduction of crime (in all its forms), two conditions are decisive for effectiveness. First of all, it depends on accurate predictions as to where, when, by whom (and against whom) crimes are committed. Of course, this alone is not sufficient. For, the knowledge that leads to the prediction must be translated into effective prevention, i.e. measures or interventions. Only the combination of accurate prediction and effective intervention can produce benefits in the form of crime prevention.

The start of a predictive police is now set with the implementation of CompStat in the New York police force. The implementation of CompStat was based on a combination of real-time oriented data processing and use in police practice, the adaptation of organization and operations to precisely defined goals as well as the immediate verification of targets by individual police authorities (Bureau of Justice Assistance 2013). Furthermore, CompStat is embedded in a strategy of zero tolerance policing based on the "Broken Windows" theory, police organizational reform and a policy strictly oriented towards cost–benefit analyses.

3 Starting Points

The starting points for predictive policing, however, go back further than Compstat. They are geared to individuals, incidents and spaces. In the case of proactive policing of relevant individuals, the question is whether individuals can be identified whose risk of becoming perpetrators or victims of crime is significantly higher than the baseline of crime participation or victimization (at least to the extent that interventions pay off, see Saunders 2016). In terms of incidents, the main focus is on predicting rather rare events rather than mass crimes. In fact, there is no need for sophisticated mathematical instruments to predict that shoplifting occurs rather frequently in large department stores in city centres; higher mathematics is also not necessary to predict drug transactions in the (geographically manageable) surroundings of various main railway stations in Germany.

In particular, different degrees of the threat of terrorist violence are displayed in different colours in many countries since 9/11 and, according to official announcements, refer to data and data analysis which are obviously intended to help determine the degree of terrorist threats, but which are not disclosed (for reasons of secrecy). Predictions coming with less secrecy were presented by amok researchers who interpreted so-called leaking, i.e. the announcement of extreme violence, in particular in social media, as a central variable of (explanation) and predictability (Heubrock et al. 2005). After all, the historical legislator has already put the announcement of severe violence under the threat of punishment in wise foresight of the findings of recent amok research (§126 StGB).

The prediction of crime is closely linked to the question of space and time, i.e. where and when certain criminal offences will occur. This is the focus of the approaches of predictive policing discussed and implemented today.

Risk assessment of individuals has a long history, as it is already part of the modern program of criminal law aimed at rehabilitation and the protection of legal interests and criminal sanctions, the imposition and method of enforcement of which are dependent on the risk of recidivism. This refers to predictive criminal law (or consequence-oriented criminal law) and predictive prison work or probation assistance, which in recent decades has increasingly been based on statistical risk assessment instruments, especially in the risk assessments of sexual and violent offenders. A methodically (and theoretically) sound attempt to identify high-risk individuals using standardized prediction instruments has, in contrast to other areas of criminal justice such as probation services or the penal system, only slowly developed in the police internationally. Thus, the Federal Criminal Police Office is now actually praising a standardized instrument for assessing the risk of violence among Salafists, which has been given the name RADAR iTE, and which, as far as the description permits a judgement, is more or less oriented towards conventional instruments of violence prediction such as the Violence Risk Appraisal Guide (VRAG). The population to be assessed with RADAR iTE is likely to coincide to a large extent with the Salafists classified as high risks, who are under observation at the Joint Anti-Terrorism Centre or have been included in the Joint Anti-Terrorism File after an essentially qualitative

evaluation and classification by various intelligence services, police and judicial authorities. This is because §2 of the Anti-Terror Law basically only permits the inclusion of personal data where there are actual indications that these are members of terrorist groups and associations or are preparing for serious (terrorist) acts of violence.

Police authorities in various European countries, including Germany, have developed and implemented "risk control programs" (Gefährderprogramme) to varying degrees and with different structures and legal frameworks (Chalkiadaki 2017), although these programs did not become a prominent theme in public, political or professional discourses (cf. now the stocktaking on predictive policing in Gluba 2014, where risk control programs are not even rudimentarily mentioned). In this respect, it is also understandable that empirical research, in particular evaluation research, on risk control programs has remained limited. Risk control programs essentially correspond to the model of predictive policing, as it is now clearly visible and discussed in the burglary prediction programs which also contain elements of a "focused deterrence" (Braga and Weisburd 2012). However, the programs are not related to the prediction of incidents, but to the identification of individuals who are considered to be at particular risk of involvement in various forms of crime. Since the 1990s, risk control programs for career or multiple offenders (Lesmeister 2008), domestic violent offenders (Greuel 2009), sexual offenders (Koch-Arzberger et al. 2011), football hooligans (Albrecht 2006) and people with an affinity for terrorism (Antwort der Bundesregierung 2017) have been launched and implemented (Chalkiadaki 2017). These programs follow a preventative logic and are based, at least in relation to young career criminals, on a well-known distribution of crime, first reported by the Philadelphia Cohort Study, according to which the greater part of serious crime, and in particular violent crime, is committed by about 3% of the members of a birth cohort (Wolfgang et al. 1972).

