18

Legal, Ethical, and Social Issues of AI and Law Enforcement in Europe

The Case of Predictive Policing

Rosamunde Van Brakel

18.1 INTRODUCTION

Artificial intelligence (AI)[1] increasingly plays a role within law enforcement. According to Hartzog et al., "*[w]e are entering a new era when large portions of the law enforcement process may be automated … with little to no human oversight or intervention*."[2] The expansion of law enforcement use of AI in recent years can be related to three societal developments: austerity measures and a push toward using more cost-effective means; a growing perception that law enforcement should adopt a preventive or preemptive stance, with an emphasis on anticipating harm; and, finally an increase in the volume and complexity of available data, requiring sophisticated processing tools, also referred to as Big Data.[3]

AI is seen as providing innumerable opportunities for law enforcement. According to the European Parliament, AI will contribute "*to the improvement of the working methods of police and judicial authorities, as well as to a more effective fight against certain forms of crime, in particular financial crime, money laundering and terrorist financing, sexual abuse and the exploitation of children online, as well as certain types of cybercrime, and thus to the safety and security of EU citizens*."[4] Some of the main current applications include predictive policing (see further), traffic control

[1] For an overview of AI as a technology, see Chapter 1 of this book.

[2] Woodrow Hartzog, Gregory Conti, John Nelson, and Lisa A. Shay, "Inefficiently automated law enforcement" (2016) *Michigan State Law Review* 2015: 1763–1796.

[3] Alexander Babuta en Marion Oswald, "Machine learning predictive algorithms and the policing of future crimes: governance and oversight," in *Policing and Artificial Intelligence*, ed John L. M. McDaniel and Ken Pease (London: Routledge, 2021), 214–236; Rosamunde Van Brakel, pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing, in Bart van der Sloot, Dennis Broeders, and Erik Schrijvers (eds) *Exploring the Boundaries of Big Data* (Amsterdam University Press, 2016), 117–141.

[4] European Parliament, European Parliament resolution of October 6, 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

(automated license plate detection and vehicle identification),[5] cybercrime detection (analysis of money flows via the dark web/ detection of online child abuse),[6] and smart camera surveillance (facial recognition and anomaly detection).[7]

The goal of this chapter is to introduce one type of AI used for law enforcement: predictive policing and discuss the main concerns this raises. I first examine how predictive policing emerged in Europe and discuss its (perceived) effectiveness (Section 18.2). Next, I unpack, respectively, the legal, ethical, and social issues raised by predictive policing, covering aspects relating to its efficacy, governance, and organizational use and the impact on citizens and society (Section 18.3). Finally, I provide some concluding remarks (Section 18.4).

18.2 PREDICTIVE POLICING IN EUROPE

18.2.1 *The Emergence of Predictive Policing in Europe*

The origins of predictive policing can be found in the police strategy "Intelligence-led policing", which emerged in the 1990s in Europe.[8] Intelligence-led policing can be seen as "*a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders.*"[9] One of the developments within intelligence-led policing was prospective hotspot policing, which focused on developing prospective maps. Using knowledge of crime events, recorded crime data can be analyzed to generate an ever-changing prospective risk surface.[10] This then led to the development of one of the first predictive policing applications in the United Kingdom,

[5] Kirstie Ball, "Search and identify: Automatic Number Plate Recognition in Europe" in Kirstie Ball and William Webster (eds), *Surveillance and Democracy in Europe* (London: Routledge, 2019); Francesco Ragazzi, Elif Kuskonmaz, Ildikó Plájás, Ruben van de Ven, and Ben Wagner *Biometric and behavioural mass surveillance in EU member states: report for the Greens/EFA in the European Parliament* (Greens/EFA, 2021), https://scholarlypublications.universiteitleiden.nl/handle/1887/3256585.

[6] Stephan Raaijmakers, "Artificial Intelligence for law enforcement: challenges and opportunities" (2019) *IEEE Security & Privacy* 17(5): 74–77.

[7] Rosamunde Van Brakel, "Democratic oversight of algorithmic police surveillance in Belgium" (2021a) *Surveillance & Society*, 19(2): 228–240; Peter Fussey and Darragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. (Human Rights and Big Data Project, University of Essex July 2019), https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf.

[8] Mike Maguire, "Policing by risks and targets: some dimensions and implications of intelligence-led crime control" (2000) *Policing and Society*, 9: 315–336; Paul De Hert, Wim Huisman and T. Vis (2005) "Intelligence Led Policing ontleed" (2005) *Tijdschrift voor Criminologie* 4(48): 365–376.

[9] Jerry H. Ratcliffe, *Intelligence-Led Policing* (Portland, OR: Willan, 2008).

[10] Kate. J. Bowers, Shane D. Johnson, and Ken Pease, "Prospective hot-spotting: the future of crime-mapping?" (2004) *British Journal of Criminology*, 44(5): 641–658.

known as ProMap.[11] Early in the twenty-first century, the rise of the use of predictive machine learning led to what is now known as predictive policing.

