'PREDICTIVE POLICING', 'PREDICTIVE JUSTICE', AND THE USE OF 'ARTIFICIAL INTELLIGENCE' IN THE ADMINISTRATION OF CRIMINAL JUSTICE IN GERMANY

By Johanna SPRENGER and Dominik BRODOWSKI[*]

Abstract

In ever more areas, it becomes evident that the transformative power of information technology – and so-called 'artificial intelligence' in particular – affects the administration of criminal justice in Germany. The legal framing of issues relating to the use of 'AI technology' in criminal justice lags behind, however, and is of high complexity: In particular, it needs to take the European framework into account, and has to cope with the German peculiarity that the prevention of crimes by the police is a separate branch of law, which is regulated mostly at the 'Länder' (federal states) level, while criminal justice is regulated mostly on the federal level. In this report, we shed light on the practice, on legal discussions, and on current initiatives relating to 'predictive policing' (1.), 'predictive justice' (2.) as well as evidence law and the use of 'artificial intelligence' in the administration of criminal justice (3.) in Germany.

1 'Predictive Policing' in the Administration of Criminal Justice in Germany

German Law does not provide for a legal definition of the term 'predictive policing'. When focusing on the most characteristic function of 'predictive policing', the description 'prediction-based police-work'[1] seems most suitable because it stresses the prognostic element of predictive policing, while not strictly excluding forms that do not entail highly advanced or intelligent technology.[2] Further definitions used are, for example, 'tech-based analytical procedures aiming to predict the probability of future offences, offenders or crime scenes'[3] as well as 'computer-assisted method for spatially

[*] Johanna Sprenger is a legal officer with the Federal Ministry of Justice; all views reflected in this article are her own. Dominik Brodowski is Professor of Criminal Law and Criminal Procedure, Saarland University, Saarbrücken, Germany, and is secretary of the German AIDP national group.

[1] Simon Egbert, 'Siegeszug der Algorithmen? Predicive Policing im deutschsprachigen Raum' [2017] APuZ 17, 19; Jörg Eisele and Kristine Böhm, 'Potential und Risiken von Predictive Policing' in Susanne Beck, Carsten Kusche and Brian Valerius (eds), *Digitalisierung, Automatisierung, KI und Recht* (Nomos 2020) 519; Tobias Knobloch, 'Vor die Lage kommen: Predictive Policing in Deutschland' (Stiftung Neue Verantwortung and Bertelsmann Stiftung 2018) 9 (translation to English by the authors).

[2] Hans-Heinrich Kuhlmann and Simone Trute, 'Predictive Policing als Formen polizeilicher Wissensgenerierung' [2021] GSZ 103, 104 (translation to English by the authors).

[3] Ines Härtel, 'Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren' [2019] LKV 49, 54 (translation to English by the authors).

based probability calculations of crime'[4], which is focused on probable crime scenes, while the term 'automated generation of suspicion'[5] seems to be slightly better suited to describe techniques focused on probable offenders (even though not necessarily limited to them). It is noteworthy that systems used by private companies as part of their compliance infrastructure are sometimes mentioned in the context of 'predictive policing' as well.[6] This concerns methods of automated fraud detection, or automated risk assessment systems regarding money laundering or insider training[7] – compliance methods which can include, very generally speaking, risk detection models similar to the ones used by the police or regulatory bodies. For the purposes of this report, however, 'predictive policing' is understood as methods applied by state authorities.

1.1 Description of AI systems used in Germany for 'Predictive Policing'

1.1.1 Geospatial systems

Approaches on 'predictive policing' that aim to identify probable crime scenes are, or at least have been for the last years, the most prevalent type in Germany. These predictive software systems are used in order to determine the probability that certain offences, mostly residential burglaries, will be committed within a certain local area. They work theory-based, ie under the criminological assumption that some types of crime occur in certain patterns, that rules can be derived from these patters, and that these rules can then be applied to the available data through the respective software.[8]

(1) PreCobs

'PreCobs' (Pre Crime Observation System) by 'Oberhausener Institut für musterbasierte Prognosetechnik GmbH' is a commercial predictive software and the first one that has been used in Germany. The software is said to be comparable to the US-American

[4] Kai Seidensticker, 'SKALA – Predictive Policing in North Rhine-Westphalia' (2021) 21 European Law Enforcement Research Bulletin 47, 48.

[5] Alexander Baur, 'Maschinen führen die Aufsicht', [2020] ZIS 275, 277; Timo Rademacher, 'Verdachtsgewinnung durch Algorithmen. Maßstäbe für den Einsatz von predictive policing und retrospective policing' in Daniel Zimmer (ed), *Regulierung für Algorithmen und Künstliche Intelligenz* (Nomos 2019) 229, 231 (translation to English by the authors).

[6] Lena Rutkowski, 'Predictive Policing am Arbeitsplatz' [2019] NZG 72.

[7] See the findings of a study by the Federal Financial Supervisory Authority (BaFin) regarding the use of Big Data Analysis and AI in regulatory compliance processes, 'Big Data trifft auf künstliche Intelligenz' (BaFin 2018) 76–78, 86–89 and advertising by software providers, eg Capgemini, 'Inventive FRC – Compliance' (2020) <https://www.capgemini.com/de-de/2020/09/inventive-frc-compliance-machine-learning/> accessed 9 August 2022.

[8] Thomas Wischmeyer, 'Predictive Policing, Nebenfolgen der Automatisierung von Prognosen im Sicherheitsrecht', in Andreas Kulick and Michael Goldhammer (eds), *Der Terrorist als Feind?* (Mohr Siebeck 2019) 193, 194; Franziska Lind, *Das raumbezogene Predictive Policing in Deutschland. Der aktuelle rechtliche Rahmen und seine Indikationen für Weiterentwicklungen des Einsatzes prädiktiver Analytik bei präventiv polizeilichem Handeln* (forthcoming).

system 'PredPol'. It aims to predict the probability of residential burglaries and applies the near-repeat theory, ie the assumption that with regard to certain types of offences, crime events are often followed by a subsequent event of crime in temporal and local proximity, especially in case of professional offenders.[9] The main prognostic feature of 'PreCops' is its assessment whether a burglary has been committed professionally.[10] The software has been in regular use by police departments in Bavaria since 2015/2016, [11] subject to a series of test runs of several months respectively in Baden-Württemberg from 2015 to 2018[12], and has been subject of a pilot project in Saxony/Leipzig from September 2019 to September 2020.[13] Notably, Baden-Württemberg has decided against further implementation of PreCobs in 2019. Bavaria decided as well to end its use for police work in 2021.[14] In both cases, the reasons were similar: there has not – or, as in Bavaria, not anymore[15] – been enough data available for the system to work efficiently.[16] In the course of this, efforts in Bavaria to enhance the software's functions to other types of offences, which was based on an alternative and more complex theoretical approach,[17] have come to a halt as well.[18]

In various federal states ('Länder') of Germany, predictive software models have been developed 'in-house' by the respective police departments:

[9] Silke Krasmann, and Simon Egbert, 'Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis' (final project report University of Hamburg 2019) 27–29.

[10] Simon Egbert, 'Predictive Policing als Treiber rechtlicher Innovation?' (2021) 41 Zeitschrift für Rechtssoziologie 26, 33.

[11] Knobloch (n 1) 14.

[12] Dominik Gerstner, 'Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany' [2018] European Journal for Security Research 115.

[13] *Polizei Sachsen* (Saxon Police Force), 'Archiv abgeschlossener Forschungsprojekte' <https://www.polizei.sachsen.de/de/79682.htm> accessed 9 August 2022.

[14] *Bayerisches Landeskriminalamt* (Bavarian State Criminal Police Office), 'Predictive Policing bei der Bayerischen Polizei' (press release 27 October 2021) <https://www.polizei.bayern.de/aktuelles/pressemitteilungen/018804/index.html> accessed 9 August 2022.

[15] Bavarian State Criminal Police Office (n 14).

[16] Nils Mayr, 'Strobl entscheidet sich gegen PreCobs' *Stuttgarter Nachrichten* (Stuttgart, 3 September 2019) <https://www.stuttgarter-nachrichten.de/inhalt.aus-fuer-die-einbruchvorhersage-software-strobl-entscheidet-sich-gegen-precobs.19a18735-9c8f-4f1a-bf1b-80b6a3ad0142.html> accessed 9 August 2022.

[17] Krasmann and Egbert (n 9) 29.

[18] Bavarian State Criminal Police Office (n 14).

(2) KLB-operativ

The prognostic system 'KLB-operativ' has been developed by authorities in Hessen and implemented in 2017. The software is now in use throughout Hessen.[19]

(3) KrimPro

Police authorities in Berlin (with some external support by Microsoft and Oraylis) have developed their system 'KrimPro' (KriminalitätsPrognose)[20] in 2016. KrimPro does not only use police data, but can also access publicly available data regarding the demographic structure and infrastructure. It is now being used not only in Berlin but also in Brandenburg and Saxony-Anhalt.[21]

(4) PreMAP

Lower Saxony began developing its software 'PreMAP' (Predictive Policing Mobile Analytics for Police) and started its use in 2017, successively expanding throughout the whole state of Lower Saxony.[22] Lower Saxony has since stopped its deployment, however, among other reasons due to its low cost/benefit ratio.[23]

KLB-operativ, KrimPro and PreMAP are based on the near-repeats hypothesis and focus on residential burglaries.

(5) SKALA

In North Rhine-Westphalia, the respective software system 'SKALA' (*System zur Kriminalitätsanalyse und Lageantizipation* – system for analysis and anticipation of crime) is in operative use since 2018 (starting with individual police stations in urban areas, and successively expanding to rural areas). It stands out due to various reasons. First, it is applied to predict not only residential but also commercial burglary and vehicle-

[19] *Hessisches Ministerium des Innern und für Sport* (Hessian Ministry of the Interior and Sport), 'Schwerpunkt-Fahndungsaktion: 564 festgestellte Straftaten und 84 Maßnahmen' (press release 25 November 2021) <https://innen.hessen.de/Presse/Schwerpunkt-Fahndungsaktion-564-festgestellte-Straftaten-und-84-Festnahmen> accessed 9 August 2022 and 'Jahresbilanz 2018', 12, 16 <https://innen.hessen.de/sites/innen.hessen.de/files/2021-10/jahresbilanz_2018_160119_web.pdf> accessed 9 August 2022.

[20] *Berliner Senatsverwaltung für Inneres und Sport* (Berlin Senate Department of Internal Affairs and Sport), LT-Drucks. (Berlin) 18/17562, 562.

[21] Stefan Löbel and Tino Schuppan, 'Potentiale und Herausforderungen einer neuen Datenorientierung im Kontext öffentlicher Aufgabenwahrnehmung' (2021) 16 Berichte des NEGZ 16–18.

[22] Kai Seidensticker, Felix Bode and Florian Stoffel, 'Predictive Policing in Germany' (University of Konstanz 2018) 4 <https://kops.uni-konstanz.de/handle/123456789/43114> accessed 9 August 2022.

[23] *Landeskriminalamt Niedersachsen* (Lower Saxony State Criminal Police Office), 'PreMAP – Predictive Policing (Vorausschauende Polizeiarbeit) in Niedersachsen' <https://www.lka.polizei-nds.de/startseite/kriminalitaet/forschung/premap/predictive-policing-in-niedersachsen-das-projekt-premap-114083.html> accessed 9 August 2022.

related crime; it is also under consideration regarding further types of crimes. Furthermore, it does not only rely on data regarding previous incidents of crime, but also on socio-economic data such as structural aspects regarding the population, rent and income structure, infrastructure and mobility opportunities within the respective area.[24] Additionally, its theoretical basis extends beyond the near-repeats hypothesis to further criminological and socio-scientific theories.[25]

1.1.2 Person-based 'Predictive Policing', individual risk assessments, and RADAR-iTE

While all of the systems mentioned above are still relatively similar to each other, the situation becomes much more complex regarding predictive methods that do not focus on probable local crime scenes but rather on probable offenders. 'Predictive policing' approaches aiming to apply individual risk assessments to natural persons are very rare in Germany. The coalition agreement of the parliamentary coalition forming the current German government indicates a very restrictive approach on such systems, as it states that the use of 'scoring' systems by state authorities shall be prohibited by EU law.[26]

As for now, the only system in Germany which is publicly known to focus on specific individuals and their respective risk potential appears to be 'RADAR-iTE' (*Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos – islamistischer Terrorismus* – rule-based analysis of potentially destructive perpetrators for an assessment of their acute risk – Islamist terrorism). RADAR-iTE is a risk-assessment tool developed by the *Bundeskriminalamt* (Federal Criminal Police Office) in cooperation with the Forensic Psychology Working Group of the University of Konstanz. RADAR-iTE serves to assess the risk that individuals – who have already been identified by the police authorities as potentially dangerous from previous law enforcement measures – are willing to commit acts of Islamist-motivated terrorism. It is used by police departments on the federal and Länder level since 2017 as a tool to assess the need for police interventions and to prioritise police resources. After evaluation, the system has been refined to its 2.0 version in 2019 according to scientific, ethical and legal aspects in cooperation with the University of Konstanz and the technical college for police in Saxony-Anhalt.[27] It evaluates both risk-increasing and risk-reducing factors. These

[24] Seidensticker (n 4) 52.

[25] Seidensticker, Bode and Stoffel (n 22) 5.

[26] Coalition agreement, lines 504–505 <https://www.wiwo.de/downloads/27830022/8/koalitionsvertrag-2021-2025.pdf> accessed 9 August 2022.

[27] Federal Criminal Police Office, 'RADAR (Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos)' <https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/Radar/radar_node.html;jsessionid=9AB1BDE4A134C483F1820378A09EAF6A.live612#doc142872bodyText4> accessed 9 August 2022; for a more detailed description Celina Sonka and others, 'RADAR-iTE 2.0: Ein Instrument des polizeilichen Staatsschutzes, Aufbau, Entwicklung und Stand der Evaluation' [2020] Kriminalistik, 386.

factors are provided in a form with question and answers categories that are completed (manually by police officers) on the basis of information that has already been gathered.[28] The system then calculates a risk factor on this basis and assigns it to one of two pre-defined risk-levels, either 'moderate' or 'high'.[29] Even though the calculation itself is processed automatically, it relies on a rather simple model based on the software Microsoft Excel.[30] The legal basis for RADAR-iTE is § 18 (3) in connection with § 18 (1) No 4, § 16 BKAG (Federal Criminal Police Office Act[31]) which does not mention the use of technology but only refers to the 'further processing of personal data' in case of indications that a person concerned is likely to commit a serious crime in the future.

So far, RADAR-iTE has been applied with regard to terrorism risks from the Islamist spectrum. Currently, the Federal Criminal Police Office, in cooperation with the Centre of Criminology and the technical college for police of Saxony-Anhalt, is working on an additional version of RADAR-iTE which focuses on terrorism risks motivated by right-wing extremism. The new version is planned to be made available for operative use in the course of 2022.[32]

1.1.3 Other forms of person-based predictive policing

Notwithstanding the restrictive approach towards individual risk-assessments mentioned above, there are now more and more algorithm-based prediction systems aiming to recognise patterns or other indicators for potential threats or potentially criminal behaviour of individuals not yet known to the state authorities. Some of them may not only aim to identify specific individuals but also dangerous objects or situations such as social media information that indicates tendencies of radicalisation.