Risk control programs consist of risk assessments and interventions adapted to them. They have been regulated in various ways in formal laws. These differences in legal forms are due to differences in data protection relevance and to differences in the interventions following the classification as dangerous individuals. As a consequence of the relevant case law of the Federal Constitutional Court, the Anti-Terror Data Bank and the Joint Anti-Terror Centre have been subject to detailed legal regulation (BVerfG, 1 BvR 1215/07 of 24.4.2013). Interventions following risk assessments are regulated for example for domestic violence in detail in the Protection against Violence Act and now for terrorist threats (beyond the measures contained in the Act on the Joint Counter-Terrorism Information System) in the Act on the Federal Criminal Police Office (inserted by Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes (Act on the Restructuring of the Federal Criminal Police Office Act), Bundestagsdrucksache 18/11163, Bundestagsdrucksache 18/11326) in §56 BKAG in the form of electronic monitoring of potential terrorists. This regulation is essentially modelled after the English "Terrorism Prevention and Investigation Act" 2011 (TPIA), but is much less differentiated, especially as regards the measures. The forerunner of the English TPIA had once (after 11 September 2011) introduced preventive detention for (foreign) individuals assessed to pose terrorist risks but who could not be deported or charged. The obvious collision with Art. 5

of the European Convention on Human Rights (and the English Human Rights Act corresponding to the Convention) then led to the lifting of preventive detention for individuals assessed to pose a terrorist threat and to a less intrusive regulation based essentially on electronic control and other surveillance measures, which now also targets "foreign terrorist combatants" and—unsurprisingly—is regarded as proportionate (Memorandum to the Home Affairs Committee 2016).

In contrast, the programs developed for young career offenders and football hooligans are not based on specific legislation, but on general police laws. In addition to retaining personal data in specific data banks and the classification of risks of violence, these lead essentially to general risk control measures, which are intended to trigger deterrence and general prevention (Braga and Weisburd 2006).

The risk control programs mentioned above are structured in a comparable way. They are assigned to police laws and the general goal of averting threats and dangers. In a first step, risk control programs are based on risk assessment and classification of individuals into different risk groups. The classification as a risk leads to the inclusion in a special police file and, in a second step, to the application of various standard measures aimed at observing and monitoring and seeking effective risk management. Individuals classified as risk are informed and warned that and why he or she is now under systematic and permanent observation and under what conditions surveillance will be terminated. In some cases, risk control programs are also linked to a case-handling strategy geared towards individuals instead of criminal offences. Accordingly, there is no assignment of cases to investigating officers on the basis of the type of criminal offence, but individuals at risk are assigned regardless of which criminal offences are committed. Monitoring of residence and placement under police surveillance can be part of standard measures of risk management. Individualized measures then may include temporary restrictions to enter a location, investigation of the whereabouts of offenders, addressing and advising former or potential victims or channelling data to other administrative bodies. In addition, some risk control programs are set up in cooperation with other authorities. The latter applies to juvenile and adolescent repeat offenders, for whom, in addition to measures based on police laws, in the event of the commission of criminal offences, acceleration of criminal proceedings and deterrent effects shall be realized (Lesmeister 2008).

While general "risk control programs"—oriented towards the risk of participation in crime and implemented since the 1990s—have actually received little attention (apart from the attention triggered by the Berlin Christmas market attack carried out by Amri who was—at the time of the attack—monitored through the Joint Counterterrorism Centre), the emergence of programs aimed at predicting and preventing crime was immediately accompanied by considerable media, public and political attention. Predictive policing initially aimed at the prevention of domestic burglary. Then, the approach became broader. It now also aims to identify potential victims of firearm violence (or homicide).

The media and politicians in particular are fascinated by the idea that the police could be given an instrument that would enable them to predict crimes in a way that can be combined with appropriate prevention measures (see only New York Times, Sending the Police Before There's a Crime, 16 August 2011). On the one hand, the

fascination is probably due to a certain inclination towards Hollywood films and the public susceptibility they promote. On the other hand, the fascination is also fuelled by stories about "Big Data". This includes also the story of Walmart, a company that obviously—inspired by data mining—now not only places more water and adhesive tape (understandable) on the shelves on the occasion of certain weather forecasts, but also more strawberry tarts (not immediately comprehensible, see for example Pearsall 2010, p. 16). Added to this is the firm belief in the capacity of mathematical solutions and the effectiveness of "information technology" in addressing social problems (cf. only IJIS Institute 2015; see also the summary provided by van Brakel and de Hert 2011) as well as the still significant appetite for large amounts of data in security and police organizations, which can now obviously be used for the common good and for the identification and prediction of focal points of crime (Bogomolov et al. 2015). Finally, rumour has it that such math-based approaches (or algorithms) have led to significant reductions in crime. The Bavarian State Criminal Police Office (Bayerisches Landeskriminalamt 2015, p. 16) reports a "decline of approx. 30%" (of the number of domestic burglaries after the introduction of Precobs in Zurich), but could also have commented on the dramatic decline in domestic burglaries in Munich between the end of the 1980s and 2010 from approx. 3500 to about 800, a decline of about 80% (admittedly related to a period of about 20 years, but without the use of Precobs, Bayerisches Landeskriminalamt 2015, p. 15). In this respect, empirical studies and theoretical explanation of the decline (not only) in domestic burglaries during this period should come first. Something must have triggered and promoted the initially quite drastic decline in burglary, on the one hand, and the still relatively modest increase from 2010, on the other. For some, "predictive policing" has even brought about the end of crime and the prospect of a world without crime (Merz 2016, p. 1). Such visions are, of course, still opposed by Émile Durkheim's still convincing theoretical argumentation, which proceeds from the normality of crime as a basic prerequisite of normatively structured human societies.