Predictive policing refers to "any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention."[12] It is a strategy that can be situated in a broader preemptive policing model. Preemptive policing is specifically geared to gather knowledge about what will happen in the future with the goal to intervene before it is too late.[13] The idea behind predictive policing is that crime is predictable and that societal phenomena are, in one way or another, statistically and algorithmically calculable.[14]

Although already being implemented since the beginning of the twenty-first century in the United States (US), Law Enforcement Agencies in Europe are increasingly experimenting with and applying predictive policing applications. Two types can be identified: predictive mapping and predictive identification.[15] According to Ratcliffe, predictive mapping refers to "*the use of historical data to create a spatiotemporal forecast of areas of criminality or crime hot spots that will be the basis for police resource allocation decisions with the expectation that having officers at the proposed place and time will deter or detect criminal activity*."[16] Some law enforcement agencies use or have used software developed by (American) technology companies such as PredPol in the UK and Palantir in Denmark, while in other countries, law enforcers have been developing their own software. Examples are the Criminality Awareness System (CAS) in the Netherlands, PRECOBS in Germany, and a predictive policing algorithm developed in Belgium by criminology researchers in cooperation with the police.[17] Predictive mapping applications have in most cases focused on predicting the likelihood that a certain area is more prone to burglaries and adjusting patrol management according to the predictions.

[11] Shane D. Johnson, Kate J. Bowers, Dan J. Birks, and Ken Pease, "Predictive mapping of crime by Promap: accuracy, units of analysis and the environmental backcloth," in David Weisburd, Wim Bernasco, and Gerben J. N. Bruinsma (eds), *Putting Crime in Its Place* (Dordrecht: Springer, 2009), 171–198.

[12] Craig D. Uchida (2009) "Predictive policing," in *Encyclopedia of Criminology and Criminal Justice* (Dordrecht: Springer, 2009), 3871–3880.

[13] Rosamunde van Brakel and Paul De Hert "Policing, surveillance and law in a pre-crime society: understanding the consequences of technology based strategies" (2011) *Cahiers Politiestudies/ Journal of Police Studies*, 20(3): 163–192; Lyria Bennett Moses and Janet Chan "Algorithmic prediction in policing: assumptions, evaluation, and accountability" (2018) *Policing and Society*, 28(7): 806–822.

[14] Simon Egbert and Susann Krasmann (2019) "Predictive policing: not yet, but soon preemptive?" *Policing and Society*, 30(8): 905–919.

[15] Van Brakel, 2016, see note 3.

[16] Jerry H. Ratcliffe, "What is the future … of predictive policing?" *Translational Criminology* (Spring 2014): 4.

[17] Rosamunde Van Brakel, "Rethinking predictive policing towards a holistic framework of democratic algorithmic surveillance," in Marc Schuilenberg and Rik Peeters (eds), *The Algorithmic Society: Technology, Power, and Knowledge* (London: Routledge, 2021b) 104–118.

Predictive identification has the goal to predict who is a potential offender, the identity of offenders, criminal behavior, and who will be a victim of crime.[18] These types of technologies build upon a long history of using risk assessments in criminal justice settings.[19] The difference is that the risk profiles are now often generated from patterns in the data instead of coming from scientific research.[20] This type of predictive policing has been mainly applied in Europe in the context of predicting the likelihood of future crime (recidivism). However, other examples can be found in the use of video surveillance that deploys behavior and gait recognition. There are also developments in lie and emotion detection,[21] the prediction of radicalization on social media,[22] passenger profiling, and the detection of money laundering.[23] A recent example can be found in the Netherlands where Amsterdam police uses what is known as the Top400. The Top400 targets 400 young "high potentials" in Amsterdam between twelve and twenty-four years old "that have not committed serious offences but whose behavior is considered a nuisance to the city."[24] In the context of the Top400, the ProKid+ algorithm has been used to detect children up to sixteen years old that could become "a risk" and might cause future crime related problems. When on the list, youngsters receive intensive counseling and they and their families are under constant police surveillance.[25]

18.2.2 *Effectiveness of Predictive Policing*

Evaluations of the effectiveness of predictive policing in preventing crime have, so far, been inconclusive due to a lack of evidence.[26] In addition, not all evaluations

[18] Van Brakel, 2016, see note 3.

[19] Van Brakel, 2021b, see note 17.

[20] Rosamunde Van Brakel, *Taming the Future? A Rhizomatice Analysis of Pre-emptive Surveillance of Children* unpublished PhD thesis (Vrije Universiteit Brussel, 2018).

[21] Javier Sánchez-Monedero and Lina Dencik, "The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl" (2022) *Information, Communication and Society*, 25(3): 413–430.

[22] Miriam Hernandez and Harith Alani, "Artificial intelligence and online extremism: challenges and opportunities" in John McDaniel and Ken Pease (eds), *Predictive Policing and Artificial Intelligence* (London: Routledge, 2021).

[23] Plixavra Vogiatzoglou, "Mass surveillance, predictive policing and the implementation of the CJEU and ECtHR requirement of objectivity" (2019) *The European Journal of Law and Technology*, 10(1): 1–18.

[24] Fieke Jansen, *Top400: A Top-Down Crime Prevention Strategy in Amsterdam*. Report, Project Interest Litigation Project, The Netherlands (November 2022): 5.

[25] Rosamunde Van Brakel and Lander Govaerts, "Exploring the impact of algorithmic policing on social justice: Developing a framework for rhizomatic harm in the pre-crime society" *Theoretical Criminology*, OnlineFirst, https://doi.org/10.1177/13624806241246267.

[26] For an overview of evaluations conducted in the US, see Van Brakel, 2021b, note 17. While writing this ` an evaluation was conducted by investigative journalists of the use of Geolitica software (previously Predpol). They examined 23,631 predictions generated by Geolitica between February 25 to December 18, 2018, for the Plainfield Police Department (PD). They noted that: "*each prediction we analyzed from the company's algorithm indicated that one type of crime was likely to occur*

have been conducted in a reliable way, and with general falling crime rates, it is hard to show that fall in crime is the result of the technology. Moreover, it is difficult to evaluate the technology's effectiveness in preventing crime as algorithms identify correlations, not causality.