(1) Passenger Name Records Data Analysis

The automated analysis according to § 4 (2) No 2 of the Act on the Processing of Passenger Name Record (PNR) Data to Implement Directive (EU) 2016/681 (PNR Act)[33] appears to be one of the most significant examples for person-focused predictive policing based on pattern recognition in Germany.

[28] For example, information on social integration (friends and family), access to weapons or explosive devices, military experience, trips to war or crisis zones, affiliation to radical groups, BT-Drucks. 18/13422, 5.

[29] The first version of the system provided a third risk level category 'noticeable', cf BT-Drucks. 19/12859, 9; for further explanation of the risk levels see BT-Drucks. 19/5648, 5 and 66.

[30] BT-Drucks. 19/1513, 7.

[31] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG), as amended.

[32] BT-Drucks. 19/32271; Federal Criminal Police Office (n 27).

[33] Unofficial translation available at <https://www.gesetze-im-internet.de/englisch_flugdag/index.html> accessed 9 August 2022.

The PNR Act obliges air carriers to transfer PNR data collected in course of their business (comprising up to 20 categories of data, see the list in § 2 [1] PNR Act) to the Federal Criminal Police Office. The Federal Criminal Police Office processes such data for automated advance checks – either before arrival or departure of the relevant flight – in order to identify individuals previously unknown to the police authorities for whom there is reason to believe that they have committed acts of terrorism or other serious crimes or will do so in the foreseeable future. In the course of these automated advance checks the PNR data are tested against certain databases or so-called 'patterns'. In case this results in a 'match', the Federal Criminal Police Office has to individually (ie by human officers) examine the results (§ 4 [2] 2 PNR Act) and may, if necessary, transfer the relevant data to other federal police or security authorities (§ 6 PNR Act).

Patterns indicating that an individual can be associated with terrorism or other serious crime could include incriminating criteria such as certain itineraries, layovers, payment methods etc. § 4 (3) of the PNR Act sets out basic rules governing the establishment of the patterns by the Federal Criminal Police Office in cooperation with its data privacy officer and other security and police authorities. In order to keep the number of individuals matching these patterns low, the incriminating criteria shall be combined with exonerating criteria. A person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation may not be used for the automated checks under any circumstances.[34] The Federal Commissioner for Data Protection and Freedom of Information shall review the production and use of the patterns at least every two years and report to the Federal Government every two years.

In 2018, the Federal Criminal Police Office began automated checks of PNR data, but limited against databases on persons or objects sought or under alert. In 2019, the German Government repeatedly announced that it did not yet operate advance checks against patterns and that it intended to do so at a later stage.[35] In 2020, all matches generated through advance checks of PNR data were still based on databases for persons or objects sought or under alert and not on checks against patterns.[36] By the time this report was finalised, it could not be confirmed whether automated checks against patterns had been put in place. Even though there is no further public information available on how the patterns are generated from a technical point of view, and how the respective advance checks will be operated in detail, the immense volume of data to be processed and the complexity of potential patterns makes the PNR system seem to be a typical use case for machine learning and big data analysis. This is also, as *Thüne* points out, indicated by the budget that has been assigned for the German PNR

[34] On the discriminatory potential, see **1.3.2** below.

[35] BT-Drucks. 19/10431, 3 and 19/12858, 3.

[36] Response of the Federal Ministry of the Interior dated 1 February 2021, BT-Drucks. 19/26440, 22.

system alone (initial costs of € 78 million and yearly costs of € 65 million).[37] Furthermore, § 4 (4) PNR Act allows the analysis of PNR data in order to produce or update patterns; this provides for a legal basis to use such data as training data for the generation of patterns by use of machine learning.[38]

The PNR system is subject to much criticism. Scholars,[39] human rights organisations[40] and the German Federal Commissioner for Data Protection and Freedom of Information[41] have complained about the general and indiscriminate nature of the transfer, automated checking and retention of PNR data affecting people without any link to the crimes the PNR system aims to prevent or investigate, the possibility of large numbers of false positives, the long retention period of PNR data (five years) and that it is – with regard to the automated checks – completely up to the administrative bodies to decide about the design of the patterns.

The legal basis for the PNR systems, meaning both the PNR Directive (on the EU level) as well as the PNR Act (on the national level), are currently being challenged in several civil and public administrative lawsuits and preliminary ruling procedures pending with the European Court of Justice (ECJ). The plaintiffs argue[42] that both the PNR Directive as well as the PNR Act are not in line with Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union in light of the rulings of the ECJ in the Digital Rights Ireland[43] and the Tele2 Sverige and Watson[44] cases as well as the ECJ's Opinion 1/15 of 26 July 2017 on the EU-Canada Passenger Name Record Agreement.[45]

A recent ruling by the ECJ promises good prospects of success for the plaintiffs. Upon referral by the Belgian Constitutional Court, the ECJ determined strict requirements on how the PNR Directive needs to be interpreted in order to be in line with Articles 7, 8 and 21 and Article 52 (1) of the Charter of Fundamental Rights of the European Union.

[37] Martin Thüne, 'Predictive Policing' (2020) 144.

[38] Lucia M Sommerer, *Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control* (Nomos 2022) 81.

[39] Clemens Arzt, 'Einladung zur anlasslosen Rasterfahndung durch das BKA' [2017] DÖV 1023.

[40] *Gesellschaft für Freiheitsrechte* (Society for Civil Rights), 'NoPNR: Keine Massenüberwachung am Himmel' <https://freiheitsrechte.org/nopnr-de/> accessed 9 August 2022.

[41] Federal Commissioner for Data Protection and Freedom of Information, '28th Annual Activity Report' (2019) section 6.4, 51.

[42] See for example the plaintiffs statement regarding Cases C-215/20 und C-220/20 <https://freiheitsrechte.org/home/wp-content/uploads/2020/09/GFF-Stellungnahme-an-den-EuGH-zur-FluggastdatenspeicherungPNR-Richtlinie-Sept2020.pdf> accessed 9 August 2022.

[43] ECJ, joined cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* ECLI:EU:C:2014:238.

[44] ECJ, joined cases C-203/15 and C-698/15 *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* ECLI:EU:C:2016:970.

[45] ECJ, opinion 1/15 on the *draft agreement between Canada and the European Union on the transfer of Passenger Name Record data* ECLI:EU:C:2017:592.

Among other quite significant aspects that might warrant adjustments to the German PNR Act in its current form, the ECJ sets important boundaries for the establishment of 'patterns' used for automated advance checks, in particular regarding machine learning: First of all, the ECJ held that member states may not operate AI systems using machine learning able to define or modify the criteria for the assessment without a human decision. In that regard, the ECJ warned against black-box effects. It stressed that any individual review of an automatically generated positive match depends on the possibility to understand the reason why the program generated a positive match. Furthermore, the ECJ sets out requirements for the pre-defined criteria in order to guarantee that the automated advance checks work in a non-discriminatory manner.[46] Given that it also recognises a high likelihood of false positives, the ECJ emphasised the importance of an individual, non-automated review of any positive match. According to the ECJ, member states are obliged to lay down clear and precise rules for such individual review and to ensure that the person concerned has an adequate understanding of the automated assessment in order to exercise their rights properly.[47]

(2) Hessen-Data and similar data analytics systems

Another project of Hessen that has attracted significant attention is the analysis system 'HessenData' which has been in use since 2017. HessenData might not (yet) qualify as 'predictive policing', but clearly has the potential to be used for predictive purposes. It is based on the Palantir software 'Gotham' and rapidly processes information from various heteronomous sources of police data (such as data from different police databases, data requested from communication service providers, data from communication surveillance measures or extracted from electronic devices seized by law enforcement authorities) in order to identify and visualise ('mapping') links and patterns.[48] Its purpose is to provide the police authorities with rapid information that can be used in order to plan police operations and deployment strategies. In contrast to the predictive policing tools mentioned above, the software does not suggest any conclusions or assumptions (eg as to a potential risk or suspicion of crime) based on these findings. The Hessian authorities further stress that the software does not by itself automatically collect and integrate data from external sources such as social media; instead, such data is otherwise retrieved by the authorities and can then be accessed by the system.[49]

[46] ECJ, case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:491 para 193–201.

[47] ECJ, case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:491 para 202–213.

[48] LT-Drucks. (Hessen) 19/6574, 17.

[49] LT-Drucks. (Hessen) 20/661, 3.

With § 25a of the Hessian Act on Public Security and Order (HSOG)[50], Hessen has introduced an explicit legal basis for HessenData limiting its use to the prevention of ('preventive fight against') those serious criminal offences listed in § 100a (2) of the German Act on Criminal Procedure (StPO)[51] or for the prevention of a danger of significant weight in justified individual cases. The provision explicitly allows to automatically identify affiliations or connections between individuals, groups, institutions, objects etc, to filter out irrelevant information and to statistically evaluate new findings and match them with known factual backgrounds. Furthermore, the decision to deploy or significantly change the software lies with the head of police, and before taking such a decision, the data protection officer needs to be consulted (without any veto rights, however).[52]

Meanwhile, other German Länder have also expressed their interest in the deployment of such a software, such as Hamburg which already introduced a legal basis identical to the one in Hessen,[53] or North Rhine-Westphalia which acquired the Palantir software and started using it for testing purposes in 2020.[54] Only recently, the legislator of North Rhine-Westphalia adopted a legal basis for operational use of the software.[55] Unlike the provisions that have been introduced in Hessen and Hamburg, North Rhine-Westphalia's provision does not restrict the use of the software to 'justified individual cases' but instead requires that its use is necessary for the prevention or preventive fight against serious crimes or of a danger of significant weight. Furthermore, the provision is missing the requirement of the head of the police or any other higher-ranking representative having to decide on the deployment or significant changes to the software, nor does it require to involve the data protection officer prior to such decisions. In contrast to the other two provisions it does, however, require the recording of each query.

[50] *Hessisches Gesetz über die öffentliche Sicherheit und Ordnung – HSOG*, as amended. On the German differentiation between such 'police laws' on the one hand, and criminal procedure on the other, see Dominik Brodowski, 'Alternative Enforcement Mechanisms in Germany' in Matthew Dyson and Benjamin Vogel (eds), *The Limits of Criminal Law* (Intersentia 2018) 365, 385–90.

[51] Unofficial translation available at <https://www.gesetze-im-internet.de/englisch_stpo/index.html> accessed 9 August 2022.

[52] For explanatory remarks on the legislative draft, see LT-Drucks. (Hessen) 19/6502, 40.

[53] Section 49 of the Hamburg Act on Data Processing by the Police (Gesetz über die Datenverarbeitung der Polizei – PolDVG), for explanatory remarks on the legislative draft see LT-Drucks. (Hamburg) 21/17906, 26.

[54] 'NRW-Polizei verteidigt umstrittene Palantir-Software' (*Zeit Online*, 3 May 2021) <https://www.zeit.de/news/2021-05/03/nrw-polizei-verteidigt-umstrittene-palantir-software?utm_referrer=https%3A%2F%2Fwww.google.com%2F> accessed 9 August 2022.

[55] Section 23 (6) of the North Rhine-Westphalia Police Act (Polizeigesetz des Landes Nordrhein-Westfalen – PolG NRW).

It is very likely that other Länder will follow, as Bavaria has also acquired the Palantir software at the beginning of 2022 under the umbrella of a framework contract that is said to cover the use by other state or Länder authorities as well.[56]

Even though in none of these cases the software is used to calculate a risk score to individuals, it seems to provide a technically very suitable basis where such preventive functions could later be built upon.[57]

The use of the software is heavily criticised.[58] Even though it processes only information which is already provided (somewhere) in police databases, it is – by definition – characterised by a very broad scope, without even requiring a concrete threshold like a concrete threat or suspicion of a crime.[59] It processes personal data without any preliminary indications whether or not there is a link between such data and the individual case at hand. Quite the contrary, one of its main characteristic features is to rapidly access thousands of personal data across various databases only to find out whether and where such a link might exist. Such an approach shows elements of a 'fishing expedition' within the relevant databases and therefore bears an undeniable indiscriminate effect. Furthermore, there is a lot of scepticism against cooperation with Palantir because of its links to US intelligence agencies and the political affiliations of the company's founder.[60]

[56] Werner Pluta, 'Bayerns Polizei bekommt Analyse-Software von Palantir' (*Golem*, 8 March 2022), <https://www.golem.de/news/big-data-bayerns-polizei-bekommt-analyse-software-von-palantir-2203-163691.html> accessed 9 August 2022; see also Clemens Arzt, 'Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr' in Matthias Bäcker, Erhard Denninger and Kurt Graulich (eds), *Handbuch des Polizeirechts* (7th edn, Beck 2021) mn 1305–1306.

[57] Markus Löffelmann, in his statement regarding the legislation draft for Section 25a HSOG describes predictive policing as its 'unspoken aim', page 107 of the committee document <https://hessischer-landtag.de/sites/default/files/scald/files/INA-AV-19-63-T1.pdf> accessed 9 August 2022; Sommerer, *Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control* (n 38) 81, describes HessenData as a 'precursor' to 'predictive policing', see also Krasmann and Egbert (n 9) 62–63 who predict a trend towards a 'one software fits all' approach including the 'platformisation' of data analytics, merging of different databases, and interoperability on several levels which allows police officers to pursue predictive work as well as data analytics for retrospective criminal prosecution.

[58] Marie Bröckling, 'Juristinnen kritisieren "Palantir-Paragraf" im geplanten Polizeigesetz' (*netzpolitik.org* 24 September 2019) <https://netzpolitik.org/2019/hamburg-juristinnen-kritisieren-palantir-paragraf-im-geplanten-polizeigesetz/> accessed 9 August 2022; Jannis Brühl, 'Palantir in Deutschland – Wo die Polizei alles sieht' *Süddeutsche Zeitung* (Munich, 18 October 2018) <https://www.sueddeutsche.de/digital/palantir-in-deutschland-wo-die-polizei-alles-sieht-1.4173809> accessed 9 August 2022.

[59] Arzt, 'Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr' (n 56) mn 1308.

[60] Pluta (n 56).

The legal basis for HessenData, § 25a HSOG, and Hamburg's corresponding provision are currently being challenged before the Federal Constitutional Court.[61] In October 2022, an additional constitutional complaint has been filed against the relevant law in North Rhine-Westphalia[62] – which had already faced harsh criticism in the course of the parliamentary debates.[63] A similar controversial debate has also started to unfold in Bavaria, whose Ministry of the Interior is still assessing whether or not it even recognises the need for a specific legal basis. In contrast, data protection advocates stress the need for specific regulations considering the intense infringements of fundamental rights the use of the software implies.[64]

(3) Intelligent video surveillance

It might be questionable whether or not intelligent video surveillance should be defined as 'predictive policing', as it does not provide any predictions but rather identifies dangerous situations and behaviours in certain locations.[65] It seems, however, difficult to draw such a clear line, especially since it is also clearly based on assumptions as to which situations or behaviours can lead to further escalations.