In the 1990s, the implementation of Compstat in New York in particular was associated with the decline in serious violent crime (but also property crime) that began at the same time (Willis 2003; Ferguson 2012, p. 326). And, as expected, the use of large amounts of data and the merging of different data sources have led to issues of protection of personal data and privacy (American Civil Liberties Union et al. 2016); predictive policing and the classification of individuals as dangerous also lead to constitutional and criminal procedural issues (Ferguson 2012; Koss 2015). In view of the debate about deadly police violence that has repeatedly flared up in the USA in recent years, the question is finally asked whether and to what extent such a strategy does promote police practices that further intensify the degree of criminal-law-based social control that is already particularly pronounced for marginalized social groups and ultimately results in racist profiling (Saunders et al. 2016, p. 367; Shapiro 2017). It is therefore advisable to pay special attention to the occurrence of systematic (and discriminatory) distortions in the use of certain algorithms (Babuta and Oswald 2019; Obermeyer et al. 2019).

In North America at least, the Compstat approach of a new police organization and above all the development of data-driven police strategies to reduce crime has largely prevailed since the 1990s. On the other hand, however, specific

predictive software is at that time not yet available. The beginning of the adoption of predictive policing approaches is dated to the end of the last decade (Perry et al. 2013, p. 4). Specific programs have so far been implemented in connection with property offences (burglary crime) and violence. In Europe, predictive policing has attracted attention mainly in England/Wales, then in Switzerland and subsequently in various police authorities in German states and have now led to projects aimed at exploring the potential of algorithms developed commercially or in-house.

A fundamental assumption of policing aimed at prevention of crime refers to the predictability of crimes, especially violence, an issue to which criminology, forensic psychiatry and psychology have devoted themselves for at least 100 years. On the one hand, it is assumed that the individual risk of committing certain crimes can be determined on the basis of actuarial instruments. Furthermore, the assumption is found here that criminals are also characterized by "habit" and therefore tend to repeat successful crimes. In addition, it is assumed that criminals tend to repeat crimes in the immediate (geographical) environment and at the same time as the previous crimes (Koss 2015, p. 302). On the other hand, it is assumed that risk profiles and certain patterns can be used to extract information from large amounts of data about persons and places through whom or where crimes are committed. In contrast to risk control programs, which focus on persons who have already appeared as criminals and which are based on the concentration of (serious) crime in a group of few (career) criminals, analysis tools geared to still unknown persons or possible crime scenes refer to the assumption that future offenders and crime scenes can be identified. On the one hand, this is associated with the initially not easily plausible hypothesis that criminals repeat the same crimes frequently and, above all, commit them in the same place or in the vicinity of the last crime. On the other hand, the identification of as-yet-unknown persons requires valid risk profiles, which will hardly be possible, especially in the case of rare events (where the problem of high numbers of false positives turns up, see Munk 2017). The situation may be different where criminal events occur frequently. An example here can be drawn from a 2017 case of repeated domestic burglaries. Hessian police arrested that year an individual suspected of 900 domestic burglaries (Spiegel Online 11.05.2017, Hundreds of burglaries—suspects captured). The suspect also looks back on a history of at least 1200 other officially recorded domestic burglaries for which he had already been convicted in 2004. However, its geographical reach extended across three federal states, which is not surprising given the simultaneous lack of residence. In contrast to this individual performance, a report by the Munich police almost fades away. In this report, it is assumed that a group of offenders who were active across borders was responsible for every fifth burglary in Germany 2017 (Zeit Online, 22 May 2017). In this respect, it should come as no surprise that when highly active persons or groups are detained and thus incapacitated, a more or less significant reduction in crime can be achieved for certain spaces (and times). These particularly active persons and groups are only marginally visible in the qualitative research results of the Kriminologisches Forschungsinstitut Hannover in a study on domestic burglars,

obtained from interviews with foreign offenders serving time for burglary in German prisons (Wollinger and Jukschat 2017, pp. 65ff).

However, assumptions about specialization obviously cannot be generalized. Life history research and research on criminal careers indicate that little specialization occurs in criminal careers (Williams and Arnold 2002, p. 2ff). If specialization occurs, it is precisely in a limited circle of property or property offences or transaction crimes (such as drug trafficking). Particularly in the area of property crime, and even more so in white-collar crime, business models are being developed which—like all useful business models—are expected to be repetitive. Various forms of larceny by trick bear witness to this as well as Nigeria fraud schemes, Ponzi systems or even the burglary of flats and other forms of theft, which are assumed to contribute disproportionately to property crime in an organized manner and with only a small group of perpetrators. In this respect, it is surprising that only recently have so many expectations been placed on an observation which, now referred to as "near repeats", expresses (no more, but no less) than that when one of the persons or groups mentioned above is active in a region, the probability increases that (in the same region) further burglaries will occur. And: the statistical evidence that houses on the same side of the street as those that have been broken into have a somewhat higher risk of being the victim of a burglary than houses on the opposite side (Bowers and Johnson 2005) is neither unexpected in view of human laziness nor suitable for the design of preventive measures. "Near repeats" simply depict, at least in part, business models, the emergence, adaptation and continuation of which should probably not be regarded in terms of parallels to the foraging of chimpanzees (Johnson 2014; Chainey and da Silva 2016). For the business models mentioned will tend to differ depending on social, economic and cultural conditions (see for example Chainey and da Silva 2016).