For instance, the Dutch Police Academy concluded in their evaluation of the CAS system that it does seem to prevent crime but that it does have a positive effect on management.[27] The evaluation study conducted by the Max Planck Institute in Freiburg of a PRECOBS pilot-project in Baden-Württemberg concluded that it remains difficult to judge whether the PRECOBS software is able to contribute toward a reduction in home burglaries and a turnaround in case development. The criminality-reducing effects were only moderate and crime rates could not be clearly minimized by predictive policing on its own.[28] In Italy, reliability of 70 percent was found for the predictive algorithm of KEYCRIME which predicted which specific areas in Milan would become a crime hotspot.[29] In their overview of recent challenges and developments, Hardyns and Rummens did not find significant effects of predictive policing and argue that more research is needed to assess the effectiveness of current methods.[30]

Apart from inconclusive evaluations, several police forces stopped using the software altogether. For instance, the use of PredPol by Kent Police was discontinued in 2019 and the German police forces of Karlsruhe and Stuttgart decided to stop using PRECOBS software because there was insufficient crime data to make reliable predictions.[31] Furthermore, amid public outcry about the use of PredPol, the Los Angeles Police Department in the US stopped using the software, yet at the same time it launched a new initiative: "data-informed community-focused policing

in a location not patrolled by Plainfield PD. In the end, the success rate was less than half a percent. Fewer than 100 of the predictions lined up with a crime in the predicted category that was also later reported to police." See Aaron Sankin and Surya Mattu, Predictive Policing Software Terrible At Predicting Crimes, *The Markup* (October 2, 2023), https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes.

[27] Bas Mali, Carla Bronkhorst-Giesen and Mariëlle Den Hengst. *Predictive policing: Lessen voor de toekomst*, *Politieacademie* (2017) www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93263.PDF.

[28] 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 of Security Research*, 3: 115–138.

[29] Bogolomov, Andrey, Lepri, Bruno, Staiano, Jacopo, Oliver, Nuria, Pianesi, Fabio and Pentland, Alex, Once Upon a Crime: Towards Crime Prediction from Demographics and Mobile Data, ACM International Conference on Multimodal Interaction (ICMI, 2014).

[30] Hardyns Wim and Rummens Anneleen, Predictive policing as a new tool for law enforcement? Recent developments and challenges (2017) *European Journal of Criminal Policy and Research*, 24: 201–218.

[31] Nils Mayer, Strobl entscheidet sich gegen Precobs, Stuttgarter Nachrichten (September 3, 2019), www.stuttgarter-nachrichten.de/inhalt.aus-fuer-die-einbruchvorhersage-softwarestrobl-entscheidet-sich-gegen-precobs.19a18735-9c8f-4f1a-bf1b-80b6a3ad0142.html.

(DICFP)."[32] The goal of this initiative is to establish a deeper relationship between community members and police, and to address some of the concerns the public had with previous policing programs. However, critics have raised questions about the initiative's similarities with the use of PredPol.[33] Similar to PredPol, the data that is fed into the system is biased and often generated through *feedback loops*. Feedback loops refers to a phenomenon identified in research that police are repeatedly sent back to the same neighborhoods regardless of the true crime rate.[34]

Regarding *predictive identification*, almost no official evaluations have been conducted. Increasingly, investigative journalists and human rights organizations are showing that there is significant bias in these systems.[35] Moreover, issues that have been raised with the effectiveness of actuarial risk assessment methods before it was digitalized, such as the (un)reliability of the risk factor research that underscores the applied theories of crime, are not solved by implementing algorithmic decision-making.[36] As to the use of *predictive analytics* in this area, the effectiveness of these systems likewise remains unclear. An assessment of a predictive model used by Los Angeles' children's services, which was promoted as highly effective in practice, "produced a false alarm 96 percent of the time."[37]

In general, the effectiveness concerns that were already identified for (prospective) hot-spot policing on the one hand and traditional risk assessments on the other, prior to the implementation of AI systems, did not disappear. With regards to predictive mapping spatial displacement, which is when crime moves to a different area after implementing a control measure such as CCTV or increased police presence is but one example.[38] It should also be noted that the long-term impacts of predictive policing on individuals and society are unclear and longitudinal research assessing

[32] Michel R. Moore, Data-Informed Community-Focused Policing in the Los Angeles Police Department (2018) https://lapdonlinestrgeacc.blob.core.usgovcloudapi.net/lapdonlinemedia/2021/12/data-informed-guidebook-042020.pdf (2019).

[33] Johana Bhuiyan, LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws *The Guardian* (November 8, 2021), www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform.

[34] Danielle Ensign, Sorelle Friedler, Scott Neville, Carlos Sheidegger, and Suresh Venkatasubramanian, Runaway feedback loops in predictive policing (2018) *Conference on Fairness, Accountability, and Transparency. Proceedings of Machine Learning Research*, 81: 1–12.

[35] Julia Angwin, Jeff Larson, Surya Mattu, Lauren Kirchner, Machine Bias, *ProPublica* (2016) www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Liberty *Policing by Machine*, Predictive policing and the threat to our rights (2019), www.libertyhumanrights.org.uk/issue/policing-by-machine/.