The first project where intelligent video surveillance went into operational deployment was initiated by the City of Mannheim. It installed a number of cameras in certain local focus-points, and connected them to an AI-based software. The software has been developed by the *Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung* (Fraunhofer Institute of Optronics, System Technologies and Image Exploitation)[66] and trained to identify dangerous behaviour and alarm law enforcement staff so that crimes can be prevented by early interventions. The first cameras were installed in 2018 at

[61] The complaint written by *Tobias Singelnstein* which has been supported by a group of organisations from the human rights and data protection sphere (Gesellschaft für Freiheitsrechte e.V. [Society for Civil Rights], Humanistische Union, Datenschützer Rhein Main and Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung) is available at <https://freiheitsrechte.org/home/wp-content/uploads/2019/07/2019-07-01-VB-Hessen-finalohneAdressen.pdf> accessed (9 August 2022).

[62] *Gesellschaft für Freiheitsrechte* (Society for Civil Rights, ‚GFF erhebt Verfassungsbeschwerde gegen uferlose Big-Data-Methoden im Polizeigesetz von NRW: Der Einsatz von Big Data braucht strenge Voraussetzungen' (press release 6 October 2022), <https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-stop-data-mining> accessed 21 October 2022; the full text of the complaint is available at < https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-NRW/2022-10-05-PolG_NRW_Palantir_Website_geschwaerzt_Punkte.pdf> accessed 21 October 2022.

[63] *Gesellschaft für Freiheitsrechte* (Society for Civil Rights), 'Stellungnahme' (28 March 2022) <https://freiheitsrechte.org/home/wp-content/uploads/2022/04/PolGNRW_Stellungnahme_GFF.pdf> accessed 9 August 2022.

[64] Elisa Harlan, Boris Kartheuser and Robert Schöffel, 'Analysetool der US-Firma Palantir: Schafft die Polizei den gläsernen Bürger?' (*Tagesschau*, 3 July 2022) <https://www.tagesschau.de/investigativ/br-recherche/polizei-analyse-software-palantir-101.html> accessed 9 August 2022.

[65] Kuhlmann and Trute (n 2) 107; arguing for a classification as predictive policing: Wischmeyer, 'Predictive Policing, Nebenfolgen der Automatisierung von Prognosen im Sicherheitsrecht' (n 8) 201.

[66] Kai Wendt, 'Zunehmender Einsatz intelligenter Videoüberwachung' [2018] ZD-Aktuell, 06122.

Mannheim's main station. By the end of 2021, 68 cameras were in place throughout three so-called 'hotspots', ie the central shopping street, a big city square as well as the forecourt of the main station. The video material is retained for 72 hours. For the time being, police officers are still watching the video in real time and decide whether or not to alarm their colleagues or paramedics.[67] The long-term aim for the software is to work on its own so that less police staff is required.[68] The legislator of the German 'Land' Baden-Württemberg has introduced a specific legal basis for the analysis of image recordings generated by video surveillance in 2017. The wording of the relevant provision is strictly limited to analyses regarding behavioural patterns that indicate the commission of a crime and therefore does not cover biometric face recognition (which is, in fact, not part of the surveillance system deployed in Mannheim).[69]

Other cities are considering the implementation of surveillance systems similar to the one in Mannheim, as well. The Bavarian legislator, however, abstained from introducing a new legal basis for intelligent video surveillance and biometric facial recognition in the course of a recent reform of its legislation governing police competences in 2018, because it was found that, based on practical experience, the necessary technology was not yet reliable enough.[70]

On the federal level, intelligent video surveillance has been tested in the course of the so-called pilot project 'Sicherheitsbahnhof' by the German Federal Police (*Bundespolizei*) in cooperation with the German railway company at the train station 'Südkreuz' in Berlin. The first part of the project was focused on biometric facial recognition. It started in 2017, and in its course, the systems 'BioSurveillance' by the company Herta Security, delivered by Dell EMC AG, 'Morpho Video Investigator (MVI)' by IDEMIA AG, and 'AnyVision' by AnyVision were used and tested.[71] The second part of the project was designed to focus on behavioural analysis, similar to technology used in Mannheim. It was supposed to start in July 2019 and to use software provided by IBM Germany

[67] Olivia Kaiser, 'Was brachte die intelligente Videoüberwachung bisher?' *Rhein-Neckar-Zeitung* (Heidelberg, 3 December 2021) <https://www.rnz.de/nachrichten/mannheim_artikel,-mannheim-was-brachte-die-intelligente-videoueberwachung-bisher-_arid,782203.html> accessed 9 August 2022.

[68] See the reasons put forward for its legal basis (§ 21 [4] Police Act Baden-Württemberg), LT-Drucks. (Baden-Württemberg) 16/2741, 9.

[69] See the reasons put forth for its legal basis (§ 21 [4] Police Act Baden-Württemberg), LT-Drucks. (Baden-Württemberg) 16/2741, 9.

[70] LT-Drucks. (Bavaria) 17/21887.

[71] *Bundespolizeipräsidium* (Federal Police National Headquarters), Final report 'Teilprojekt 1 "Biometrische Gesichtserkennung"', 22 <https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf?__blob=publicationFile> accessed 9 August 2022.

GmbH, the Hitachi Consortium (Hitachi, Conef, MIG), Funkwerk video systems GmbH, and G2K Group GmbH.[72]

Even though there is no public information on the results of the second part of the project, the former Federal Minister for the Interior repeatedly stressed the importance of both intelligent video surveillance and biometric facial recognition technology, and announced a significant expansion of video surveillance and investments of up to € 180 million for 3.000 new cameras with technology allowing high-definition pictures so that until 2024, every large train station throughout the country may be equipped with 'modern camera technology'.[73] On the other hand, critical voices argue that the results regarding facial recognition were not reliable and false positive rates were still too high. Therefore, they demand to abstain from the use of biometric facial recognition technologies.[74] This position seems to resonate with the coalition forming the current federal government which has expressly declared that video surveillance cannot substitute the presence of police officers, but that it can be used to support police work at crime hotspots. Currently, the Federal Ministry of Education and Research funds projects with a focus on intelligent video surveillance in the form of behavioural analysis, for example the development of a software program that is able to identify dangerous behaviour or medical emergencies on train stations or suspicious behaviour on airports through video-based pattern detection.[75] Aspirations regarding the use of biometric face recognition, however, appear to be at a halt as the coalition agreement states that the coalition opposes the ubiquitous use of video surveillance and any use of biometric technology for surveillance purposes.[76] Furthermore, the coalition agreement states with regard to the ongoing negotiations about the so-called Artificial Intelligence

[72] Federal Police, 'Test intelligenter Videoanalysetechnik' (press release 7 June 2019) <https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2019/06/190607_videoanalyse.html> accessed 3 April 2022.

[73] Federal Ministry of the Interior, 'Erhöhung der Sicherheit auf Bahnhöfen' (press release 12 September 2019), <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/sicherheit-auf-bahnhoefen.html> and 'Bundesregierung und Deutsche Bahn beschließen weitere Maßnahmen für mehr Sicherheit an Bahnhöfen' (press release 13 December 2020) <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/sicherheit-bahnhoefe.html> both accessed 9 August 2022.

[74] For a summary of the debate see Arzt, 'Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr' (n 56) paras 1155–1159; Johanna Sprenger, 'Verbrechensbekämpfung' in Martin Ebers and others (eds), *Künstliche Intelligenz und Robotik* (Beck 2020), paras 55–58.

[75] See the project descriptions by the Federal Ministry of Education and Research: <https://www.sifo.de/sifo/shareddocs/Downloads/files/projektumriss_apfel.pdf?__blob=publicationFile&v=1> and <https://www.sifo.de/sifo/shareddocs/Downloads/files/mustererkennung_d_adis.pdf?__blob=publicationFile&v=1> both accessed 9 August 2022.

[76] Coalition agreement, lines 3647–3649 <https://www.wiwo.de/downloads/27830022/8/koalitionsvertrag-2021-2025.pdf> accessed 9 August 2022.

Act[77] on the EU level that the use of biometric face recognition technologies in public spaces as well as the use of 'scoring' systems by state authorities shall be prohibited by EU law.[78]

(4) OSINT and SOCMINT

The German Government funds several research projects regarding software applications that strive to be able to automatically access external publicly available information in social media (open source intelligence/OSINT or social media intelligence/SOCMINT) in order to identify tendencies of extremism and radicalisation, and to prepare preventive strategies.[79]

One of these projects, X-SONAR (*Extremistische Bestrebungen in Social Media Netzwerken: Identifikation, Analyse und Management von Radikalisierungsprozessen* – extremist endeavours in social media networks: identification, analysis, and management of radicalisation processes) was conducted from 2017 to 2020 and focused on the development of an analytic tool that can assess discourses in publicly available online networks, platforms and blogs. The software crawls the relevant information in external sources (such as Facebook or Twitter), and then uses language analysis in order to identify patterns of radicalisation and indicators for early detection of radical tendencies.[80] Based on such identification, law enforcement authorities are supposed to be able to locate relevant discourses for further individual review. The software is said to work theory-based, ie (at least for now) without recourse to artificial intelligence or machine learning.[81]

A more recent example is the project ERAME (*Erkennung von Radikalisierungszeichen in Sozialen Medien* – detection of indications of radicalisation in social media). It aims to develop a software tool that helps with the assessment and analysis of content from

[77] Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM (2021) 206 final.

[78] Coalition agreement, lines 504–505 <https://www.wiwo.de/downloads/27830022/8/koalitionsvertrag-2021-2025.pdf> accessed 9 August 2022.

[79] Wolfgang Kahl, 'PANDORA, RadigZ & X-SONAR' [2017] (2) Forum Kriminalprävention 35.

[80] See the description of the cooperative partner *Landeskriminalamt Niedersachsen* (Lower Saxony State Criminal Police Office), 'Forschungsprojekt "X-Sonar" – Extremistische Bestrebungen in Social Media Netzwerken: Identifikation, Analyse und Management von Radikalisierungsprozessen' <https://www.lka.polizei-nds.de/forschung/forschungsprojekt-x-sonar---extremistische-bestrebungen-in-social-media-netzwerken-identifikation-analyse-und-management-von-radikalisierungsprozessen-113539.html> accessed 9 August 2022.

[81] BT-Drucks. 19/7604, 10–11; Deutsche Hochschule der Polizei (German Police University), 'Forschungsbericht 2018', 97 <https://www.dhpol.de/Forschungsbericht_FIN_Versand.pdf> accessed 9 August 2022; Matthias Becker, 'Fundgrube für Fahndungsdaten – Wie die Polizei soziale Netzwerke nutzt' (*Deutschlandfunk, Online edition*, 26 May 2018) <https://www.deutschlandfunk.de/fundgrube-fuer-fahndungsdaten-wie-die-polizei-soziale-100.html> accessed 9 August 2022.

video platforms (such as YouTube). Computer-linguistics shall be relied upon in order to create a catalogue which serves to identify and classify indicators for extremist content.[82]

As for now, there is no specific (explicit) legal basis for the deployment of projects such as X-SONAR or ERAME. In relation to X-SONAR, individual rights shall be protected by anonymisation and pseudonymisation, meaning that no individuals are meant to be identified.[83] The project ERAME is described to lay special emphasis on the legal assessment of the development process in order to ensure that the functions of the software are in compliance with the law.[84]

1.1.4 Transaction-based 'Predictive Policing'

(1) Advance risk assessments by Fiscal Authorities

Fiscal authorities are starting to use artificial intelligence in different areas of their responsibilities. One of these use cases is an automated analysis in order to identify cases of non-compliance with legal requirements, especially by evaluating certain risk indicators, such as irregularities etc.

The German Financial Intelligence Unit (FIU) handles reports on suspicious transaction concerning money laundering, terrorist financing and other criminal offences. These reports are filed through a software program which is an adapted version of the Software goAML that has been developed by the UN especially for use by all national Financial Intelligence Units.[85] The FIU handles these reports on the basis of a risk-based approach.[86] This means that in order to use its resources most efficiently on the vast number of suspicious transactions reported (144.005 in 2020 alone[87]) through goAML,

[82] Federal Ministry of Education and Research, 'Erkennung von Radikalisierungszeichen in Sozialen Medien (ERAME)' <https://www.sifo.de/sifo/shareddocs/Downloads/files/projektumriss_erame_bf.pdf?__blob=publicationFile&v=1> accessed 9 August 2022.

[83] According to one of the scientists working on the project with *Fraunhofer-Institut für Sichere Informationstechnologie* (Fraunhofer Institute for Secure Information Technology), Martin Steinebach, in Becker (n 80).

[84] Federal Ministry of Education and Research (n 51).

[85] Arzt, 'Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr' (n 56) mn 1281.

[86] For a detailed description: Jens Bülte, 'Risikobasierte Arbeitsweise sowie Analyse- und Weiterleitungspflichten der FIU in den Grenzen des geltenden Rechts' (expert study commissioned by the German Federal Ministry of Finance, 2021), <https://www.bundesfinanzministerium.de/Content/DE/Downloads/Publikationen/gutachten-zu-risikobasierter-arbeitsweise-der-fiu-pdf.pdf?__blob=publicationFile&v=2> accessed 9 August 2022.

[87] FIU, 'Annual Report 2020' <https://www.zoll.de/SharedDocs/Pressemitteilungen/DE/Bargeld/2021/z85_fiu_jahresbericht.html> accessed 9 August 2022; it has to be noted, though, that it is highly controversial whether the risk-based

the FIU decides on the most effective way to proceed with each individual report, according to its relevance for the prevention of money laundering and terrorist financing. The FIU reports that it has started to use an IT component based on artificial intelligence called 'FIU Analytics' since autumn 2020.[88] The software is said to help selecting cases that require further review by calculating risk scores between 1 and 100. The risk score can be subject to further changes, as new information reported through goAML is constantly matched with already existing data (as far as such data has been legally stored for such purposes). Therefore, a case that gained only a minor risk score in the beginning can be identified as part of a high-risk pattern at a later stage.[89]

The legal basis for the analysis of the incoming reports by the FIU is § 30 (2) of the Act against Money Laundering (GwG)[90] which does not specify any details of the analysis, such as the execution of advance checks or the use of technology.[91]

The automated risk management systems run by tax authorities in Germany could also be defined as 'predictive policing'.[92] In Germany, tax reports are processed automatically in case there is no indication that a manual assessment is necessary. In order to identify cases that require such comprehensive review by tax officials or further investigations, tax authorities can use so-called automated risk management systems. Cases requiring comprehensive review can be both cases with irregularities or contradictions as well as 'high-risk' cases. According to § 88 (5) of the German Fiscal Code[93], automated risk management systems must, at a minimum, ensure (1) to select a sufficient number of cases randomly, ie in addition to those that are found to require comprehensive review, (2) that all the selected cases are actually reviewed, (3) that officials can manually select cases for comprehensive review as well, and (4) that

approach is a viable and legitimate basis for the work of the FIU, see Steffen Barreto da Rosa, 'Zum "risikobasierten Ansatz" der FIU im Rahmen der operative Analyse von Meldungen nach dem Geldwäschegesetz', Der Kriminalist [2022], 23.