In this context, however, the focus of interest of Western European police today is rather on highly mobile criminal groups (or individual perpetrators) who change their activity areas at short intervals and also proceed across borders (WODC 2016). Moreover, these are said to have contributed considerably to the increase in burglary figures in various countries of the European Union. But, rapid exchange of and replacement of offenders, considerable mobility and limited data exchange between police authorities ultimately result in serious limitations as regards attribution of offences to offender groups (WODC 2016, p. 80). Furthermore, it can be assumed that here—comparable with other forms of transaction crime—replacement effects occur with regard to imprisoned actors or actors who have left the country again (WODC 2016, p. 81). Obviously, in this context—and rightly so—more preventive potential is seen in approaches that serve more to identify criminally particularly active persons and groups (WODC 2014), i.e. correspond to conventional risk control programs and are furthermore not based on predictions but on observations.

In contrast, the attempt to predict serious (terrorist) violence faces a different problem. This problem arises from the rarity of the event to be predicted. As a result, valid risk profiles cannot be developed (Munk 2017).

4 Data, Security and Protection of Privacy

Data collection, data retention and data analysis for purposes of crime control and security are embedded in a normative system of data and personality protection. In addition to national constitutional and data protection law, the protection of personal data is also governed by European Union law and the European Convention on Human Rights. The security-driven demand for large and unselected data collections has given rise to a field of conflict that has in the last decade become apparent, in particular, in the retention of telecommunications data introduced by Directive 2006/24 EC and then in the bulk meta data collection programs of the US National Security Agency (disclosed by Snowden). The decision of the European Court of Justice (Judgment of the Court (Grand Chamber) in Joined Cases C 293/12 and C 594/12) issued on 8 April 2014, however, found that Directive 2006/24 EC violated the European Charter of Fundamental Rights and was therefore null and void overall.

The Court first of all emphasizes that Directive 2006/24 EC entails general retention of all telecommunication traffic data and thus interferes with the fundamental right to privacy and the right to the protection of personal data (Art. 7, 8 of the European Charter of Fundamental Rights) without individuals concerned giving a concrete reason for retaining their data. This interference affects indiscriminately (almost) all persons living in member states of the European Union and the right to privacy protected by Article 7 of the Charter of Fundamental Rights (for the privacy properties of meta data see Mayer et al. 2016). The simultaneous interference with the right to data protection (Art. 8) is placed in connection with intrusion into the right to privacy. According to the Court, the protection of personal data is of particular importance for the right under Article 7 of the Charter of Fundamental Rights (European Court of Justice (Grand Chamber), Judgement as of 8 April 2014, in Joined Cases C-293/12 and C-594/12, No. 53). The Luxembourg court repeats here a statement of the European Court of Human Rights, which in its decision M. K. v. France (Application no. 19522/09, Judgement as of April 18, 2013, No. 32) also assumes that the protection of personal data is of outstanding relevance for the right to privacy under Art. 8 ECHR and that therefore the state is obliged to ensure effective protection of personal data against any use which cannot be reconciled with Art. 8. The need for protection is set higher in the case of automated data processing and processing for security and criminal justice purposes.

The European Court of Justice considers that data retention is, in principle, a necessary and appropriate means of furthering the prosecution of serious crime and of ensuring the prevention of serious dangers. Data retention is assessed to be necessary because of the outstanding importance of the fight against organized crime and terrorism for public security, and investigation methods based on telecommunication traffic data are assumed to make a considerable contribution to this (European Court of Justice, Judgement in Joined Cases C-293/12 and C-594/12), No. 51). The argument put forward in the submissions that the allocation of traffic data to specific persons could be undermined in various ways

is only briefly dealt with. According to the court, anonymous communication is certainly possible, but this does not make data retention completely unsuitable.

Both the European Court of Justice (Luxembourg) and the European Court of Human Rights stress the importance of efficient investigation and information gathering methods for security and for the prosecution of serious crime. It is therefore not a question of the legitimacy of covert information gathering and access to telecommunications data; this is not doubtful. Rather, it is a question of how an appropriate balance can be struck between the interest in security and effective prosecution on the one hand and fundamental rights on the other. In its decision of 8 April 2014, the Luxembourg Court relied on the case law of the European Court of Human Rights, and in particular on two decisions, Marper v. United Kingdom (2008) and M. K. v. France (2013), to answer the question of how interests should be weighed and balanced. In both cases, the question was under which conditions personal data could be included in police information systems (used for prevention and investigation). In the case of Marper v. United Kingdom, the inclusion of DNA profiles in the English DNA database was disputed. In the case of M. K. v. France, it was the inclusion in the fingerprint database of the French police authorities that was dealt with by the Strasbourg court. Both cases did not concern the usefulness of fingerprint files or DNA databases for law enforcement purposes. This was as uncontroversial as the legitimacy of the objective of retaining the data, namely effective prosecution. The question was what the conditions would be for the data to be retained and what reason could justify the inclusion of a person's DNA or fingerprints in the databases. In both cases, persons had been included in the files for whom there was suspicion but no conviction. In the case of M. K. v. France, the Court stressed that the purpose of the database was to maximize the number of fingerprints (ECHR, M.K. v. France, (Application no. 19522/09), Judgement as of 18. April 18, 2013, No. 36). The Court also dealt with the French authorities' objection that the recording of fingerprints was also a way of establishing the innocence of suspects and thus in the interest of the person registered. In that regard, the Court held that, if such an argument could be accepted, the storage of information on the entire French population could be justified. However, according to the court, the storage of data on all inhabitants and without cause would clearly be "excessive and irrelevant" (ECHR, M.K. v. France, No. 37). As a result, in both cases the Strasbourg court considered the mere suspicion of an offence as insufficient to strike a balance between the interest in effective prosecution and the interest in the protection of privacy (Article 8 ECHR).