[36] Van Brakel, 2018, see note 20; Babuta and Oswald, 2020, see note 3. See also SyRI judgement in the Netherlands, ECLI:NL:RBDHA:2020:1878, https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:1878.

[37] Christopher E. Church and Amanda J. Fairchild, In search of a silver bullet: child welfare's embrace of predictive analytics (2017) *Juvenile & Family Court Journal*, 68(1): 71.

[38] David Weisburd, Laura A. Wyckoff, Justin Ready, John E. Eck., Joshua C. Hinkle, and Frank Gajewski, Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits (2006) *Criminology*, 44(3): 549–592.

this is not conducted. Finally, as demonstrated by the earlier overview, it is unclear if the adoption of predictive mapping will reduce overall crime, and whether it will be able to do so for different types of crime.[39]

18.3 A LEGAL, ETHICAL, AND POLICY ANALYSIS OF PREDICTIVE POLICING

18.3.1 *Legal Issues*

The European Union regulation on AI, published by the European Commission in 2024, provides numerous safeguards depending on how much risk a certain AI application poses to fundamental rights.[40] As Chapter 12 of this book more extensively explains, the AI Act classifies AI systems into several categories, including low or limited risk (not subject to further rules), medium/opacity risk (with new transparency obligations), high risk (with a broad set of conformity assessment requirements), and unacceptable risk (which are prohibited).

In its amendments published in June 2023, the European Parliament clearly opted for stricter safeguards by removing exceptions for law enforcement's use of real-time remote biometric identification systems, and prohibiting some applications that the Commission had previously classified as high risk, such as predictive policing, and more specifically predictive identification applications used in criminal justice.[41] However, ultimately, the final text provides extensive exceptions for law enforcement when it comes to real-time remote biometric identification systems[42] and does not prohibit place-based predictive policing. It does prohibit predictive identification in so far the risk assessments are solely based on the "profiling of a natural person or on assessing their personality traits and characteristics."[43] It remains to be seen to what extent the interpretation, implementation, and enforcement of the regulation will provide sufficient democratic safeguards to protect the fundamental rights of citizens.

In addition to the AI regulation, the use of AI for law enforcement purposes is also regulated by the transposition into national laws of member states of the Law

[39] David Weisburd and Cody W. Telup, Hot spots policing: what we know and what we need to know (2014) *Journal of Contemporary Criminal Justice*, 30(2): 200–220.

[40] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[41] Amendment 224, Article 5(1d a). Amendments adopted by the European Parliament on June 14, 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

[42] Article 5(1h) Artificial Intelligence Act.

[43] Article 5(1d) Artificial Intelligence Act.

Enforcement Directive (LED).[44] The application of this directive concerns the processing of personal data by competent authorities for the prevention, investigation, detection, and prosecution of criminal offenses or the execution of criminal penalties.[45] It does not apply in the context of national security, to EU institutions, agencies, or bodies such as Europol, and it only applies to processing of personal data wholly or partly by automated means. The directive came about primarily out of the need felt by law enforcement agencies, including in response to terrorist attacks in the US and Europe in the first decades of the twenty-first century, to exchange data between member states. The directive, therefore, aims to strike a balance between law enforcement needs and the protection of fundamental rights.[46]

The focus of the directive is on "personal data." This is defined as "any information relating to an identified or identifiable natural person ('data subject')."[47] An identifiable natural person is one who can be "identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person."[48] Already in 2007 the European advisory body, the Data Protection Working Party Article 29 (WP29),[49] proposed a very broad interpretation of personal data: "any information" includes not only objective and subjective information, but even false information. It does not just concern private or sensitive information.[50] Information can be associated with an individual in three ways: (1) content (when it is about a particular person); (2) purpose (when data is used to evaluate, treat, or influence an individual's status or behavior in a certain way) and (3) result (when it is likely to have an impact on the rights and interests of a particular person taking into account all the circumstances of a particular case).[51]

It is often questioned, especially by law enforcement agencies themselves, if predictive mapping applications process "personal data." Lynskey argues that based

[44] Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive).

[45] Article (1), Law Enforcement Directive.

[46] Paul De Hert and Vagelis Papakonstantinou The new police and criminal justice data protection directive (2016) *New Journal of Criminal Law*, 7(1): 7–19.

[47] Article (3)1, Law Enforcement Directive.

[48] Art. 3(1) Law Enforcement Directive.

[49] The Article 29 Data Protection Working Party (Art 29 WP) was established by Directive 95/46/EC. It dealt with issues relating to the protection of privacy and personal data until May 25, 2018 when the GDPR entered into force. From then on, the European Data Protection Board (EDPB) took over its role.

[50] The Article 29 Data Protection Working Party Opinion on the concept of Personal Data 01248/07/EN WP 136 2007 See also Case C-434/16, Nowak v. Data Protection Commissioner EU:C:2017:994.

[51] Orla Lynskey, Criminal justice profiling and EU data protection law: precarious protection from predictive policing, *International Journal of Law in Context* (June 2019): 162–176.

on the advice of WG 29 and case law, it is possible to conclude that data processing in predictive mapping involves the processing of personal data.[52] The data processed are potentially linked to the data subject because of the purpose (to treat people in a certain way) or the effect (impact on those identified in the hotspots). Regarding predictive identification, it is clearer that personal data are processed, both when it comes to the input data (as the content concerns the data subject) and the output data (as the purpose and effect of the data are used to influence the prospects of an identified individual). In practice, however, interpretations diverge. For instance, in the case of the CAS system in the Netherlands, the Dutch law enforcement authority nevertheless concluded that it is not processing personal data and, therefore, that the data protection regulation does not apply to the system's use.[53] This example shows that lack of clear guidance and specific regulation when it comes to the use of AI by law enforcement raises questions about the effectiveness of the current legislative safeguards for these applications.