[88] FIU, 'Annual Report 2020', 11 and 'Annual Report 2021', 30 < https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html> accessed 30 September 2022; see also BT-Drucks. 19/30278, 2; as to the rather vague and partly inconsistent communication regarding the functions and use of 'FIU Analytics', see Steffen Barreto da Rosa 'Vorbemerkungen zu Abschnitt 5 – Zentralstelle für Finanztransaktionsuntersuchungen' in Felix Herzog and Christoph Achtelik, 'Geldwäschegesetz' (Beck, 5th edn (forthcoming) mn 37.

[89] Publicly available information on the details on how FIU Analytics works are very rare, these clarifications stem from the protocol of an exchange with representatives of the Customs Directorate General and staff counsel representatives as well as representatives of the IT company Capgemini (BDZ Personalräte Kompakt 11/2019) <https://bdzovbremen.blogspot.com/2019/11/gzd-financial-intelligence-unit-automatisierte-vorbewertung-kuenstliche-intelligenz-ki.html> accessed 9 August 2022.

[90] Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten.

[91] On the relation to evidence law and the generation of an 'initial suspicion', see **3.1.3.(3)** below.

[92] Rademacher (n 5) 235.

[93] Unofficial translation available at <https://www.gesetze-im-internet.de/englisch_ao/index.html> accessed 9 August 2022.

regular reviews are conducted to determine whether risk management systems are fulfilling their objective. *Baur* argues that it follows from § 88 (5) 2 AO – which demands that the risk management systems take the principle of cost-effective administration into account – that petty cases are to be excluded from the selections.[94] § 88 (5) 4 AO expressly states that further details of the risk management systems do not have to be made public. Therefore, not much is known about the technologies tax authorities rely on. The Federal Ministry of Finance stated in 2021 that the systems used for tax assessment currently work theory-based, but that artificial intelligence technology could be implemented in upgrades.[95]

(2) Risk assessments by Custom Authorities

In a similar vein, the German custom authorities are starting to use artificial intelligence to determine which goods to examine at custom controls. According to Article 46(2) of the (European) Union Customs Code, '[c]ustoms controls, other than random checks, shall primarily be based on risk analysis using electronic data-processing techniques, with the purpose of identifying and evaluating the risks and developing the necessary counter-measures, on the basis of criteria developed at national, Union and, where available, international level'. Public information on this risk analysis is scarce. Yet, it has been reported that German custom authorities employ – and intend to expand the use of – 'neural networks' and 'artificial intelligence' in a project called ZERBERUS.[96]

1.1.5 Objectives, effects and reception of 'Predictive Policing' in Germany

Even though the 'predictive policing' models described above vary significantly in both their functions and their concrete objectives, they all serve the general aim to link and analyse data more efficiently in order to rationalise the allocation of the relevant authorities' resources. In particular, they aim to use scarce resources in a more focused and efficient manner, and thereby allow authorities to fulfil their responsibilities more effectively. This is in line with the Artificial Intelligence Strategy of the German Federal Government: 'In the context of policing, the use of AI is an important strategic aspect of domestic security. For instance, it can help to significantly enhance existing capabilities and make police work more targeted and effective. […] In each specific use case, though, it must be examined whether and how AI can be deployed in a policing context in compliance with fundamental rights.'[97]

[94] Baur (n 5) 283; with doubts: Rademacher (n 5) 238.

[95] BT-Drucks. 19/30278, 4; see also Thomas Wischmeyer, 'Regulierungs- und Verwaltungshandeln durch KI' in Martin Ebers and others (eds), *Künstliche Intelligenz und Robotik* (Beck 2020) mn 26–27 who assumes that artificial intelligence is used for investigations on VAT carousels.

[96] BT-Drucks. 19/30278, 3.

[97] <https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf> accessed 9 August 2022.

The perception among practitioners is documented mainly for location-based predictive policing systems, because among all of the different models, it is the one that has been the main subject to research projects and evaluations so far. For example, research projects on the use of KrimPro in Berlin and of PreCobs in Baden-Württemberg have shown that the perception among police officers is very ambivalent. Findings from Baden-Württemberg suggest that the view is more positive among higher ranks in the hierarchy and more pessimistic among patrol officers.[98] However, scepticism is not only expressed by patrol officers. Some analysts have stated that the software merely confirmed findings that they had previously been able to reach through classical police work – which some felt was now less appreciated.[99] Some officers have said they felt pressured to follow the system's advice or at least that doing so made it much easier to justify their operational decisions.[100] A distinctive challenge for the acceptance of 'predictive policing' software – or for preventive police work in general – seems to be best described by the almost proverbial phenomenon that 'there is no glory in prevention': While the software was found to have little to no effect on actual arrests, its preventive value is less evident and can only be deducted from statistical evaluations. Therefore, prevention can be felt to be less satisfying.[101] That being said, a lot of police officers also perceived 'predictive policing' software as a useful supplement for their work and stated that it had a significant effect not only on the planning of operations, but also on the actual pursuit, as they acted more cautiously in locations that had been flagged as high risks.[102] Many leading officers further reported that the software had a very useful effect on their work in that it made it much easier to successfully request additional police forces to a certain area.[103]

Reception of 'predictive policing' in the general public is very diverse. Journalists, critical voices in legal literature, non-governmental organisations and the Federal Commissioner for Data Protection and Freedom of Information warn against negative effects of 'predictive policing', such as excessive use of personal data, blind trust in technology, lack of quality of data, direct and indirect discriminatory effects, as well as so-called 'chilling effects' of automated policing.[104] This does not mean that the majority

[98] Gerstner (n 12) 134.

[99] Löbel and Schuppan (n 21) 20 and 22.

[100] Albert Meijer, Lukas Lorenz and Martijn Wessels, 'Algorithmization of Bureaucratic Organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems' (2021) 81 Public Administration Review 837, 842.

[101] Löbel and Schuppan (n 21) 20; Gerstner (n 12) 134, Krasmann and Egbert (n 9) 51.

[102] Egbert, 'Predictive Policing als Treiber rechtlicher Innovation?' (n 10) 35–36.

[103] Meijer, Lorenz and Wessels (n 100) 841–842.

[104] See Sprenger (n 74) paras 40–44; Lind, *Raumbezogenes Predictive Policing in Deutschland* (n 8).

of these critics dismiss the idea of 'predictive policing' completely.[105] Furthermore, as seen above, the points of criticism differ depending on the specific system in question. What can be noted on a general level, however, is a call for stricter regulation of predictive policing systems, implying the need for specific and restrictive legal bases including effective legal safeguards, transparency and supervision requirements as well as thorough evaluation both prior to their introduction and continuously during the time of their use.[106]

1.1.6 Assessment of the reliability, impartiality and effectiveness of 'preventive policing' technology in Germany

As for the time being, most of the information on evaluations regarding 'predictive policing' systems that is publicly available pertains to location-based 'predictive policing' systems. These evaluations have in common that it was found to be simply impossible to prove a casual effect of the relevant prevention method on the development of crime or even to assess the accuracy of its individual predictions. The evaluations focused also on other aspects, such as practical and technical aspects on the handling of the relevant systems, its effect on the police work itself and perceptions among practitioners (see **1.1.5** above). The conclusion drawn from the evaluation of the PreCobs system in Baden-Württemberg seems to be exemplary in that regard: 'despite some positive findings, the impact on crime remains unclear and the size of crime reducing effects appears to be moderate. Within the police force, the acceptance of predictive policing is a divisive issue.'[107]

1.2 Normative framework

1.2.1 Law and soft law

(1) Specific legal bases for use of person-focused 'predictive policing' systems

In contrast to location-based predictive policing systems and OSINT/SOCMINT, some of the above-mentioned examples of person-focused predictive policing already have a

[105] Note, however, that in March 2022, 41 mostly European civil society organisations published an open letter in which they urge the Council of the European Union, the European Parliament, and all EU member state governments to prohibit AI predictive and profiling AI systems in law enforcement and criminal justice in the Artificial Intelligence Act; see Fair Trials International, European Digital Rights and others, 'Civil Society calls on the EU to prohibit predictive and profiling AI systems in Law Enforcements and Criminal Justice' (March 2022) https://www.fairtrials.org/app/uploads/2022/03/Ban_Predictive_Policing_Criminal_Justice_Statement.pdf accessed 9 August 2022.

[106] See Federal Commissioner for Data Protection and Freedom of Information, 'Einsatz von Künstlicher Intelligenz im Bereich der Strafverfolgung und Gefahrenabwehr' (thesis paper, 23 March 2022) <https://www.bfdi.bund.de/DE/DerBfDI/Inhalte/Konsultationsverfahren/KI-Strafverfolgung/KI-Strafverfolgung-Thesen-BfDI.html> accessed 9 August 2022; Lind (n 8).

[107] Gerstner (n 12) 115.

specific basis in law. The content of these provisions differs depending on the relevant methods. They do have in common, however, that they do not mention artificial intelligence explicitly but rather use more *technology-open wordings* such as 'automated analysis', 'automated comparisons' or 'automated systems'. In some cases, they do not even refer to automation at all but merely to the relevant task such as 'analysis' or 'further processing of personal data'. The relevant provisions define the use-cases of these automated measures. Partly, there are also rules in place on *substantial requirements* as to the characteristics of the relevant technology, or *procedural rules* regarding its use (eg human intervention), the decision regarding deployment or changes to the technology in use, and/or regular monitoring of the technology in question (see **1.1.2** and **1.1.3.(2)** above and **1.2.3.(2)** below for further details).

(2) Lack of general legislation on predictive policing/use of AI

In contrast to these specific legal bases, there is – as of now – no general legislation on the use of artificial intelligence for 'predictive policing'. Whether or not such legislation might be adopted in the future also depends on the outcome of the negotiations on the so-called Artificial Intelligence Act, the European Commission's draft proposal to regulate artificial intelligence (AI) systems, including in the area of law enforcement and criminal justice.[108]

(3) Compliance with EU law, constitutional law, and the data protection framework

All 'predictive policing' systems must, however, comply with

- constitutional law, in particular the fundamental right to *informational self-determination* following from Article 2 (1) in conjunction with Article 1 (1) of the German Basic Law[109] and the general principle of *equality*, especially the *ban on discrimination* according to Article 3 of the German Basic Law;
- EU primary law, especially the EU Charter of Fundamental Rights, in particular the rights to privacy (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter) as well as the right to non-discrimination (Article 21 of the Charter), whenever the Charter is applicable in accordance with Article 51 of the Charter; and
- European and German Data Protection Law, in particular the rules on the *automation of individual decisions* and on *impact assessments*.

[108] COM (2021) 206 final (n 77).

[109] Basic Law for the Federal Republic of Germany. Unofficial translation available at <https://www.gesetze-im-internet.de/englisch_gg/index.html> accessed 9 August 2022.

(4) Soft law

The *Artificial Intelligence Strategy of the German Federal Government* stresses compliance with fundamental rights and points to the recommendations made by the Data Ethics Commission, which call for a risk-adapted regulatory system.[110] On this basis, algorithmic systems with potential for harm should be regulated with instruments that may, depending on the severity of that harm, include 'formal and substantive requirements (eg transparency obligations, publication of a risk assessment) and monitoring procedures (eg disclosure obligations towards supervisory bodies, ex-post controls, audit procedures)', ex-ante approval procedures or – in cases with serious potential for harm – additional measures such as enhanced ('always-on') oversight and extensive transparency obligations. The Federal Government's Data Ethics Commission recommends to assess the 'use of algorithmic systems by state bodies' as 'particularly sensitive – entailing at the very least a comprehensive risk assessment.' It further stresses that 'decisions taken by the State on the basis of algorithmic systems must still be transparent, and it must still be possible to provide justifications for them. It may be necessary to clarify or expand the existing legislation on freedom of information and transparency in order to achieve these goals. Furthermore, the use of algorithmic systems does not negate the principle that decisions made by public authorities must generally be justified individually; on the contrary, this principle may impose limits on the use of overly complex algorithmic systems.'[111]

Only recently, the *Federal Commissioner for Data Protection and Freedom of Information* conducted a public consultation on the use of AI for preventive police work and criminal prosecution, and emphasised that more concrete regulatory standards are needed with regard to the use of AI for preventive police work and criminal investigations. The consultation entailed seven theses, starting with (1) the need for a broad public debate and comprehensive empiric review in order to clarify the benefits of AI applications in this area and its potential risks for individual rights, including potential discriminatory effects as well as its meaning for democratic and rule of law procedures. In that regard, the Federal Government should also provide an overall account of all police powers (especially surveillance measures). Furthermore, (2) the use of AI should always require a specific legal basis and must not be based on mere general clauses regarding police work. (3) The use of AI must be in compliance with the general

[110] Artificial Intelligence Strategy (2018) <https://www.bundesregierung.de/resource/blob/975226/1550276/3f7d3c41c6e05695741273e78b8039f2/2018-11-15-ki-strategie-data.pdf?download=1> accessed 9 August 2022.

[111] Opinion of the Data Ethics Commission (2019) <https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/datenethikkommission-abschlussgutachten-lang.pdf;jsessionid=A6ACB701AD91D0CFE71972B454523A7E.2_cid364?__blob=publicationFile&v=4> accessed 9 August 2022.

rules on data protection and may not weaken individual remedies. (4) AI needs to be explainable; the quality of data, also of data used for training purposes, must be ensured. (5) The core area of private conduct of life and the guarantee of human dignity must not be affected. (6) Data protection authorities must be able to effectively supervise the use of AI; and (7) there must always be a privacy-impact assessment prior to the use of AI for the purpose of preventive police work and criminal prosecution.[112]

1.2.2 Case Law

While not all decisions of judicial bodies in Germany are published, the case law available to us does not address the use of AI-based systems for 'predictive policing' as such. Some guidance can be drawn, though, from the jurisprudence of the Federal Constitutional Court and the ECJ.