Now, the parallel in the decisions Marper v. United Kingdom and M. K. v. France on the facts underlying the storage of telecommunications metadata is on the one hand obvious, on the other hand differences also become apparent. In the case of fingerprints and DNA profiles, information systems are managed by police authorities and data are collected by law enforcement authorities. Metadata storage, on the other hand, is carried out by telecommunications companies and in the private sector. Telecommunications metadata, fingerprints and DNA profiles concern personal data whose potential to interfere with fundamental rights is undisputed. However, the potential interference with communication metadata goes further than with fingerprints and DNA profiles. The latter can essentially only be used to identify a person (if DNA profiles are limited to non-coding parts of DNA). Metadata, on the other

hand, allows considerable and very accurate insight into a person's habits, movements and social and professional contacts. The main difference is that telecommunication metadata are necessarily generated by using communication devices (and can be retained by telecommunication companies) during the course of communication processes. Fingerprints and DNA profiles, on the other hand, require intervention by police or other investigating authorities. They are not generated quasi-automatically (apart from the fact that people leave traces in the form of fingerprints or DNA tests of accessible material), but require a legally justified selection criterion from the outset, which will usually coincide with criminal suspicion. In the case of DNA databases and fingerprint files, it is a question of gradually building up information systems (which, as the ECHR stated, is characterized by the objective of expansion). In the case of the retention of metadata, the aim is to preserve the data generated and keep them for security and law enforcement purposes.

However, it cannot make any difference whether data is held by telecommunications providers or police. It depends solely on who initiated compulsory data retention and who can access and use the data. Since state requirements, including sanction threats, justify the storage obligation of telecommunications companies and the sole use is intended for averting danger and criminal prosecution, data retention is attributable to the state. Furthermore, the collection of metadata must also be treated as if it had been collected by state authorities. If, due to flat rates or prepaid communication, there is no reason for telecommunications companies to collect traffic data and if billing purposes do not require traffic data retention, the obligation to retain the data for security and criminal justice purposes must be subject to a proportionality test provided for in Art. 15 of Directive 2002/58/EC (Directive on privacy and electronic communications). Here, also the question arises whether the standards developed by the Strasbourg Court for DNA databases and fingerprint files should also be applied to the retention of telecommunications metadata.

The European Court of Justice (Luxembourg) obviously and rightly assumes the applicability of these standards. In particular, the Court points out that, although the aim of retention is to combat serious crime and prevent serious dangers, the retention rules do not require any link between the data retained and a particular geographical region, time period or group of persons exhibiting particular risks which could provide for a reasonable ground for retention. This consideration suggests that the court may be more inclined towards a procedure similar to quick freeze (although the term is not mentioned in the grounds given in the judgment).

In dealing with the question of proportionality, the European Court of Justice does not address the effectiveness of data retention in the grounds of the application. The Court contents itself with brief remarks on necessity and appropriateness, whereby the practically existing possibilities to undermine data retention purposes are not regarded as legally relevant. However, this is not convincing from the perspective of an effective proportionality test. For example, the German Federal Constitutional Court points out that it is precisely when interference with fundamental rights is at issue, the effects of which are not yet known to the legislature and can only be very roughly estimated, that it is incumbent upon the legislature to initiate evaluation research and then, depending on the results, to make appropriate amendments to the laws (Bundesverfassungsgericht, Judgement, March 3, 2004—1

BvR 2378/98, 1 BvR 1084/99). In this respect, evaluation research is an important element in the implementation of the principle of proportionality. The legislature is initially entitled to a margin of appreciation, which is caused by uncertainty in the assessment of efficacy. In return, however, the legislature must ensure that this uncertainty is reduced or, if possible, even eliminated altogether.

Before the adoption of Directive 2006/24/EC, there was little systematic and independent research on the use and consequences of telecommunications metadata for prevention and investigation of serious crime in Europe (Albrecht et al. 2008; Albrecht 2011). Directive 2006/24/EC indeed required explicitly an investigation into the effectiveness of data retention in combating organized crime and terrorism. However, the 2011 evaluation report revealed little that could be used to assess the effectiveness of data retention. The incomplete data do not even provide an answer to the question of how often traffic data were used for the purpose of investigating crime. The latest statistical report of the European Commission, published in accordance with Article 2 of Directive 2006/24/EC, states that in about 2.5 million cases retained data have been accessed by law enforcement bodies. However, the data provided by the Member States do not permit such a statement, as the report itself explains. Obviously, the member countries have supplied different types of data. According to European Commission statistics, in 2012 in almost 2.5 million cases retained metadata were retrieved from telecommunication providers. However, two countries alone account for about 92% of the reports (England/Wales and Poland), with one country, Poland, accounting for two thirds of all cases (European Commission 2013, p. 16). The conclusion is simple: a meaningful interpretation of such statistics is not possible (Guild and Carrera 2014).

It should also be noted that the Directive does not provide for precise requirements regarding access to and retrieval of retained data. No restrictions apply in terms of, for example, seriousness of the offence, need of a judicial warrant or security organizations which may have access to retained data. Finally, the European Court of Justice emphasized that the duration of the retention period also requires precise regulation and cannot remain in the setting of a general target between "6 months and two years". With regard to the fundamental right to the protection of personal data, and this corresponds to the decision of the German Federal Constitutional Court, the special need for protection of traffic data recorded over a longer period of time is underlined and it is demanded that special data protection regulations, which above all also include the conditions of deletion, are therefore indispensable. In addition, a valid directive must already stipulate that retained data must remain within the territory of the European Union and may not be outsourced.