18.3.2 *Ethical and Social Issues*

Predictive policing raises several ethical and social issues. These issues are dependent on what type of technology is implemented and the way the technologies are governed.[54] They can not only impact the effectiveness and efficacy of the technology, but they can also cause harm.[55] Below, I respectively discuss concerns pertaining to efficacy, governance, organization, and individual and social harms.

18.3.2.1 Efficacy

Several issues can be identified as regards the efficacy of predictive policing and of the use of AI by law enforcement more generally. Efficacy refers to the capacity to produce a desired result (in the case of predictive policing, a reduction in crime). First, law enforcement and technology companies often claim that the accuracy of the system's prediction is high. However, these claims of "predictive accuracy" are often mistaken for efficacy, whereas the level of accuracy does not say anything about the system's impact on crime reduction, making it difficult for a police force to assess a tool's real-world benefits.[56] Second, the way the AI system is designed and purposed

[52] Lynskey, 2019, see note 52.

[53] Interview conducted with representative Amsterdam police in the context of the WRR Big Data, privacy and security project (2015), www.wrr.nl/adviesprojecten/big-data-privacy-en-veiligheid.

[54] Van Brakel, 2018, see note 20; Rosamunde Van Brakel, Hartmut Arden, Elisabeth Aston, Sharda Murria, and Zjelko Kerras, "The possibilities and pitfalls of the use of accountability technologies in the governance of police stops" in Elizabeth Aston, Sofie De Kimpe, Janos Fazekas, Genevieve Lennon and Mike Rowe (eds) *Governing Police Stops Across Europe* (Palgrave MacMillan, 2023).

[55] van Brakel, 2021b, see note 17; Van Brakel and Govaerts 2024, see note 25.

[56] Babuta and Oswald, 2020, see note 3.

is largely driven by data science and technology companies, with comparatively little focus on the underlying conceptual framework, criminological theory, or legal requirements.[57] Third, specifically with regards to predictive policing, runaway feedback loops are a significant issue (see previous text).[58] Fourth, lack of transparency in the way algorithms are designed and implemented, the exact data, formulas, and procedures carried out by the software developers and the way the AI system works ("the black box"[59]) makes it harder to evaluate its operation. It also makes it more difficult for independent researchers to replicate methods using different data.[60] Fifth, the role of technology companies can also have an impact on efficacy.

A first example arises when law enforcement authorities work with software developed by (non-EU) technology companies. Such companies often foresee a vendor lock in the software, which implies that law enforcement is not able to adjust or tweak the software themselves and are dependent on the companies for any changes. A second example is that cultural differences and/or translation issues can arise when buying software from other countries. For instance, in Denmark, a hospital invested in a digital hospital management system, EPIC, developed by an American company.[61] The software was translated into Danish using Google Translate and this led to significant errors. This was not merely a translation issue. In fact, the "design of the system was so hard-coded in U.S. medical culture that it couldn't be disentangled," hence making it problematic for use in a Danish context.[62] A third example is that technology companies can also have an impact on how predictive policing is regulated. To provide another example from Denmark: The Danish government recently adjusted its police law to enable the use of an intelligence-led policing platform developed by Palantir.[63] Finally, a lack of academic rigor can be identified in this field. Since there are not many publications by researchers evaluating and testing predictive policing applications, there is still little reliable evidence on whether it works.[64] The lack of scientific evidence raises questions about the legitimacy and

[57] Ibid.

[58] Ensign, Friedler, Neville, Sheidegger, and Venkatasubramanian, 2018, see note 34.

[59] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Boston MA: Harvard University Press, 2015).

[60] Van Brakel, 2016, see note 3; Rachel B. Santos, Critic: Predictive policing: where's the evidence? In David Weisburd and Anthony A. Braga (eds) *Police innovation: contrasting perspectives* (Cambridge University Press, 2019): 366–396.

[61] See the website of EPIC: https://open.epic.com/CountrySpecific/Denmark.

[62] Morten Hertzum, Gunnar Ellingsun and Åsa Cajander, Implementing large-scale electronic health records: experiences from implementations of Epic in Denmark and Finland, *International Journal of Medical Informatics*, 167.

[63] See nr 671 af 08/06/2017 Lov om ændring af lov om politiets virksomhed og toldloven. EDRI New legal framework for predictive policing in Denmark, https://edri.org/our-work/new-legal-framework-for-predictive-policing-in-denmark/.

[64] National Academies Sciences, Engineering, Medicine, Law Enforcement Use of Predictive Policing Approaches: A Workshop, June 24-25, 2024, www.nationalacademies.org/event/42513_06-2024_law-enforcement-use-of-predictive-policing-approaches-a-workshop-public-session; Santos, 2019, see note 59.

proportionality of the application of predictive policing. When law enforcement deploys technology that poses an intrusion of fundamental rights law, law enforcement needs to demonstrate the necessity for the application in a democratic society and proportionality. However, considering the earlier discussion, that there is insufficient proof to show the efficacy and effectiveness of the technology the question arises if the fundamental rights test can be conducted in a reliable way and if the implementation of such technologies is justifiable.