In the decisions relevant in the context of 'predictive policing', the Federal Constitutional Court assessed whether certain forms of processing of personal data by law enforcement authorities in order to prevent crime constitute an infringement of the right to informational self-determination derived from Article 2 (1) in conjunction with Article 1 (1) of the German Basic Law that could be justified because it is necessary and proportionate in order to serve a legitimate purpose. Some of the findings in that regard seem of particular relevance for 'predictive policing':

(1) Infringement of the right to informational self-determination

As a starting point, all 'predictive policing' methods that process personal data constitute an infringement of the right to informational self-determination that requires justification. In its decision regarding automated number plate recognition, the Federal Constitutional Court (BVerfG) recently held (and explicitly overturned previous decisions to the contrary) that it even constitutes a relevant infringement of the right to informational self-determination when personal data is checked automatically with police data, the result is a 'no match', and the data is deleted immediately.[113] Furthermore, the Federal Constitutional Court also recognises an infringement of the right to informational self-determination when personal data that has already been

[112] Federal Commissioner for Data Protection and Freedom of Information, 'Einsatz von Künstlicher Intelligenz im Bereich der Strafverfolgung und der Gefahrenabwehr' (report on the public consultation process, 23 March 2022) <https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Konsultationsbericht.pdf;jsessionid=A459A4FEDC511B17C2035C0FC5C5ADB9.intranet241?__blob=publicationFile&v=3> accessed 9 August 2022.

[113] BVerfG, order of 18 December 2019 – 1 BvR 142/15 *Automatic number plate recognition II* ECLI:DE:BVerfG:2018:rs20181218.1bvr014215 = BVerfGE 150, 244.

collected by state authorities is used beyond the specific purpose of the data collection (further use).[114]

As to the weight of the infringement, the jurisprudence of the Federal Constitutional Court but also of the ECJ indicates that a broad personal scope of the relevant measure, ie a high number of persons potentially affected as well as the use of modern technologies allowing 'data mining' or 'complex forms of data cross-checking' increases the weight of the infringement.[115]

(2) Justification

In order to be justified, an infringement must be necessary to serve a legitimate purpose, such as the prevention of crime or other threats. With regard to the processing of personal data, that means that there needs to be a link between that purpose and the data to be processed. This requirement has been highlighted in the Federal Constitutional Court's decision regarding the Federal Criminal Police Office Act. It stated that both the collection of personal data by state authorities as well as its 'further use' (beyond the purposes that were initially justified) require sufficiently specific grounds or another specific relation to its purpose, such as the targeting of specific risky activities or special sources of danger.[116] This is in line with the position taken by the ECJ regarding data retention for the purposes of prevention, investigation, detection and prosecution of serious crime, where it requires that objective criteria are met that establish a connection between the data to be retained and the objective pursued. That means that there must be objective evidence for a link between the persons concerned with serious criminal offences, for example a connection to certain groups or areas with a high risk that such offences might be committed.[117]

There might be additional requirements depending on the weight of the infringement. For instance, in its decision regarding the extended use of data within the joint database for police authorities and intelligence services according to the Counter-Terrorism Database Act, the Federal Constitutional Court required at least the existence of a sufficiently identifiable danger or a suspicion based on specific facts that are supported

[114] BVerfG, judgment of 20 April 2018 – 1 BvR 966/09, 1 BvR 1140/09 *BKAG* ECLI:DE:BVerfG:2016:rs20160420.1bvr096609 = BVerfGE 141, 220 para 289.

[115] BVerfG, judgment of 19 May 2020 – 1 BvR 2835/17 *Federal Intelligence Service – foreign surveillance* ECLI:DE:BVerfG:2020:rs20200519.1bvr283517 = BVerfGE 154, 152 para 192 and BVerfG, order of 10 November 2020 – 1 BvR 3214/15 *Counter-Terrorism Database Act II/Data-Mining* ECLI:DE:BVerfG:2020:rs20201110.1bvr321415 = BVerfGE 156, 11 para 109; ECJ, case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:491 paras 98–111.

[116] BVerfG, judgment of 20 April 2018 – 1 BvR 966/09, 1 BvR 1140/09 *BKAG* ECLI:DE:BVerfG:2016:rs20160420.1bvr096609 = BVerfGE 141, 220 para 289.

[117] ECJ, joined cases C-203/15 and C-698/15 Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others ECLI:EU:C:2016:970 para 111.

by sufficiently concrete and tangible circumstances.[118] Depending on the weight of the infringement, the Federal Constitutional Court also sets restrictions as to which kind of crime to be prevented or the interests to be protected. With regard to automated number plate recognition, it ruled that '[g]iven the weight of its interference, automatic number plate recognition must serve to protect legal interests of at least considerable weight, or comparably weighty public interests'.[119] In a similar vein, the ECJ recently stressed that, in relation to data gathering without initial suspicion, there must be 'clear and precise rules governing the scope and application of the measures provided for', which must include 'safeguards, so that the persons whose data have been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse.' The legislation 'must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.' [120]

Notably, the Federal Constitutional Court expressly referred to the use of algorithms in its ruling on foreign surveillance by the Federal Intelligence Services, and stated that the legislator may have to lay down the modalities of their use, in particular to ensure that their use can generally be reviewed by the independent oversight regime.[121] Similarly, the ECJ stressed that the need for 'safeguards is all the greater where personal data are subject to automated processing.'[122]

1.2.3 Substantive guarantees

In addition to Constitutional and European Law as interpreted in the jurisprudence described above, data protection law and a few provisions governing specific methods of 'predictive policing' provide for some substantive guarantees.

(1) Data protection law

§ 54 of the Federal Data Protection Act[123] implementing Article 11 of Directive (EU) 2016/680 sets out limits for '*decision(s) based solely on automated processing* which

[118] BVerfG, order of 10 November 2020 – 1 BvR 3214/15 *Counter-Terrorism Database Act II/Data-Mining* ECLI:DE:BVerfG:2020:rs20201110.1bvr321415 = BVerfGE 156, 11; Golla argues that the findings of this decision are applicable to the legal basis for 'HessenData' (as well as its Hamburg equivalent) with the consequence that these provisions would not meet the constitutional requirements either, Sebastian Golla, 'Algorithmen, die nach Daten schürfen – "Data-Mining" zur Gefahrenabwehr und zur Strafverfolgung', [2021] NJW 667, 670–672.

[119] BVerfG, order of 18 December 2019 – 1 BvR 142/15 *Automatic number plate recognition II* ECLI:DE:BVerfG:2018:rs20181218.1bvr014215 = BVerfGE 150, 244.

[120] ECJ, case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2016:970 para 117.

[121] BVerfG, judgment of 19 May 2020 – 1 BvR 2835/17 *Federal Intelligence Service – foreign surveillance* ECLI:DE:BVerfG:2020:rs20200519.1bvr283517 = BVerfGE 154, 152.

[122] ECJ, case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2016:970 para 117.

[123] An unofficial translation is available at <https://www.gesetze-im-internet.de/englisch_bdsg/index.html> accessed 9 August 2022.

produces an adverse legal effect concerning the data subject or significantly affects him or her'. However, none of the 'predictive policing' systems explained above aim to generate automated decisions. Rather, it is regularly being emphasised that the relevant technologies serve as a mere means of support and the decision itself is still up to (a) human officer(s)[124] – although that decision may yet be 'anchored' in the suggestion made by technology.[125]

Therefore, § 67 of the Federal Data Protection Act implementing Article 27 of Directive (EU) 2016/680 seems of higher practical relevance as it requires to conduct, prior to the processing of personal data, a *data protection impact assessment* whenever data is to be processed by means of a new technology likely to result in a substantial risk to the legally protected interests of data subjects.

(2) Method-specific provisions

§ 4 (3) of the PNR Act (see **1.1.3.(1)** above), which regards the patterns to be automatically matched against PNR-data, is one of the few examples setting out at least basic requirements as to both the design of the technology being used as well as procedural requirements for its establishment and further use. As to the design of the patterns, it prescribes the *combination of incriminating and exonerating criteria* in order to limit the amount of potential false-positives. Furthermore, and in order to *prevent discrimination*, it prohibits the use of information on a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. From a procedural point of view, the Federal Criminal Police Office must establish the patterns in *cooperation with its data privacy officer* and other security and police authorities. *Review by an independent body* is also guaranteed as the Federal Commissioner for Data Protection and Freedom of Information shall review the production and use of the patterns at least every two years, and report to the Federal Government every two years.

Another more detailed example is shown by § 88 (5) of the German Fiscal Code for automated risk assessment systems used by fiscal authorities (see **1.1.4.(1)** above). According to its second sentence, risk management systems have to take the *principle of cost-effective administration* into account.[126] The third sentence of this provision addresses the *reliability* of the use of these systems, as it requires (1) them to, at a minimum, select a sufficient number of cases randomly, ie in addition to those identified through the automated risk assessment, (2) that all the selected cases are actually reviewed, (3) that officials can also manually select cases for comprehensive review and (4) that *regular*

[124] Arzt, 'Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr' (n 56) mn 1294; Lucia M Sommerer, *Personenbezogenes Predictive Policing* (Nomos 2020) 130.

[125] See **1.1.5** above.

[126] Baur (n 5) 283; with doubts: Rademacher (n 5) 238.

reviews are conducted to determine whether risk management systems are fulfilling their objective. The provision also *limits transparency* explicitly as § 88 (5) 4 states that further details of the risk management systems do not have to be made public.

§ 25a HSOG and § 49 PolDVG (see **1.1.3.(2)** above) do not provide any requirements as to the design of the software, but at least define its tasks (automatically identify affiliations or connections between individuals etc), limit its use to the prevention of crimes or threats of significant weight in individual justified cases, and regulate the decision-making process on deployment or significant changes to the software. § 23 (6) PolG NRW, on the other hand, entails a rather generic description of the relevant tasks (comparisons, preparation or analysis of data), provides for less restrictive definitions of the purposes of its use and lacks further regulation of the decision-making progress mentioned above (in contrast to the other two provisions it does, however, require recording of each query).

Other provisions, such as § 21 (4) of the Police Act Baden-Württemberg on intelligent video surveillance (see **1.1.3.(3)** above) merely regulate the use of 'automatic analysis' for specific purposes, but do not provide further details as to the design of the relevant technology or its monitoring.

Notably, § 30 (2) of the Act against Money Laundering merely refers to the assessment of incoming money laundering reports, but does not specify any details of the analysis, especially neither the execution of advance checks nor the use of technology (see **1.1.4.(1)** above).

1.3 General principles of Law

The potential effects of predictive policing on constitutional rights, proportionality and the rule of law are subject to a controversial debate. As stated above, the majority of the voices raising concerns do not seem to oppose the use of 'predictive policing' methods in general, but call for more legal safeguards and restrictions.

1.3.1 General limitations of predictive policing

Many commentators point to the inherent limitations of automated 'predictive policing' solutions and their potential negative side-effects. They point out that 'predictive policing' solutions base their assumptions on patterns and correlations rather than on an analysis of the root causes of crime and that therefore, its purpose will always be restricted to crime control through surveillance and short-term interventions. This might distract from the need for more complex but also more sustainable strategies against crime, such as efforts to remedy the social problems that can facilitate criminality.[127]

1.3.2 *Discriminatory potential of predictive policing*

Another characteristic limitation of automated 'predictive policing' is its dependency on data. Since every automated solution is only as good as the data it is trained on and provided with, all its accuracy relies on the data. Every imbalance, every error or incompleteness within the relevant data sets is likely to be reproduced in the assumptions and recommendations produced by the software in question.[128] This can have an adverse effect on groups within the population that are already vulnerable. If – for example – a certain community is already subject to high police attention, more crimes occurring within this group will be documented and more crime data relating to this group will be fed into the system.[129] Such negative feedback loops can increase discriminatory effects, even in case the relevant software does not process protected characteristics such as religion or ethnic background, but so-called proxies, ie circumstances that correlate with such characteristics (for example certain neighbourhoods, religious sites, travel routines, etc).[130] These concerns are also an issue of proportionality, as the consequences of biased 'predictive policing' are usually connected with police interference; therefore, the effects of false positives can interfere with the right to liberty and security.

1.3.3 *Potential remedies*

Potential remedies against biased and false automation results are one of the most imminent topics within the current debate.

(1) Exclusion of certain categories of data

In order to prevent discrimination, § 4 (3) of the PNR Act excludes protected characteristics from processing. This is in line with the approach of § 56 of the Federal Data Protection Act defining stricter conditions and safeguards for the processing of protected categories of data. These restrictions do, however, only focus on the protected characteristics, and therefore can only prevent direct discrimination. In order to identify the discriminatory potential of other data or so-called proxies, some commentators even

[127] Knobloch (n 1) 30; Sommerer, *Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control* (n 38) 85–87.

[128] Sommerer, *Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control* (n 38) 87–93; Hauke Bock and Katrin Höffler, 'Künstliche Intelligenz und Kriminalität' [2022] KriPoZ 257, 262.

[129] Henning Hofmann, *'Predictive Policing'* [Duncker & Humblot 2020], 281-283.

[130] Carsten Orwat, *Diskriminierungsrisiken durch Verwendung von Algorithmen* (Nomos 2019) 62–66 <https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/DE/publikationen/Expertisen/studie_diskriminierungsrisiken_durch_verwendung_von_algorithmen.pdf?__blob=publicationFile&v=3> accessed 9 August 2022.

consider it to be necessary to process the protected characteristics and evaluate potential correlations to otherwise 'neutral' data.[131]

(2) The relevance of human intervention – risks of automation bias

A huge majority of commentators agrees that automated 'predictive policing' systems must never replace human decisions and responsibilities – and that therefore individual users also should not follow automated findings blindly. It should always be up to a human officer to scrutinize the relevant results before responding to them with potential follow-up measures.[132] Critical voices raise doubts as to whether it can be realistically expected from relevant users to maintain a critical attitude towards such automated support tools, and even warn against inappropriate trust in automated recommendations ('automation bias').[133] As has been seen with regard to location-based 'predictive policing' systems, even a human operator might feel a strong incentive to follow automated results, either because of an inappropriate trust in the relevant technology, or because doing so might seem less controversial and easier to justify.[134] To make it worse, there are also indications that deployment of 'predictive policing' might even increase racial profiling among human operators. In this regard, *Egbert* points to empirical studies showing that patrol officers who are deployed to 'high-risk' locations are more likely to act suspicious towards individuals within these areas, especially towards individuals fulfilling certain visible stereotypes.[135]

(3) Transparency and explainability

These concerns become even more relevant in case the police officers in question do not have an understanding of the way the relevant technology works, especially with regard to 'predictive policing' models that operate on machine learning technology which cannot be explained with recourse to a certain theory. Therefore, transparency and explainability seem to be crucial for an effective human control. Research on the question of how these can be provided even for machine learning systems – for example through ex-post validation[136] – is still in an early stage.[137]

[131] Rademacher (n 5) 265–266; Wischmeyer, 'Predictive Policing, Nebenfolgen der Automatisierung von Prognosen im Sicherheitsrecht' (n 8) 205.

[132] Hofmann (n 129) 292.

[133] Tobias Singelnstein, 'Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention' [2018] NStZ 1, 4.

[134] See **1.1.5** above.

[135] Egbert, 'Predictive Policing als Treiber rechtlicher Innovation?' (n 10) 39–42.

[136] Benedikt Kohn, *Künstliche Intelligenz und Strafzumessung* (Nomos 2021) 284.

[137] Sommerer, *Personenbezogenes Predictive Policing* (n 124) 206–221.