In joined cases C-203/15 (Tele2 Sverige AB v Post-och Telestyrelsen) and C-698 (Secretary of State for Home Department v Tom Watson and Others) of 21 December 2016, the European Court of Justice has ruled that European Union law (after Directive 2006/24 EC was declared to be null and void) precludes national legislation of member countries from general and indiscriminate retention of telecommunication traffic data using the same argumentation as in the judgment of 2014. The Court stresses again that—in order to comply with fundamental rights of privacy and data protection—a relationship between retained data and a threat to public security is required. Data retention may be permitted on the basis of Art. 15 (1)

Directive 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector) as a preventive and investigative measure in the fight against serious crime, but must be targeted in terms of a particular time period, a geographical area or groups of persons. In face of these requirements, it seems clear that German telecommunication data retention law, reintroduced as "retention light" in 2015 (but suspended due to several administrative courts' decisions), will not comply with European law. However, the German Federal Administrative Court of Justice recently has requested a preliminary ruling of the European Court of Justice (Bundesverwaltungsgericht 2019) on the question whether Art. 15 (1) Directive 2002/58/EC will "under no circumstances" allow indiscriminate data retention or whether strict and restrictive regulation of data protection and access to retained data might create interpretative room for allowing "retention light".

After all, the decisions of the European Court of Justice have set quite high thresholds for a new edition of Directive 2006/24/EC as for national legislation on bulk telecommunication traffic data retention. The real challenge lies in the indication that the Directive should provide for restrictions by specifying "targets" (in terms of space, time, groups, individuals) of data retention. Such a restriction is probably only feasible with an extended "Quick Freeze" regulation.

5 What Do We Know About the Results of Predictive Policing?

The introduction of specific predictive software, related organization of the police and implementation of interventions based on predictions are accompanied by high expectations not only in Germany (cf. only Heitmüller 2017). These expectations concern a significant reduction in certain forms of crime and not least the prevention of serious (terrorist) violence. This expectation requires a certain change in perspectives. This is because conventional crime prevention research has always been interested in recidivism rates (and in a comparative analysis of recidivism rates for different forms of criminal sanctions), which is quite understandable in the wake of modern criminal law. The concepts of predictive police and policing, however, are oriented towards the goal of reducing crime by preventing crime.

In Germany, evaluation research on risk control programs and predictive police has so far only been carried out in isolated cases. An evaluation of various risk control programs implemented by police of North Rhine-Westphalia focusing on young career offenders led to evidence of reduced crime participation in a comparison of program participants and control groups (Bliesener et al. 2010, p. 184). However, these were relatively small groups on the one hand, and the research design included only a short probation period on the other. Finally, due to a lack of data, not all potentially relevant variables (in particular detention periods) could be controlled. The question of reducing crime rates in the areas covered by the risk control programs was not raised. Rather, it was probably assumed that a lower participation of career offenders in crime would lead to corresponding reductions in the overall crime load.

The evaluation of a predictive policing project aimed at potential victims in Chicago then led to disputes. This project was concerned with the prevention of the use of firearms and homicides on the basis of the identification of persons who had been classified as particularly at risk of becoming victims of homicide (Saunders et al. 2016). These were predominantly young African-American men (Saunders et al. 2016, p. 358). The intervention—no targets were set—probably consisted essentially of "more frequent contacts" by the police with the "endangered" (who, however, could simultaneously pass as suspects; Saunders et al. 2016); thus, a conventional risk control program was implemented, about 20 years after the first programs were launched in Germany. A special effect in the form of the reduction of homicide could not be proven with a quasi-experimental design (and for version 1 of the risk assessment instrument). The outcome of the program was not really surprising: a higher probability of persons on the list of possible victims of homicide being arrested for firearms offences (Saunders et al. 2016, p. 365). Chicago's police were not very pleased with this result and responded quickly by pointing out that a more advanced version of the assessment instrument was now in use, with which—it was suggested—Chicago police could achieve better results (Johnson and Guglielmi 2016). In view of the still manageable risk of fatal violence even for members of violent gangs in Chicago, which of course is at least 0.7% per year and thus 233 times the risk of the ordinary Chicago resident, and the observation that of the 405 persons killed in Chicago during the period under study, 3 were on the list of persons classified as particularly at risk (Saunders 2016), the question then arises whether there is any realistic prospect of at least perceptible preventive effects through an improvement in prediction and, in particular, intervention.

Previous studies on the effectiveness of "predictive policing", corresponding software and interventions based on them have been limited and have so far provided no evidence that these approaches were superior to conventional methods of police work and that they could have significantly prevented crimes (Hunt et al. 2014; Moses and Chan 2016; Gerstner 2017).

Little is known about the effectiveness of data bulk data retention for the prevention and investigation of serious crime. This applies to retention and analysis of telecommunications traffic data and air passenger data. Furthermore, there is still controversy as to whether the bulk surveillance of telecommunication, as used by intelligence services, can prevent terrorist violence. Particularly in the area of anti-terrorism strategies, it is noticeable that evaluation research has so far been almost completely lacking (Lum et al. 2008; Bellasio et al. 2018). However, optimistic reports from security authorities and policymakers are opposed here by rather cautious statements from research. The examination of cases that are used as evidence of the effectiveness of mass surveillance measures shows, in any case, that the triggers of interventions that then led to the arrest of persons suspected of terrorism (and thus possibly to the prevention of terrorist violence) can be found predominantly in conventional investigative approaches (Jonas and Harper 2006; Bergen et al. 2014; Houston 2017).