18.3.2.2 Social Issues

There is increasing scientific evidence that AI applications and the poor-quality data the algorithms are trained on are riddled with error and bias.[65] They raise social and ethical concerns beyond undermining privacy and causing individual harm such as discrimination, stigmatization and social harms,[66] but they also can have an impact on society.[67] Predictive policing is a form of surveillance. Research in surveillance studies has shown that digital (police) surveillance potentially leads to several unintended consequences that go beyond a violation of individual privacy. For instance, surveillance can lead to social sorting cumulative disadvantage, discrimination, and chilling effects, but also fear, humiliation, and trauma.[68] Importantly, the harms raised by AI-driven predictive policing are also increasingly becoming cumulative through the significant increase of the more general implementation of surveillance in society.[69]

[65] Van Brakel, 2016, see note 3; Kristen Lum and William Isaac, To predict and serve? (2016) *Significance Magazine Royal Statistical Society*, 13(5): 14–19, Andrew G. Ferguson, *The Rise of Big Data Policing* (New York: NYU Press, 2017); Patrick Williams and Erik Kind, Data-driven policing: The hardwiring of discriminatory policing practices across Europe. Report, ENAR (March 2019); Rashida Richardson, Jason Schultz and Kate Crawford, Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice (2019) *New York University Law Review*, 94: 192–233; Babuta and Oswald, 2020, see note 3.

[66] Van Brakel, 2016, see note 3; Mali, Bronkhorst-Giesen and Den Hengst, 2017; Ferguson, 2017; Santos, 2019, see note 59; Egbert, Simon and Krasmann, Susanne, Predictive policing: not yet, but soon preemptive? (2019) *Policing & Society*, 30(8): 905–919; Fussey and Murray, 2019, see note 7; Van Brakel and Govaerts, 2024, see note 25.

[67] Nathalie A. Smuha, "Beyond the individual: governing AI's societal harm" (2021) *Internet Policy Review*, 10(3): https://policyreview.info/articles/analysis/beyond-individual-governing-ais-societal-harm; Van Brakel 2022, see note 72.

[68] David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination* (London: Routledge, 2003); Gandy Jr., O. H. (2009) *Coming to Terms With Chance: Engaging Rational Discrimination and Cumulative Disadvantage*, London: Ashgate; Jonathon W. Penny, Understanding Chilling Effects (2022) *Minnesota Law Review*: 1451–1530; Daragh Murray Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki, and Amy Stevens, The chilling effects of surveillance and human Rights: insights from qualitative research in Uganda and Zimbabwe (2023) *Journal of Human Rights Practice*: 1–16; John Gilliom, *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy* (Chicago University Press, 2001).

[69] Thomas Mitchener-Nissen, Failure to collectively assess security surveillance technologies will inevitably lead to an absolute surveillance society (2014) *Surveillance & Society*, 12(1): 73–88.

More specifically, in the United Kingdom, a recent study concluded that national guidance is urgently needed to oversee the use of data-driven technology by law enforcement amid concerns that it could lead to discrimination.[70] In the US an example of harms of predictive policing can be found in a lawsuit that has been filed against Pasco County Sheriff's Office (PCSO) in Florida.[71] This concerns a predictive policing application which, without notice to parents and guardians, places hundreds of students on a secret list, created using an algorithmic risk assessment identifying those who they believe are most likely to commit future crimes. When children are on the list, they are subject to persistent and intrusive monitoring. The criteria used to target children for the program are believed to have a greater impact on Black and Brown children.[72] Similarly, in the Netherlands a mother of a teenage boy, who was taken up in the Top400 list (see earlier content), states that as the result of police harassment she feels "like a prisoner, watched and monitored at every turn, and I broke down mentally and physically, ending up on cardiac monitoring."[73]

When law enforcement's use of AI systems leads to these harms, this will also have an impact on police legitimacy. As was already mentioned when discussing hot-spot policing, intensive police interventions may erode citizen trust in the police and lead to fear through over-policing, and thus lead to the opposite result of what the technology is intended for.[74]

18.3.2.3 Governance

AI has been heralded as a disruptive technology. It puts current governance frameworks under pressure and is believed to transform society in the same way as electricity.[75] It is therefore no surprise that several concerns arise around the governance structure of this disruptive technology when it is used to drive predictive policing. First, there is a lack of clear guidance and codes of practice outlining appropriate constraints on how law enforcement should trial predictive algorithmic

[70] Babuta & Oswald, 2020, see note 3.

[71] CAIR Florida, Inc vs Christopher Nocco, Sherrif of Pasco County, 13 09 2022, www.splcenter.org/sites/default/files/petition_-_pages_1_to_144.pdf. Another lawsuit is in process against the Sherrif for another type of predictive policing program as well: Case: Taylor v. Nocco 8:21-cv-00555 | U.S. District Court for the Middle District of Florida, https://clearinghouse.net/case/18194/.

[72] The Southern Poverty Law Centre Civil Rights Groups sue for public records linke dot Pasco County's predictive policing program (September 14, 2022) www.splcenter.org/presscenter/civil-rights-groups-sue-public-records-linked-pasco-countys-predictive-policing-program.

[73] Diana Sardjoe, My sons were profiled by a racist predictive policing system – the AI Act must prohibit these systems, *Medium* (September 28, 2022), https://medium.com/@FairTrials/my-sons-were-profiled-by-a-racist-predictive-policing-system-the-ai-act-must-prohibit-these-b2ea66a9a763.