(4) Surveillance and chilling effects

On another note, critical voices complain that 'predictive policing' typically affects a broad range of individuals without any (or at least any clear) relation to the crimes which the software aims to prevent. 'Predictive policing' tools, which process personal data before any suspicion is established, are partially viewed as a disproportionate interference with the right to privacy. In this manner, the prevalence of 'predictive policing' could contribute to a feeling of 'overall surveillance'.[138] There is substantial concern that this can lead to chilling effects among the population, and impair the right to freedom of expression. Therefore, some consider the existing normative framework to be insufficient in order to safeguard compliance with the standards of the German Constitutional Law or the Law or Fundamental Rights in EU Law.

In order to monitor the overall proportionality of the interference with the right to privacy, many stress the need for a constant overview of all surveillance and similar measures ('Überwachungsgesamtrechnung').[139] The parliamentary coalition forming the current German government agreed to establish such an overview, and to conclude an independent scientific evaluation of all legislation on security matters, including their effects on freedom and democracy, as well as considering technological developments, until the end of 2023.[140]

2 'Predictive Justice' in the Administration of Criminal Justice in Germany

As 'predictive justice', we understand AI-based or AI-assisted assessments of recidivism and of sentencing. On this basis, criminal justice in Germany does – as of now – not make use of such IT tools (see **2.1** below on recidivism assessments), and the prevailing viewpoint in the legal literature in Germany is highly sceptical of such tools (see **2.3** below),[141] with one notable exception: the introduction of a sentencing database which may, with the assistance of AI, point to precedents and provide soft guidance to judges in sentencing (see **2.2** below).

2.1 Assessments of recidivism

[138] Bock and Höffler (n 128), 263 (with regard to video surveillance).

[139] Federal Commissioner for Data Protection and Freedom of Information, 'Einsatz von Künstlicher Intelligenz im Bereich der Strafverfolgung und der Gefahrenabwehr' (report on the public consultation process, 23 March 2022) <https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Konsultationsbericht.pdf;jsessionid=A459A4FEDC511B17C2035C0FC5C5ADB9.intranet241?__blob=publicationFile&v=3> accessed 9 August 2022; Rademacher (n 5) 268.

[140] Coalition agreement, lines 3638–3643 <https://www.wiwo.de/downloads/27830022/8/koalitionsvertrag-2021-2025.pdf> accessed 9 August 2022.

[141] For an overview see Kohn (n 136) 173.

Assessments of recidivism are of high importance in German criminal justice, in particular in relation to decisions on probation and parole, and whether a convicted offender is to be placed or kept in measures of reform and prevention, in particular in the so-called 'preventive detention'.[142] To assess the risk of recidivism, expert reports – and their oral reports as expert witnesses – continue to be the *state of the art* in Germany. These experts, mostly psychologists and psychiatrists, do not and, according to case law, must not[143] rely on a statistical analysis, but must conduct an individual and all-encompassing evaluation of the respective person.[144] At most, they may take statistical base rates or a standard instrument to assess recidivism as a starting point, but then need to 'individualise' any such mathematical/statistical finding.[145] The use of such instruments seems even more questionable when following *Zimmermann*'s approach, who argues that decisions on probation should not primarily be based on predictions of reoffending but rather on an inherently normative assessment of the individual offender's expectations of social rehabilitation.[146]

2.2 Sentencing database

In recent years, some academics have pointed to differences in sentencing levels in Germany, consider these to be unjustified and therefore have launched attempts to investigate these differences further with the ultimate aim to harmonise the sentencing levels across Germany.[147] As a starting point, they identified a need for better data. While all reasoned decisions by the Federal Court of Justice are published and available electronically,[148] only a handful of decisions by the courts of first instance are published. To address this lack of data, the new coalition government agreed to push for the publishing of all judgments in criminal matters, in machine-readable and anonymised form.[149]

In the meantime, a research project led by *Rostalski* aims to create a sentencing database (with a specific focus on theft offences) and to analyse the sentencing criteria and the

[142] For a background on 'preventive detention' and its role in German criminal justice, cf *M v Germany* ECHR 2009–VI 169.

[143] BVerfG [2004] NJW 750, 759; BGH [2005] NStZ 561, 563.

[144] Axel Boetticher and others, 'Empfehlungen für Prognosegutachten' [2019] NStZ 553, 558.

[145] BGH, order of 30.03.2010 – 3 StR 69/10 = [2010] NStZ-RR 203, 204.

[146] Stefan Zimmermann, *Die Erwartung künftiger Straffreiheit* (Mohr Siebeck 2022).

[147] See, in particular, Johannes Kaspar, 'Verhandlungen des 72. deutschen Juristentages Leipzig 2018 Bd. I: Gutachten Teil C'.

[148] <https://www.bundesgerichtshof.de/DE/Entscheidungen/entscheidungen_node.html> accessed 9 August 2022.

[149] Coalition agreement, lines 3570–3571 <https://www.wiwo.de/downloads/27830022/8/koalitionsvertrag-2021-2025.pdf> accessed 9 August 2022.

argumentation in relation to sentencing in criminal justice.[150] To extract this information, she and her team employ AI technology.[151]

It should be noted, however, that the proponents of sentencing databases do not call to replace the judicial decision on sentencing with an AI-based tool. Instead, they strive for an additional input to be given to judges: By using such tools, they would like to point to precedents or 'similar cases' and their sentencing levels. That would likely anchor future sentencing decisions, require judges to reason any (significant) deviations from previous sentencing levels and therefore harmonise – but also petrify[152] – levels of sentencing.[153]

2.3 Scepticism on 'predictive justice'

Beyond such usage of AI technology to find precedents, in particular in relation to sentencing, there is a widespread scepticism on 'predictive justice' and AI-based assessments of recidivism in particular. For example, the presidents of the Higher Regional Courts recently discussed the use of AI in the realm of criminal law, eg relating to sentencing, recidivism or evidence assessment. They highlighted 'risks of discriminatory tendencies due to biased programming' and of 'unfair proceedings resulting from lack of transparency or unavoidable influence on the independent judge'[154]. On this basis, they adopted a common statement raising serious concerns against the introduction of AI-based standardisations for criminal procedures.[155]

This scepticism mostly stems from the viewpoint that the central assessment of guilt, of sentencing and of (continuing) enforcement of imprisonment is vested with judges as

[150] Legal Tech Lab Cologne eV, 'Smart Sentencing' <https://legaltechcologne.de/2021/12/21/smart-sentencing/> accessed 9 August 2022.

[151] Legal Tech Lab Cologne eV, 'Smart Sentencing' <https://legaltechcologne.de/2021/12/21/smart-sentencing/> accessed 9 August 2022.

[152] On this criticism, see Franz Streng, 'Digitalisierung und Strafzumessung' in Elisa Hoven and Hans Kudlich, *Digitalisierung und Strafverfahren* (Nomos 2020) 205, 212.

[153] Frauke Rostalski and Malte Völkening, KriPoz 5 (2019) 265; Streng (n 152) 211–214.

[154] Dickert and others, 'Einsatz von KI und algorithmischen Systemen in der Justiz, Grundlagenpapier zur 74. Jahrestagung der Präsidentinnen und Präsidenten der Oberlandesgerichte, des Kammergerichts, des Bayerischen Obersten Landesgerichts und des Bundesgerichtshofs' (2022) 32–34, 41 <https://www.justiz.bayern.de/media/images/behoerden-und-gerichte/oberlandesgerichte/nuernberg/einsatz_von_ki_und_algorithmischen_systemen_in_der_justiz.pdf> accessed 9 August 2022 (translation to English by the authors).

[155] 'Beschluss der Präsidentinnen und Präsidenten der Oberlandesgerichte, des Kammergerichts, des Bayerischen Obersten Landesgerichts und des Bundesgerichtshofs' (31 May 2022) <https://oberlandesgericht-celle.niedersachsen.de/startseite/aktuelles/ergebnisse_der_74_jahrestagung_zum_einsatz_kunstlicher_intelligenz_in_der_justiz_u_a/ergebnisse-der-74-jahrestagung-zum-einsatz-kunstlicher-intelligenz-in-der-justiz-u-a-212102.html> accessed 9 August 2022. A more positive outlook, at least for specific judicial decisions, is taken by Simon Eisbach, Michael Heghmanns and Guido Hertel, 'Künstliche Intelligenz im Strafverfahren am Beispiel von Kriminalprognosen', [2022] ZfIStw 489.

human beings.[156] Their involvement, and their (ultimate) decision is seen as a safeguard to an individualised,[157] all-encompassing[158] and therefore just decision,[159] highlighting a fear of too schematic decisions being taken in the sensitive area of criminal justice. Moreover, there seems to be a lack of trust in the validity of AI tools,[160] in particular the risk of an inherent bias,[161] and the problem to 'understand' the methodology employed by AI tools ('black box'[162], even in light of the trend to 'explainable AI'[163]).

The most obvious point of reference of these concerns are AI-based solutions that 'prepare, suggest or even substitute decisions by a human judge'[164]. Such use could even collide with constitutional principles, especially those guaranteeing that the judicial powers are vested in judges (Article 92 of the German Basic Law), that judges shall be independent and subject only to the law (Article 97 [1] of the German Basic Law), that no one may be removed from the jurisdiction of their lawful judge (Article 101 [1] of the German Basic Law), and potentially also with further fundamental (procedural) rights of the accused.[165] The question of where to draw a line between such problematic cases and AI tools restricted to reasonable technical support is much more difficult to answer.[166] Moreover, even the use of AI tools to merely assist (human) prosecutors and judges should not be underestimated. Their findings are subject to the same risks (in particular of bias, incompleteness and 'black box'), but may set a strong 'anchor'.[167] It is well understood in psychology that any anchoring can have a strong effect on human

[156] Frauke Rostalski, 'Judex ex machina? Zum Einsatz neuer Technologien in der Rechtsfindung' in Elisa Hoven and Hans Kudlich, *Digitalisierung und Strafverfahren* (Nomos 2020) 263, 275–276; see also Luís Greco, 'Richterliche Macht ohne richterliche Verantwortung: Warum es den Roboter-Richter nicht geben darf' [2020] Rechtswissenschaft 29; see also Bock and Höffler (n 128), 266.

[157] Malin Ebersbach, 'Big Data, Algorithmen und Bewährungsentscheidungen' in Carsten Momsen and Mathis Schwarze, *Strafrecht im Zeitalter von Digitalisierung und Datafizierung* (KriPoZ 'Junges Publizieren' Series 2020) 25, 34 and 33–35 with an overview on further shortcomings of algorithmic predictions; see further Brian Valerius, '"Legal Tech" im Strafverfahren?' (2021) 133 ZStW 152, 158–168.

[158] See Mario Martini und David Nink, 'Strafjustiz ex machina?' in *Automatisch erlaubt?* (Bertelsmann Stiftung 2020) 44, 60–61 highlighting not only the complexity of all relevant circumstances in each individual case but also the importance of normative components of their assessments.

[159] See also Hannah Ofterdinger, 'Strafzumessung durch Algorithmen?' [2020] ZIS 404, 410.

[160] Mario Martini, 'Algorithmen als Herausforderung für die Rechtsordnung' (2017) 72 JZ 1017, 1018.

[161] Kohn (n 136) 260.

[162] Kohn (n 136) 260.

[163] Sommerer, *Personenbezogenes Predictive Policing* (n 124) 204–205; Eisbach, Heghmanns and Hertel (n 155) 495.

[164] Dickert and others (n 154) 41.

[165] Dickert and others (n 154) 6–18.

[166] Peter Biesenbach, Markus Hartmann and Rolf Schwartmann, 'Der elektronische Gerichtsdiener' *Frankfurter Allgemeine Zeitung* (online edition, Frankfurt, 9 July 2022) <https://www.faz.net/aktuell/karriere-hochschule/hoersaal/ki-in-der-justiz-der-elektronische-gerichtsdiener-18084850.html?premium> accessed 9 August 2022.

[167] See already, in the context of 'predictive policing', **1.1.5** above; see additionally Eisbach, Heghmanns and Hertel (n 155) 492.

decision-making. Similarly, prosecutors or judges could be susceptible to a so-called automation-bias as well and perceive automated results as more rational or objective than they actually are.[168] Therefore, it is of utmost importance that the workings and limitations of an AI-based tool are well understood and internalised by decision-makers, and that, in the meantime, much care is taken that such anchoring effects are avoided.

3 Evidence Law and the Use of Artificial Intelligence in the Administration of Justice in Germany

3.1 Evidence gathering and filtering through AI-based systems

In criminal investigations, German law enforcement authorities – and independent experts they contract[169] – have to sift through ever more electronic data to find 'evidence'[170] pertaining to the alleged offence and to build up 'information positions'[171] in furtherance of the investigation.

3.1.1 Extensive legal framework on the obtaining and on the later use of data

Traditionally, the German Act on Criminal Procedure (StPO) puts significant emphasis on governing – and restricting – the obtaining of objects (such as computers or mobile phones) and data (such as e-mails) for the purpose of criminal investigations.

(1) Electronic surveillance and the protection of the core area of private conduct of life

In particular, § 100a StPO sets out material and procedural requirements under which an Internet connection may be wiretapped, § 100b StPO the conditions for a covert remote search of information technology systems, § 100c StPO the conditions for an acoustic surveillance of private premises, and §§ 100g, 100j and 100k StPO the conditions to request subscriber and other meta-data from telecommunication and telemedia service providers. Additional rules in these and further provisions govern and restrict the subsequent use of such data in the criminal prosecution and as evidence in court. For instance, any evidence may later on be inspected by counsel according to § 147 StPO, and any reports included in the case file become accessible to suspects and counsel according to §§ 32f, 147 StPO. In contrast, a legal framework on the intermediate step – the analysis and filtering of the data – is almost non-existing.[172]

[168] Martini and Nink (n 158) 50–51.

[169] Just see Janique Brüning, 'Privatisierungstendenzen im Strafprozeß – Chancen und Risiken der Mitwirkung sachverständiger Privatpersonen im strafrechtlichen Ermittlungsverfahren' [2008] StV 100.

[170] Data itself cannot be presented as evidence in court, but needs to be transformed first. On this issue, see **3.2.1.** below.

[171] Lorena Bachmaier Winter, 'Section III: Criminal Procedure. Information Society and Penal Law' (2014) 85 RIDP 75, 89–90.

[172] On the lack of regulation in the field of IT forensics, see **3.1.2** below.