However, this also reveals the problem already mentioned above of developing suitable methodological approaches for proper evaluation of assessment and prediction tools aimed at identifying risk patterns or profiles (van Uma and Pisoiu 2015).

The same applies to the development of valid approaches for determining the risk of terrorist violence in individual (already known) persons (either in the form of determining the risk of relapse into terrorist violence or assessing the risk of terrorist (or other violence) in security checks before recruitment in certain occupational areas, Monahan 2011; RTI International 2018). In this respect, the response of the Federal Government to an inquiry in the German Bundestag on the results of investigating bulk air passenger data is not surprising. In addition to the confession that it was not possible to answer the question as to the extent to which the transmitted data subsequently contributed or will contribute to the prevention/prosecution of criminal offences, it was pointed out that 514 hits followed from matching a total of 31,617,068 PNR data records with police data (Federal Government's answer 2019, p. 5). Thus, out of ca. 60,000 data records one turns out to be relevant for policing purposes. However, this small outcome is further relativized by the type of hits. The hits concern 57 individuals with arrest warrants, 76 persons under open and covert observations and 381 residence investigations. These cases, in turn, are linked to 27 terrorism-related offences and 482 offences that fall under the category of other serious crime which, however, is defined as offences with a maximum sentence of at least three years imprisonment (so, ultimately insults and damage to property are not eligible).

Acknowledgements Open access funding provided by Projekt DEAL.

References

Albrecht H-J (2006) Fußball und Gewalt. Entwicklungen, Erklärungsansätze und Prävention. Monatsschrift für Kriminologie und Strafrechtsreform 89:158–174

Albrecht H-J (2011) Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten. Max-Planck-Institut für Ausländisches und Internationales Strafrecht, Freiburg

Albrecht H-J (2016) Der Rückgang der Jugendkriminalität setzt sich fort. Recht der Jugend und des Bildungswesens 64:395–413

Albrecht H-J, Grafe A, Kilchling M (2008) Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100 g, 100 h StPO. Duncker & Humblot, Berlin

American Civil Liberties Union et al (2016) Predictive policing today: a shared statement of civil rights concerns. August 13, 2016

Antwort der Bundesregierung (2017) Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Frank Tempel, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 18/11959, Deutscher Bundestag, Drucksache 18/12196, 18. Wahlperiode, 2. 5. 2017

Babuta A, Oswald M (2019) Data analytics and algorithmic bias in policing. Royal United Services Institute for Defence and Security Studies, London
Bellasio J et al (2018) Counterterrorism evaluation. Taking stock and looking ahead. RAND Europe, Cambridge
Bergen P et al (2014) Do NSA's bulk surveillance programs stop terrorists?. New America Foundation, Washington
Bliesener T et al (2010) Eine Prozess- und Wirkungsevaluation polizeilicher Konzepte zum Umgang mit jungen Mehrfach-/Intensivtätern in NRW. Universität Kiel, Kiel
Bogomolov A et al (2015) Moves on the street: classifying crime hotspots using aggregated anonymized data on people dynamics. Big Data 3:148–158
Bowers KJ, Johnson SD (2005) Domestic Burglary repeats and space-time clusters. The dimensions of risk. Eur J Criminol 2:67–92
Braga A, Weisburd D (2006) The effects of focused deterrence strategies on crime: a systematic review and meta-analysis of the empirical evidence. J Res Crime Delinq 49:323–358
Bundesverwaltungsgericht (2019) Pressemitteilung Nr. 66/2019 vom 25.09.2019. EuGH soll Vereinbarkeit der deutschen Regelung zur Vorratsdatenspeicherung mit dem Unionsrecht klären
Bureau of Justice Assistance (2013) Compstat: its origins, evolution, and future in law enforcement agencies. Bureau of Justice Assistance, Washington
Chainey SP, da Silva BFA (2016) Examining the extent of repeat and near repeat victimisation of domestic burglaries in Belo Horizonte, Brazil. Crime Sci 5:1–10
Chalkiadaki V (2017) Gefährderkonzepte in der Kriminalpolitik. Rechtsvergleichende Analyse der deutschen, französischen und englischen Ansätze. Springer, Wiesbaden
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2019) Tätigkeitsbericht 2017 und 2018. Silber Druck, Bonn
European Commission (2010) Communication from the Commission to the European Parliament and the Council of 22 November 2010—the EU Internal Security Strategy in action: five steps towards a more secure Europe COM(2010) 673 final
European Commission (2013) Statistics on requests for data under the data retention directive. DG Home Affairs, Brussels
European Commission (2016) Communication from the Commission to the European Parliament, the European Council and the Council, delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union. Brussels, 20.4.2016 COM(2016) 230 final
Ferguson AG (2012) Predictive policing and reasonable suspicion. Emory Law J 62:261–325
Gerstner D (2017) Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl: Evaluationsergebnisse zum Baden-Württembergischen Pilotprojekt P4. Freiburg: edition iuscrim
Gluba A (2014) Predictive Policing – eine Bestandsaufnahme. Historie, theoretische Grundlagen, Anwendungsgebiete und Wirkung. Landeskriminalamt, Hannover
Greuel L (2009) Gewalteskalation in Paarbeziehungen. Institut für Polizei und Sicherheitsforschung, Bremen
Guild E, Carrera S (2014) The political and judicial life of metadata: digital rights ireland and the trail of the data retention directive. CEPS, Brussels
Heitmüller U (2017) Predictive policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report. heise online, 17.04.2017
Heubrock D et al (2005) Prävention von schwerer zielgerichteter Gewalt an Schulen - Rechtspsychologische und kriminalpräventive Ansätze. Polizei und Wissenschaft 6:43–57
Houston T (2017) Mass surveillance and terrorism: Does PRISM keep Americans safer?. University of Tennessee, Knoxville
Hunt P, Saunders J, Hollywood JS (2014) Evaluation of the shreveport predictive policing experiment. RAND, Santa Monica, Washington
Institute IJIS (2015) Predictive analytics: a critical tool supporting evidence-based decision making. George Washington University, Ashburn
Johnson SD (2014) How do offenders choose where to offend? Perspectives from animal foraging. Legal Criminol Psychol 19:193–210
Johnson ET, Guglielmi A (2016) CPD welcomes the opportunity to comment on recently published RAND review. Chicago Police Department, Chicago
Jonas J, Harper J (2006) Effective counterterrorism and the limited role of predictive data mining. CATO Institute, Washington