[74] Dennis P Rosenbaum, The limits of hot spots policing. *Police Innovation: Contrasting Perspectives*: 245–263 (Cambridge University Press, 2006).

[75] Shana Lynch, Why AI is the new electricity? www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity, *Insights by Stanford Business* (March 11, 2017).

tools[76] and implement them in practice.[77] Second, there is a lack of quality standards for evaluations of these systems.[78] Whenever evaluations do take place, there is still a lack of attention to data protection and social justice issues, which also impact evidence-based policy that is based on such evaluations.[79] Third, there is a lack of expertise within law enforcement and oversight bodies,[80] which raises issues about how effective the oversight over these systems really is.

Finally, even when predictive machine learning does not process personal data or where it is compliant with the LED, there are still other concerns as we discussed earlier. These social and ethical concerns need to be addressed through innovative oversight mechanisms that go beyond judicial oversight.[81] Current oversight mechanisms are geared to compliance with data protection law, they do not address ethical or social issues discussed earlier (Van Brakel, 2021a).

New types of oversight bodies could be inspired by adding a relational ethics perspective to the current rational perspective. Governance structures must also involve citizens, and they should specifically engage with targeted and vulnerable communities when making policy decisions about implementing AI.[82] An example of a step in the right direction is the establishment of the Ethics Committee by the Westmidlands Police.[83] The committee evaluates pilot projects and implementation of new technologies by the police. What is positive about the committee is that it works in a transparent way publishing the reports fully on the website of the committee and the members of the committee are diverse. Members include representatives from the police, civil society, and community and academic experts in law, criminology, social science, and data science. However, to be successful and sustainable, such initiatives should also ensure that people are sufficiently compensated for their time and work, and this they not merely rely on volunteers and goodwill of the members.[84]

[76] Babuta and Oswald, 2019, see note 3.
[77] Van Brakel, 2021b, see note 17.
[78] Ibid
[79] Ibid.; Ralph B. Taylor and Jerry H. Ratcliffe, Was the pope to blame? Statistical powerlessness and the predictive policing of micro-scale randomized control trials (2020) *Criminology & Public Policy*, 19(3): 965–996; Robin Khalfa and Wim Hardyns, De evaluatie van big data policing: krijtlijnen voor het opzetten van een geschikt experimenteel evaluatiemodel (2023) *Cahiers Politiestudies Big Data*, 66: 179–208.
[80] Van Brakel, 2021b, see note 17; Hielke Heijmans and Rosamunde van Brakel, 2023. Article 44 in Eleni Kosta and Franziska Boehm (2023) *The Law Enforcement Directive. A Commentary*. Oxford University Press.
[81] Van Brakel, 2021a, see note 7; 2022; Elizabeth Aston (2023) *Independent Advisory Group on Emerging Technologies in Policing Final Report*. Scottish Government.
[82] Abeba Birhane, "Algorithmic injustice: a relational ethics approach" (2021) *Patterns*, 2(2): 1–9; Rosamunde Van Brakel, De controle op het gebruik van algoritmische surveillance onder druk? Een exploratie door de lens van de relationele ethiek (2022) *Tijdschrift voor Mensenrechten*, 1: 23–28.
[83] West-Midlands Police Ethics Committee, www.westmidlands-pcc.gov.uk/ethics-committee.
[84] Van Brakel, 2021b, see note 17.

18.3.2.4 Organizational Issues

The implementation of AI in policing by law enforcement also raises several organizational issues. The LED foresees a right to obtain human intervention when an impactful decision is taken solely by automated means.[85] This has been referred to as a "human in the loop,"[86] which is a safeguard to protect the data subject *against* "*a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces harm.*"[87] However, in practice, this legal provision raises several challenges.

First, the directive does not specify what this "human in the loop" should look like or in what way the human should engage with the loop (on the loop, in the loop, or outside of the loop).[88] According to advice of the Article 29 Working Party, it is necessary to make sure that "*the human intervention must be carried out by someone who has the appropriate authority and capability to change the decision and who will review all the relevant data including the additional elements provided by the data subject.*"[89]

According to Methani et al., meaningful human control refers to control frameworks in which humans, not machines, remain in control of critical decisions.[90] This means that, when it comes to AI, the notion of human oversight should extend beyond mere technical human control over a deployed system: It also includes the responsibility that lays in the development and deployment process, which entirely consists of human decisions and is therefore part of human control. The concept of meaningful human control should, in addition to mere oversight, also include design and governance layers into what it means to have effective control. However, these aspects are currently insufficiently taken into consideration, and guidance on how law enforcement must deal with this is lacking. Questions remain, therefore, how law enforcement officers need to be in the loop to make sure this safeguard is effective.