The sole notable exception is § 100d (2) 1, (3) 2 StPO: If, during the analysis of data obtained by a wiretap, a remote search of information technology systems or an acoustic surveillance of private premises, data pertaining to the 'core area of private conduct of life' is determined, such data is to be deleted immediately. This 'core area' relates to highly personal expressions,[173] such as prayers, sexuality, or soliloquy,[174] which are – according to the jurisprudence of the Federal Constitutional Court – protected by human dignity (Article 1 [1] Basic Law) and out of bounds for any interference by the state. Not part of the 'core area' are, however, expressions concerning the planning or execution of criminal offences.[175]

In light of this constitutional requirement to protect the 'core area of private conduct of life', two scholars, *Esser* and *Reißmann*, have recently suggested creating and utilising a 'weak' AI system.[176] In their view, such a system could stop the surveillance measure temporarily in case this 'core area' is affected, and automatically filter out 'core area'-related data.[177] They argue that a well-trained system may achieve the goal – the state should not obtain any knowledge of 'core area'-related data – much better than the present filtering by humans, as it avoids or at least reduces any human involvement.[178] Therefore, they consider it to be a constitutional requirement to make use of promising AI technology in this field.[179]

(2) Search and seizure of physical objects and data

In a similar vein, the German Act on Criminal Procedure sets out quite specific rules under which conditions premises may be searched (§§ 102–110 StPO) and objects (such as computers or mobile phones) or data (such as e-mails) of interest for the criminal investigation may be seized (§§ 94–98 StPO). During the search of a premise, however, authorities first need to identify the objects and data of interest, for example the letter or e-mail containing a 'smoking gun' pertaining to the alleged offence. For this intermediate phase, which is legally still part of the search,[180] the recently amended §

[173] See recently BVerfG, judgment of 19 May 2020 – 1 BvR 2835/17 *Federal Intelligence Service – foreign surveillance* ECLI:DE:BVerfG:2020:rs20200519.1bvr283517 = BVerfGE 154, 152 para 200–201.

[174] See recently BVerfG, judgment of 19 May 2020 – 1 BvR 2835/17 *Federal Intelligence Service – foreign surveillance* ECLI:DE:BVerfG:2020:rs20200519.1bvr283517 = BVerfGE 154, 152 para 202 and BGH, judgment of 22.11.2011 – 2 StR 509/10 = BGHSt 57, 71.

[175] See recently BVerfG, judgment of 19 May 2020 – 1 BvR 2835/17 *Federal Intelligence Service – foreign surveillance* ECLI:DE:BVerfG:2020:rs20200519.1bvr283517 = BVerfGE 154, 152 para 202.

[176] Robert Esser and Ludwig Reißmann, 'Schutz des Kernbereichs privater Lebensgestaltung durch den Einsatz künstlicher Intelligenz (KI) – Neue Perspektiven für Strafverfolgung und Gefahrenabwehr' [2021] StV 526.

[177] Esser and Reißmann (n 176) 530.

[178] Until such a system is sufficiently trained, however, they call for an additional – manual – review of the data; cf Esser and Reißmann (n 176) 530.

[179] Esser and Reißmann (n 176) 530–532.

[180] Just see BVerfG, order of 30.11.2021 – 2 BvR 2038/18 ECLI:DE:BVerfG:2021:rk20211130.2bvr203818 para 44.

110 StPO sets out implicitly that such (physical) objects and (electronic) data may be seized temporarily ('vorläufige Sicherstellung'), and explicitly allows that public prosecutors and specifically authorised police officers may inspect this material and select the relevant parts for formal seizure (and later use in the criminal investigation and trial). Jurisprudence calls, on the basis of the proportionality principle, for a swift process;[181] as a rule of thumb, the material needs to be inspected within six months. There are conflicting views on whether suspects and their counsel have a right to be present during such inspection;[182] in any case, their presence may help in quickly finding the relevant evidence, and avoid the timely and costly analysis of irrelevant data.

3.1.2 Unclear legal framework on the forensic analysis of data

German law is silent, however, on how specifically objects and data seized temporarily (**3.1.1.(2)** above) or obtained by means of electronic surveillance (**3.1.1.(1)** above) may be analysed. Only slowly, standards of IT forensics are evolving, and these standards relate mostly on the repeatability of their analysis and on the reporting of the forensic findings to the court.[183] While the 'AI Act' proposed on the EU level[184] may (re-)shape the framework on the use of IT forensics in future, we will focus on two aspects already under discussion under present German criminal procedure law:

(1) Breaking encrypted IT devices

German law enforcement authorities employ different commercially available IT forensic tools, such as *Cellebrite* or *X-Ways Forensics*, as well as self-developed tools to analyse IT devices and the data stored therein, and to potentially break any encryption they encounter. While a suspect or accused person may not be compelled to assist in such steps, in particular by handing over passwords or PINs, law enforcement authorities opine that as they are allowed to seize the object of interest (such as an encrypted cell phone), they are then also allowed to analyse the object by all available means, including brute-force attacks, side-channel attacks and other means to circumvent or break encryption.[185]

[181] Just see BGH, Order of 20.05.2021 – StB 21/21 ECLI:DE:BGH:2021:200521BSTB21.21.0 = [2021] NStZ 623.

[182] On this discussion, see Momme Buchholz, 'Das Anwesenheitsrecht bei der Durchsicht von Datenbeständen nach § 110 Abs. 1 StPO' [2021] NZWiSt 369; Kristina Peters, 'Anwesenheitsrechte bei der Durchsicht gemäß § 110 StPO: Bekämpfung der Risiken und Nebenwirkungen einer übermächtigen Ermittlungsmaßnahme' [2017] NZWiSt 465.

[183] See, in particular, Dennis Heinson, *IT-Forensik. Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen* (Mohr Siebeck 2015); Andreas Dewald and Felix Freiling, *Forensische Informatik* (2nd edn, Books on Demand 2015).

[184] COM (2021) 206 final (n 77).

[185] See, for instance, Maik Bäumerich, 'Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung. Neue Technologien, alte Befugnisse' [2017] NJW 2718, 2720.

Some in German legal literature argue differently, however: According to them, an encrypted IT system deserves much higher legal protection, as personal IT systems and the (highly) personal data stored therein give extensive insights to the personal life. And as authorities employ specific 'technical means' to 'gain […] access to an information technology system used by the person concerned and to extract data from that system', they argue that the same standard which governs the covert remote search of IT systems (§ 100b StPO) should be employed for breaking encryption of (openly) seized IT systems.[186]

Neither the legislature nor courts have taken a definite stance on this issue so far. In our view, the first standard – authorities may employ *any* means – pays too little attention to the needs of data protection also within criminal investigations, yet the second standard – § 100b StPO – seems to be too restrictive, as it governs a *covert* surveillance measure; therefore, a future standard should strive for some middle ground.

(2) 'Data mining' in criminal files

Using the same and similar tools mentioned above (including HessenData and Palantir[187]), law enforcement authorities also employ 'data mining' in the evidence obtained within a specific criminal investigation. Moreover, § 98c StPO explicitly allows to automatically match data from one criminal proceeding with other data stored for the purpose of criminal investigations, the execution of sentences, or the averting of dangers, providing an explicit legal basis to utilise 'data mining' techniques to investigate a (specific) criminal offence or to locate a (specific) offender.[188] However, this provision is only applicable within a criminal investigation, and therefore does not allow for a 'fishing expedition' to find out indications of previously unknown offences. Moreover, such an automatic matching is only allowed within criminal proceedings specifically pre-selected for this purpose, and not with all data stored in electronic case files; this also precludes 'fishing expeditions' (§ 498 [2] StPO).

3.1.3 Specific usages of AI systems

Three specific usages of AI technology in evidence gathering and filtering implemented or under discussion in Germany warrant a highlighting:

(1) ZAC-AI Enabled Rapid Assessment (ZAC-AIRA)

In investigations of sexualised violence against children, it becomes ever more common that law enforcement authorities seize terabytes of electronic evidence. There is an

[186] Mathias Grzesiek and Daniel Zühlke, 'Die Entschlüsselung von Smartphones gegen den Willen des Beschuldigten zum Zwecke der Durchführung des Strafverfahrens' [2021] StV-S 117.

[187] See **1.1.3.(2)** above.

[188] Cf Markus Jäger, '§ 98c' in von Heintschel-Heinegg and Bockemühl (eds), *KMR – Kommentar zur Strafprozessordnung* (111th supp, Heymanns 2022) mn 2.

urgent need to analyse this data rapidly, particularly if such data contains unknown child sexual abuse material (CSAM) hinting to ongoing abuse, as such information enables authorities to protect victims from further harm. Yet, it is a psychologically challenging and time-consuming effort to manually evaluate this data. Therefore, a research project lead by a specialised public prosecutor's office in the German state of North Rhine-Westfalia, the *Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen* (ZAC NRW)[189] evaluated the opportunity to use machine learning technology for a rapid, first and preliminary assessment of CSAM.

Particular attention was spent on the need to protect and safeguard the extremely sensitive data concerned: The possession and transfer of CSAM is a felony offence under German criminal law, and only permissible to a very limited extent (cf § 184b StGB). Moreover, it must strictly be avoided that CSAM can fall into the hands of unrelated third parties, including attackers of the IT systems involved. To achieve this goal, the following innovative approach was used: Both for the training of the AI model and then for the classification of data, the images are preprocessed locally (on-premise) to data where the original content (be it CSAM, be it lawful material) is no longer recognisable. As far as is known, this preprocessing is also non-reversible. Therefore, this 'deconstructed' data no longer constitutes CSAM material, does not fall under the criminal provision of § 184b StGB, and cannot be misused by third parties. Only such 'deconstructed' data is then transferred to a remote 'cloud' service for machine learning and/or classification. In test cases, the AI model classified over 90% of images correctly as either CSAM (differentiated between children aged below 14 years of age, and youths between 14 and 18 years of age), 'adult' pornography or other images. Starting in April 2022, a production system building upon this ZAC-AIRA research project entered service in North Rhine-Westfalia.

It must be noted, however, that this tool merely aims at filtering the evidence: It provides a fast evaluation whether CSAM may be present on a storage device, and directs investigators to images which are, to a high probability, CSAM. Any image flagged by this system then is to be evaluated independently by the police, by public prosecutors and ultimately by the courts. As this system is specifically designed to prefer false-positive to false-negative results, much attention must be spent at these later stages of the criminal process to assess the potential CSAM anew, without 'trusting' the classification given by the AI system. Moreover, it is well understood by the ZAC-AIRA research group that such a tool requires constant evaluation and re-training – for instance, if it is determined that certain categories of CSAM are flagged insufficiently.

[189] In collaboration with Microsoft Deutschland GmbH and academics from Saarland University, including the second author of this article.

(2) Use of AI in 'Internal Investigations'

German corporations oftentimes engage in 'internal investigations', in particular to seek non- or deferred-prosecution agreements in transnational prosecutions by (in particular) US authorities, but also in national quasi-criminal enforcement proceedings. In such 'internal investigations', it is of paramount importance to sift through vast amounts of (electronic) evidence for potential criminal activity. While that task was, in the past, usually given to junior staff in law offices, these tend to rely more and more on IT-enabled solutions to search through the data, potentially also making use of AI systems. Owing to the peculiar, oftentimes transnational focus of these tools, and insufficient information available on their specific use in Germany, we will not address these tools in further detail.

(3) AML and Hate Speech reporting obligations

A recent change in the German criminal law provision on money laundering (§ 261 StGB) also means that relevant actors have to report many more instances of suspicious activities to the German FIU (cf § 43 GwG); estimations range between several hundred thousand to millions of such reports per year.[190] In a similar vein, § 3a NetzDG[191] requires social media networks to report, to the Federal Criminal Police Office certain instances of illegal content in their networks. In case content within the social media network is reported to the network provider *and* there are concrete indications that this content is in violation of a number of criminal law provisions (eg, it threatens with the commission of a serious offence, it contains CSAM, or disturbs public peace by threatening to commit offences), the service provider must report this content and some meta-data to the BKA. Around 250.000 such reports are expected per year.[192]

To filter through these reports, to determine which point to criminal activity (and which do not), and to prioritise high-profile cases, the use of AI systems has been suggested, and – in relation to the FIU – reported to be already in use.[193] However, there is insufficient information available on the design, features and safeguards of such systems. [194] It should be noted again, however, that such systems would only flag reports as warranting particular attention: It remains the task and duty of the police and the public prosecution to evaluate whether a sufficient factual indication for a crime ('*Anfangsverdacht*') exists to initiate a criminal investigation; later on, all evidence must

[190] Cf Dominik Brodowski, 'Tue Böses und rede darüber – Geldwäscheverdachtsmeldungen und das Strafrecht' [2021] wistra 417. See also **1.1.4.(1)** above.

[191] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, as amended.

[192] BT-Drucks. 19/18470, 12.

[193] See already **1.1.4.(1)** above; see also Bock and Höffler (n 128) 262, referring to another research project lead by the ZAC NRW regarding a chat bot that can support to evaluate reports of online hate speech incidents.

[194] See already **1.1.4.(1)** above.

then be fully assessed by the prosecution (in its decision to bring charges) and by the court (when convicting a defendant).

3.2 Evidence produced by AI-based systems

So far, the use of AI-based systems hardly ever produces 'evidence' in the strict sense of the word (see **3.2.1** below). More often, it is used in German criminal justice for what *Bachmaier Winter* has coined as the 'building up of information positions',[195] that is as merely an intermediate step within a criminal investigation measure (see **3.2.2** below), or to assess (other) evidence (see **3.3** below).

3.2.1 AI-generated evidence as (digital) evidence

Generally speaking, the results and effects of an AI system may be introduced and used as evidence in a criminal proceeding same as any other (digital) evidence. Although German criminal procedure limits the *means* of evidence in trial to written documents, to visual inspection, and (expert) witnesses, it hardly puts any bounds to the *content* (and therefore the *admissibility*) of evidence, and *exclusionary rules* are the rare exception in criminal trials.[196] Instead, it puts high focus on the *assessment* of all of the evidence presented in court.[197] In relation to AI, there is no specific normative framework concerning these questions of evidentiary law, meaning the common standards apply.[198] It remains to be seen, however, whether the 'AI Act' proposed by the EU Commission[199] may lead to specific AI standards in the future.

To illustrate the approach taken in German criminal justice, let us assume that a car contains an AI-based 'drowsiness detection' system, and law enforcement authorities have launched a criminal investigation against the driver for negligently causing injury (§ 229 StGB) in a car accident. On this basis, the car (including the 'drowsiness detection' system) may be seized as evidence of relevance in the criminal investigation (§ 94 StPO). Then, forensic experts (from the police or independent) may forensically analyse this system,[200] print out raw data or reports from that system, and create diagrams showing how the driver got ever more sleepy. Such reports may then be introduced as written documents ('*Urkunden*') in the criminal trial, a diagram from the system may then be viewed as evidence by the court ('*Inaugenscheinnahme*'), and the forensic experts may be questioned as (expert) witnesses in court ('*Zeugenbeweis*' and

[195] Bachmaier Winter (n 171) 89–90.

[196] For a recent overview, see Steven Thaman and Dominik Brodowski, 'Exclusion or Non-Use of Illegally Gathered Evidence in the Criminal Trial: Focus on Common Law and German Approaches' in Kai Ambos and others (eds), *Core Concepts in Criminal Law and Criminal Justice*, vol 1 (CUP 2020) 428.

[197] See **3.3** below.

[198] One of the few limitations in German criminal procedure law is that the core area of private conduct of life must not be intruded; therefore, evidence pertaining to that is out of bounds. See already **3.1.1.(1)** above.