Koch-Arzberger C et al (2011) Rückfallgefährdete Sexualstraftäter in Hessen. Hessisches Landeskriminalamt, Wiesbaden
Koss KK (2015) Leveraging predictive policing algorithms to restore fourth amendment protections in high-crime areas in a post-Wardlow World. Chic Kent Law Rev 90:301–334
Landeskriminalamt Bayerisches (2015) Erfahrungsbericht über die Machbarkeitsstudie „PRECOBS“ bei der Bayerischen Polizei. Landeskriminalamt, München
Landeskriminalamt NRW (2017) Forschungsbericht Wohnungseinbruchdiebstahl. Basisbericht. Landeskriminalamt, Düsseldorf
Lesmeister D (2008) Polizeiliche Prävention im Bereich jugendlicher Mehrfachkriminalität. Dargestellt am tatsächlichen Beispiel des Projekts „Gefährderansprache“ des Polizeipräsidiums Gelsenkirchen. Hamburg
Lum C, Kennedy LW, Sherley A (2008) Is counter-terrorism policy evidence-based? What works, what harms, and what is unknown. Psicothema 20(1):35–42
Mayer J, Mutchler P, Mitchell JC (2016) Evaluating the privacy properties of telephone metadata. PNAS 113:5536–5541
Memorandum to the Home Affairs Committee (2016) Post-legislative assessment of the Terrorism Prevention and Investigation Measures Act 2011. Home Office, London
Merz C (2016) Predictive policing—Polizeiliche Strafverfolgung in Zeiten von Big Data. www.abida.de/de/blog-category/dossiers. Accessed 1 Dec 2019
Monahan J (2011) The individual risk assessment of terrorism. University of Virginia School of Law: Public Law and Legal Theory Working Paper Series
Moses LB, Chan J (2016) Algorithmic prediction in policing: assumptions, evaluation, and accountability. Polic Soc. https://doi.org/10.1080/10439463.2016.1253695
Munk T (2017) 100.000 false positives for every real terrorist: why anti-terrorist algorithms do not work. First Monday 22 (9), peer-reviewed journal on the internet
Obermeyer Z et al (2019) Dissecting racial bias in an algorithm used to manage the health of populations. Science 366:447–453
Pearsall B (2010) Predictive policing: the future of law enforcement? Natl Inst Just J 266:16–19
Perry WL et al (2013) Predictive policing. The role of crime forecasting in law enforcement operations. RAND, Washington
RTI International (2018) Countering violent extremism: the application of risk assessment tools in the criminal justice and rehabilitation process. Literature Review. Research Triangle Park, North Carolina
Saunders J (2016) Pitfalls of predictive policing. U.S. News & World Report, October 7, 2016
Saunders J, Hunt P, Hollywood JS (2016) Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. J Exp Criminol 12:347–371
Schürmann D (2015) Predictive Policing als praxisorientiertes Projekt der Polizei NRW. www.bka.de/SharedDocs/…/kiforum2015SchuermannPositionspapier.pdf. Accessed 2 Nov 2019
Shapiro A (2017) Reform predictive policing. Nature 541:458–460
Tegner Anker AS, Doleac JL, Landersø R (2018) The effects of DNA databases on the deterrence and detection of offenders. The Rockwool Foundation, Copenhagen
Van Brakel R, de Hert P (2011) Policing, surveillance and law in a pre-crime society: understanding the consequences of technology based strategies. Cah Politiestud 20:163–192
van Uma E, Pisoiu D (2015) Dealing with uncertainty: the illusion of knowledge in the study of counter-terrorism effectiveness. Crit Stud Terror 8(2):229–245
Willis JJ et al (2003) COMPSTAT in practice: an in-depth analysis of three cities. Police Foundation
WODC (2014) Facilitating itinerant crime groups. Research synthesis. WODC, Den Haag
WODC (2016) Crossing borders on the trail of thieves. Research on facilitating itinerant crime groups based on fifteen criminal investigation studies in the Netherlands. WODC, Den Haag
Wolfgang M, Figlio D, Sellin T (1972) Delinquency in a birth cohort. Cambridge University Press, Chicago
Wollinger GR, Jukschat N (2017) Reisende und zugereiste Täter des Wohnungseinbruchs. Ergebnisse einer qualitativen Interviewstudie mit verurteilten Tätern. Kriminologisches Forschungsinstitut Niedersachsen, Hannover