Second, not everybody is enthusiastic about new technologies. Resistance against surveillance is hence important to consider when implementing AI in law enforcement and evaluating its effectiveness. Research by Sandhu and Fussey on predictive

[85] Article 11 LED.
[86] Article 11 LED.
[87] Recital 38 LED.
[88] "Human on the loop" means that the human is part of every decision in the cycle of the system, "human in the loop" means that the human is a supervisor that controls the decisions and might intervene, and "human outside of the loop" means that the human is pushed entirely out of the control loop, allowing the system to independently execute its task. See for a more elaborate discussion, Leila Methnani, L., Andrea Aler Tubella, Virginia Dignum and Andreas Theodorou, Let Me Take Over: Variable Autonomy for Meaningful Human Control (2021) *Frontiers in Artificial Intelligence*, www.frontiersin.org/articles/10.3389/frai.2021.737072/full.
[89] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (October 3, 2017): 10.
[90] Methnani, Tubella, Dignum and Theodorou, 2021, note 79.

policing has shown that many police officers have a skeptical attitude toward and reluctance to use predictive technologies.[91] A third implementation issue concerns automation bias, whereby a person will favor automatically generated decisions over a manually generated decision.[92] This is what Fussey et al. have called deference to the algorithm, when evaluating Live Facial Recognition Technology piloted by the London Metropolitan Police.[93] It also involves potential de-skilling, which implies that by relying on automated processes, people loose certain types of skills and/or expertise.[94] Of course, not everyone will respond to the use of such systems in the same way. However, this risk is something that needs to be taken seriously by both law enforcement agencies and by policymakers. At the same time, Terpstra et al. have suggested that as policing is becoming more dependent on abstract police information systems, professional knowledge, and discretion are becoming devalued, which may have negative impacts on officers' sense of organizational justice and self-legitimacy.[95]

18.4 CONCLUSION

In this chapter, I discussed predictive policing in Europe and its main legal, ethical, and social issues. Law enforcement will become increasingly dependent on AI in the coming years, especially if it is considered to be superior to traditional policing methods, and cheaper than hiring more officers. Current models of regulating, organizing, and explaining policing are based on models of human decision-making. However, as more policing will be performed by machines, we will urgently need changes to those assumptions and rules.[96] Hence, the challenge lies not only in rethinking regulation but also in rethinking policy and soft law, and exploring what role other modalities can play. Consideration must be given to how the technology is designed, how its users and those affected by it can be made more aware of its impact and be involved in its design, and how the political economy affects this impact. Current policy tools and judicial oversight mechanisms are not sufficient to address the broad range of concerns that were identified in this chapter. Because the harm that AI can cause can be individual, collective, and social, and

[91] Ajay Sandhu and Peter Fussey, The "uberization of policing"? How police negotiate and operationalise predictive policing technology (2020) *Policing & Society*, 31(1): 66–81.

[92] Linda J Skitka, Kathleen L. Mosier, and Mark Burdick, Does automation bias decision-making? (1999) *International Journal of Human-Computer Studies*, 51(5): 991–1006.

[93] Peter Fussey, Bethan Davies, and Martin Innes, Assisted facial recognition and the reinvention of suspicion and discretion in digital policing (2021) *The British Journal of Criminology*, 61(2): 325–344.

[94] Elizabeth Joh, The consequences of automating and deskilling the police (2019) *UCLA Law Review*, 67: 133–164.

[95] Jan Terpstra, Nicholas R. Fyfe, and Renze Salet, The Abstract Police: a conceptual exploration of unintended changes of police organisations (2019) *The Police Journal: Theory, Practice and Principles*, 92(4): 339–359.

[96] Joh, 2019.

often stems from an interaction of an existing practice with technology, an individualistic approach with a narrow technological focus, is not adequate.[97]

While some of the earlier mentioned issues and challenges are dealt with by the upcoming AI regulation, as shown, it remains to be seen to which extent these safeguards will be taken up and be duly applicable in the context of law enforcement. Like the way regulation of data processing by law enforcement is always striving to find a balance between law enforcement goals and fundamental rights, the proposed AI regulation aims to find a balance between on the one hand corporate and law enforcement needs and on the other protecting fundamental rights. However, to address the social and ethical issues of AI, it is necessary to shift the focus in governance from the compulsion to show "balance" by always referring to AI's alleged potential for good by acknowledging that the social benefits are still speculative while the harms have been empirically demonstrated.[98]

Considering, on the one hand, the minimal evidence of the impact of predictive policing on crime reduction, and on the other hand, significant risks for social justice and human rights, should we not rethink the way AI is being used by law enforcement? Can it at all be used in a way that is legitimate, does not raise the identified social and ethical issues and is useful for police forces and society? Simultaneously, the question arises if the money that is invested in predictive policing applications should not be invested instead in tackling causes of crime and in problem-oriented responses, such as mentor programs, youth sports programs, and community policing, as they can be a more effective way to prevent crime.[99]

As Virginia Dignum nicely puts it: "AI is not a magic wand that gives their users omniscience or the ability to accomplish anything."[100] To implement AI for law enforcement purposes in a responsible and democratic way, it will hence be essential that law enforcement officials and officers take a more nuanced and critical view about using AI for their work.

[97] Van Brakel, 2021a, see note 7; Jonas Breuer, Rob Heyman, and Rosamunde Van Brakel, Vulnerable data protection as privilege – factors to increase meaning of GDPR in vulnerable groups (2022) *Frontiers in Sustainable Cities*, 4, www.frontiersin.org/articles/10.3389/frsc.2022.977623/full; Van Brakel and Govaerts, 2024, see note 25.

[98] Dan McQuillian, We come to bury ChatGPT not to praise it, www.danmcquillan.org/chatgpt.html.

[99] Van Brakel, 2016, see note 3; Litska Strikwerda, Predictive policing: the risks associated with risk assessment *The Police Journal: Theory* (2021) *Practice and Principles*, 94(3): 422–436. See also work on best practices by the International Center for the Prevention of Crime and the Policing Project, www.unodc.org/unodc/en/commissions/CCPCJ/PNI/institutes-ICPC.html.

[100] Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way* (Dordrecht: Springer, 2019).