[199] COM (2021) 206 final (n 77).

[200] On the lack of a clear legal standard, see **3.1.2** above.

‘*Sachverständigenbeweis*’).[201] This highlights that the evidence in court is not the AI system itself or the electronic data stored therein, but always a *transformation*.[202] Any evidence introduced in trial then will be assessed by the court,[203] but its validity and significance can be questioned and brought into doubt by all participants of the trial. For instance, they may question the (expert) witnesses, they may introduce another (expert) witness to refute the other statement, or they may introduce scientific literature bringing the validity of the AI system into doubt.[204]

For intermediate decisions – such as on pre-trial detention or on ordering the taking of evidence, eg by a search of the defendant’s premises –, the same standard applies: the authorities in question (in particular the public prosecutor or the investigation judge) have to assess all the evidence, and also have to take conflicting evidence into account when making that assessment.

3.2.2 Building up of information positions using AI systems: the example of vehicle registration plate scanning

The ‘building up of information positions’ using AI systems is probably best described on the basis of a provision introduced in July 2021, § 163g StPO: To identify suspects of a specific crime of significant seriousness and within a specific criminal investigation,[205] and/or to apprehend them, authorities may automatically scan vehicle registration plates. This measure may only be used limited in time and regional scope. Importantly, the automatic scanning only serves as a first step: Without undue delay, the scanned vehicle registration codes have to be matched against a case-specific, limited list of known suspicious codes. In case the automatic system reports a match, this has to be

[201] Sabine Gless and Thomas Weigend, ‘Intelligente Agenten als Zeugen im Strafverfahren?’ [2021] JZ 612 consider findings of AI systems to constitute evidence *sui generis*. To overcome the difficulties of reliability and of explainability of AI-generated evidence, they propose certification, the interpretation by expert witnesses, and the use of artificial counter-intelligence to assess the validity of the presented evidence. In our view, the *introduction* of AI-generated evidence does not require a new category but can follow traditional means, while for the *assessment* of AI-generated evidence, the court must take its (lack of) reliability and explainability into account.

[202] On the need to transform data into evidence, just see Gless and Weigend (n 201) 614; Heinson (n 183) 113; Matthias Jahn and Dominik Brodowski, ‘Digitale Beweismittel in Hauptverhandlung und Revision’ in Bernd Hecker, Bettina Weißer and Christian Brand (eds), *Festschrift für Rudolf Rengier zum 70. Geburtstag* (Beck 2018) 409, 410–412; Laura Iva Savić, ‘Beweisführung mit digitalen Medien im Strafprozess. Im Vergleich und unter Berücksichtigung der ZPO und VwGO (sowie weiterer Rechtsvorschriften)’ in Almuth Buschmann and others (eds), *Digitalisierung der gerichtlichen Verfahren und das Prozessrecht* (Duncker & Humblot 2018) 71, 79–82; all with further references.

[203] See **3.3** below.

[204] Critically on the effectiveness of the existing procedural opportunities Gless and Weigend (n 201) 616–618; Sabine Gless, ‘AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials’ (2020) 51 GJIL 195, 247–249.

[205] This focus on a specific, already ongoing criminal investigation differentiates this measure from measures of preventive policing (see **1** above).

verified manually without undue delay. Otherwise, or in case the manual verification does not support the finding, the data has to be erased completely immediately (§ 163g [2] 4 StPO).

What is noteworthy here is that this approach results in full human oversight, as each and every match needs to be verified by a police officer, and only matches can result in further, specific measures in furtherance of the criminal investigation – for example, the identified car may be stopped down the road, and then the police will identify the suspect using 'traditional' means (ID papers, fingerprints, etc). Therefore, this automatic scanning merely helps in building up an information position, but does not serve as 'evidence' in a criminal trial itself.

In a similar vein, video systems for the biometric identification of (known) suspects were tested by German authorities for the purpose of apprehending them, once identified by such a system at a place of travelling (such as a train station).[206] This biometric identification would then not be used as evidence in a criminal trial, but only as an indication to apprehend the suspect and to identify them.

3.3 Evidence assessed through AI-based systems

In Germany, a defendant may only be convicted for an offence if there is objectively a high probability and if the judge(s) is/are subjectively convinced that the defendant committed the offence (§ 261 StPO). Therefore, the assessment of *all* evidence presented in a criminal trial is first and foremost a judicial prerogative in German criminal justice,[207] and cannot (as of now) and is unlikely to be deferred to an AI-based system in future. Unlike for DNA data, there is no precedent-based standard on how electronic evidence and its assessment (including AI-based assessments) are to be reported in judgments.

3.3.1 Assessment of an exhibit of evidence by additional evidence

In case the court lacks the expertise to fully assess a specific exhibit of evidence, it is required, as far as necessary to determine the 'material truth' (§ 244 [2] StPO), to obtain further evidence on the evidence. It is then required to introduce, as additional evidence in the trial, a report and/or statement by an expert witness addressing the validity of the exhibit. Same as any other evidence, such a report or statement may be brought into doubt by the participants of the trial.

To illustrate this, let us assume that a German criminal court needs to assess whether a document introduced as evidence in trial was forged. In case there are evident signs of

[206] See **1.1.3.(3)** above.

[207] Just see BVerfG, order of 26.08.2008 – 2 BvR 553/08 ECLI:DE:BVerfG:2008:rk20080826.2bvr055308 para 11–12 and **2.3.** above.

forgery recognisable by the court itself, it can refer to its own expertise and make use of this expertise in the assessment of the document, and convict the defendant of forgery. If there are no such evident signs of forgery, the court cannot simply upload the image to an online AI-based tool, and base its judgment on the result returned by the AI-based tool. Instead, it has to introduce *additional* evidence in trial: For instance, it could introduce a written document on the processing and evaluation of the document by an AI-based tool, or it could question an (expert) witness who has used an AI-based tool to assess whether the document was forged. Then, eg the defendants may take the validity of this *additional evidence* into doubt. They may argue, for instance, that this tool has a too high error rate as evidenced by a scientific review, that this expert lacks the specific knowledge necessary, or they may introduce a counter (expert) witness refuting the report by the first (expert) witness. Within this process, scientific standards, guidelines or 'soft law' provisions – such as evolving European guidelines on AI systems (see Annex III Section 6 lit d of the EU Commission's Proposal on an 'AI Act'[208]) – may be taken into account and strengthen (or weaken) the assessment of the evidence; yet such standards do not fully bind the criminal courts when assessing the evidence introduced in trial.

3.3.2 AI-based polygraphs

Although the court may generally introduce *additional* evidence to assess other exhibits of evidence, there is one noteworthy exception: According to jurisprudence by the German Federal Court of Justice, a polygraph is completely unsuitable as evidence, even if taken with the consent or upon request by the questioned person (defendant or witness), as there is '"no specific [physiological] lie response"'.[209] Recently, *Rodenbeck*[210] and *Ibold*[211] have discussed whether this same restriction holds true for AI-based determinations of the validity of a (defendant or witness) statement, which use measurements of non-verbal activities (such as facial movements) as input. As they rightly point out, the available tools do not (yet) reach a sufficient reliability for use in criminal justice;[212] in particular, advertised rates of 96% accuracy of such systems are based on a 'laboratory study' which does not properly reflect the situation within a criminal investigation.[213] Additionally, *Ibold* argues that the 'black-box' feature of current AI systems is incompatible with the constitutional requirement to explain and

[208] COM (2021) 206 final (n 77).

[209] BGH, judgment of 17.12.1998 – 1 StR 156/98 = BGHSt 44, 308, 316 (translation to English by the authors).

[210] Julian Rodenbeck, 'Lügendetektor 2.0 – Der Einsatz von Künstlicher Intelligenz zur Aufdeckung bewusst unwahrer Aussagen im Strafverfahren' [2020] StV 479.

[211] Victoria Ibold, 'Künstliche Intelligenz im Strafprozess – KI-basierte Lügendetektoren zur Tatsachenfeststellung?' (2022) 134 ZStW 504.

[212] Rodenbeck (n 210) 481–483.

[213] Ibold (n 211) 516–517, 522.

convey the rationale of judicial decision-making[214] – a requirement which secures against 'black-box' decisions in criminal justice, and which enhances the rationality and lawfulness of the criminal process.[215] However, *Rodenbeck* opines that such tools could, in future, be reliable enough to *assist* judges in their assessment of (witness) statements, and that the factual and legal requirements on their use yet require more thought.[216] Since the EU Commission listed both 'polygraphs and similar tools' and systems 'to detect the emotional state of a natural person' as high-risk applications in its proposal for an 'AI Act' (see Annex III Section 6 lit b)[217], the EU legislator might take a stance on these considerations in the not too far future.

4 Concluding remarks

The use of 'AI technology' is already present within the German criminal justice system. The technologies used today employ, more often than not, an algorithmic, deterministic, rule- and theory-based approach. In some notable instances, however, machine learning technology is starting to be used for the identification of dangerous objects or situations through video analysis and in the administration of criminal justice, in particular with a view to filter through vast amounts of raw evidence to find the 'needle in the haystack'. Compared to other high-profile criminal justice systems and their use of 'black-box', machine learning technology to 'predict' the future behaviour of suspects, accused persons and convicted criminals, the approach currently taken by the German criminal justice system is best described as nuanced and careful, even reluctant: There is widespread scepticism against vesting more trust in AI than in human decision-makers (in particular judges). This scepticism is, in particular, fuelled by the fear of 'black-box', unexplainable, and, in the end, irrational (eg biased) decision-making by machines. In addition, building upon its renowned jurisprudence on the protection of personal data, the German criminal justice system is still hesitant against the accumulation of vast amounts of data and its assessment by state authorities.

The legal framework for the use (or non-use) of AI technology in criminal justice is, at most, quite fragmentary, both at the federal and at the 'Länder' level. In particular, the instances where such technology is in use today are not governed by specific rules addressing the use of AI technology in detail, but tend to focus more on the implications to data protection and data usage. Jurisprudence is lacking as well; however, a number of pending cases – such as relating to HessenData[218] or PNR data[219] – will likely serve

[214] Ibold (n 211) 518–529.

[215] Ibold (n 211) 531–532.

[216] Rodenbeck (n 210) 483.

[217] COM (2021) 206 final (n 77).

[218] See **1.1.3.(2)** above.

[219] See **1.1.3.(1)** above.

as cornerstones in the future development of the legal framework on the use of AI in criminal justice.

Much more detailed frameworks, guidelines and statements on the use of AI in German criminal justice can be found in independent oversight bodies (such as on data protection), in expert groups, and legal literature. In contrast to some civil society organisations, these generally do not call for a ban of *all* AI technology outright, there is widespread consensus on the need for strong legal safeguards on the use of AI, in particular to avoid discrimination and effects of *bias*, to assert the explainability of AI technology as well as human oversight, and to preserve the rights to privacy, to data protection and to the inviolability of the core area of private conduct of life.[220] As AI technology of today – and in all likelihood also of the near future – lacks sufficient reliability, explainability, and rationality, there is a strong consensus that some instances of decision-making in criminal justice – ranging from the assessment of witness statements[221] to the sentencing of convicted criminals[222] – need to remain a *domaine réservé* for human decision-making (in particular by judges) for the time being.[223]

With criminal justice systems becoming ever more intertwined, however, our view is that a common trans- and international understanding of the chances, challenges, and risks of the use of AI in criminal justice is required. Building upon such a common understanding, a harmonised legal framework should preserve the human element to criminal justice, but also allow for the use of AI wherever it aligns with the goals and interests of criminal justice and as long as it is in compliance with a strong protection of human and fundamental rights. The 'AI Act' proposed by the European Commission,[224] which strives to regulate the use of AI in all EU criminal justice systems, as well as similar considerations at the Council of Europe,[225] promise to be an important step forward, although much of its content still warrants further discussion.

Selected Literature

Egbert S, 'Predictive Policing als Treiber rechtlicher Innovation?' (2021) 41 Zeitschrift für Rechtssoziologie 26

[220] See, in particular, **1.2.1.(4)** above.

[221] See **3.3.2.** above

[222] See **2.3.** above

[223] See, in particular, **1.2.1.(4), 2.3.** and **3.3.2.** above

[224] COM (2021) 206 final (n 77).

[225] See report of the Council of Europe Ad hoc Committee on Artificial Intelligence (CAHAI) dated 17 December 2021, document CM(2021)173-add, <https://rm.coe.int/possible-elements-of-a-legal-framework-on-artificial-intelligence/1680a5ae6b> accessed 9 August 2022.

Eisbach, S, Heghmanns M and Hertel G, ‘Künstliche Intelligenz im Strafverfahren am Beispiel von Kriminalprognosen’ [2022] ZfIStw 489

Esser R and Reißmann L, ‘Schutz des Kernbereichs privater Lebensgestaltung durch den Einsatz künstlicher Intelligenz (KI) – Neue Perspektiven für Strafverfolgung und Gefahrenabwehr’ [2021] StV 526

Gless S, ‘AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials’ (2020) 51 GJIL 195

Gless S and Weigend T, ‘Intelligente Agenten als Zeugen im Strafverfahren?’ [2021] JZ 612

Greco L, ‘Richterliche Macht ohne richterliche Verantwortung: Warum es den Roboter-Richter nicht geben darf’ [2020] Rechtswissenschaft 29

Ibold V, ‘Künstliche Intelligenz im Strafprozess – KI-basierte Lügendetektoren zur Tatsachenfeststellung?’ (2022) 134 ZStW 504

Jahn M and Brodowski D, ‘Digitale Beweismittel in Hauptverhandlung und Revision’ in Hecker B, Weißer B and Brand C (eds), *Festschrift für Rudolf Rengier zum 70. Geburtstag* (Beck 2018) 409

Kohn B, *Künstliche Intelligenz und Strafzumessung* (Nomos 2021)

Lind F, *Das raumbezogene Predictive Policing in Deutschland. Der aktuelle rechtliche Rahmen und seine Indikationen für Weiterentwicklungen des Einsatzes prädiktiver Analytik bei präventiv polizeilichem Handeln* (forthcoming)

Rademacher T, ‘Verdachtsgewinnung durch Algorithmen. Maßstäbe für den Einsatz von predictive policing und retrospective policing’ in Zimmer D (ed) *Regulierung für Algorithmen und Künstliche Intelligenz* (Nomos 2019) 229

Rodenbeck J, ‘Lügendetektor 2.0 – Der Einsatz von Künstlicher Intelligenz zur Aufdeckung bewusst unwahrer Aussagen im Strafverfahren’ [2020] StV 479

Rostalski F, ‘Judex ex machina? Zum Einsatz neuer Technologien in der Rechtsfindung’ in Hoven E and Kudlich H, *Digitalisierung und Strafverfahren* (Nomos 2020) 263

Sommerer LM, *Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control* (Nomos 2022)

Sprenger J, ‘Verbrechensbekämpfung’ in Ebers M and others (eds), *Künstliche Intelligenz und Robotik* (Beck 2020)