

**EUCPN**  
EUROPEAN CRIME PREVENTION NETWORK

# Artificial intelligence and predictive policing: risks and challenges

---

Recommendation paper

# TABLE OF CONTENTS

PREFACE	3
INTRODUCTION	4
1. HOW DOES PREDICTIVE POLICING WORK?	5
2. THE RELEVANT LEGAL FRAMEWORK	7
3. PREDICTIVE POLICING IN THE EUROPEAN UNION	8
4. IMPORTANT CONSIDERATIONS TO KEEP IN MIND	10
RECOMMENDATIONS	14
GLOSSARY OF TERMS	17
ENDNOTES	18



We should aim for a more nuanced perspective. AI should not be viewed as a 'panacea' in crime prevention, yet at the same time, its potential benefits should not be ignored either. A productive use of AI in predictive policing with beneficial outcomes is dependent on a human rights compliant use of AI which keeps in mind the critical areas broken down above: transparency, accountability and bias.



# PREFACE

---

Artificial Intelligence makes it possible to create autonomous systems that can execute highly complex tasks, such as processing enormous amounts of information, forecasting future events, and learning to adapt through experience. This opens up possibilities for predictive policing: AI applications can handle large amounts of complex data (crime data, video streams from security cameras, ...) and predict when or where crimes will take place. But there are risks to it as well: such systems must respect the freedom and integrity of citizens, the protected nature of personal data, and must not reproduce or introduce illegal profiling or inequities. This paper explains the technology behind predictive policing computer programmes and provides an overview of the opportunities and risks of AI applications for the purpose of predictive policing.

## Citation

EUCPN (2022). Artificial intelligence and predictive policing: risks and challenges. Brussels: EUCPN.

## Legal notice

The contents of this publication do not necessarily reflect the official opinion of any EU Member State or any agency or institution of the European Union or European Communities.

## Author

Majsa Storbeck, Intern, EUCPN Secretariat



Part of the project 'EUCPN Secretariat', June 2022, Brussels  
With financial support from the European Union's Internal  
Security Fund - Police

# INTRODUCTION

---

Artificial Intelligence (AI) is hot. For the first time in human history, it is possible to create autonomous systems that approach or exceed human cognitive capacity. AI systems can execute highly complex tasks, such as processing enormous amounts of information, forecasting future events, and learning to adapt through experience.<sup>1</sup> This has created new possibilities in many domains, including health care, education, cybersecurity and environmental protection. Law enforcement agencies have shown an increased interest in AI. In all corners of the EU, police departments have put faith in AI tools in hopes of rendering law enforcement more effective and cost-efficient.<sup>2</sup> In particular, 'Predictive Policing' is proclaimed as the future of policing, in response to reduced budgets and staffing.<sup>3</sup> Using AI, the main purpose of predictive policing is to generate crime predictions and ultimately make a significant contribution to crime prevention.<sup>4</sup> Yet, in spite of its potential in crime prevention, policymakers and human rights groups around the globe have expressed concern regarding the use of predictive policing, as inappropriate use leads to an erosion of fundamental human rights.<sup>5</sup>

# I. HOW DOES PREDICTIVE POLICING WORK?

The use of statistics in law enforcement is nothing new. In the 1990s, emphasis was placed on intelligence-led policing. Now, new opportunities presented by Big Data are changing the nature of policing.<sup>6</sup> Big Data refers to vast amounts of data that can be analysed and reveal unexpected connections and/or correlations.<sup>7</sup> Yet, what Big Data knows is only one side of the coin. The other side entails the technology used to manipulate and organise that data, that is, algorithms. Algorithms are essentially mathematical processes which make educated guesses regarding the meaning of correlations in the data. Whereas some of these algorithms are relatively simple, others are built using machine-learning models.

Machine-learning (ML) algorithms differ from 'simple' algorithms in that they learn and adapt by experience. This occurs in different ways: in supervised learning, the ML algorithm uses training data that is correctly pre-labelled by developers. In unsupervised learning, the ML algorithm independently identifies patterns and correlations in 'raw' data.<sup>8</sup> An easy example of a ML algorithm is a music streaming service. To decide whether to recommend a particular song to a listener, the ML algorithm associates the listener's preferences with other listeners who have a similar taste in music. Thus, the ML algorithm not only looks for patterns, it also learns from that data, making the algorithm progressively better over time.

Certain branches of machine learning, such as deep learning, are inspired by human brain. Deep learning models, put simply, can make informed decisions without being given the rules (an algorithm) of performing that task. They power the most complex and capable AI systems, such as self-driving cars, drones, and other robotics. AI models used in predictive policing are most often rule-based machine learning models and rarely deep learning models.

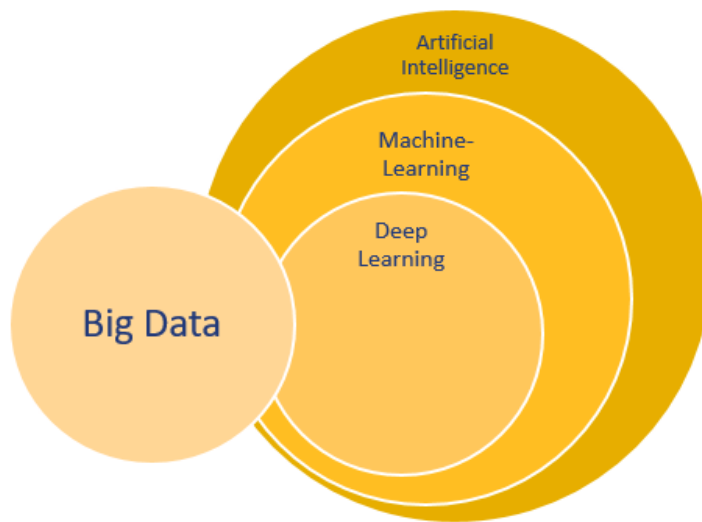


Figure 1. Breaking down AI.

In the context of law enforcement, this practically means that predictive policing can be divided in two consecutive steps: (1) data collection and (2) data modelling. First, with database storage ever increasing, enormous amounts of (un)structured data from different sources is collected.<sup>9</sup> Typically, this includes historical crime data (time, place and type), sometimes supplemented with socio-economic data and opportunity variables (e.g. close access to a highway).<sup>10</sup> Romania, for instance, uses data from probation and social services in addition to police data.<sup>11</sup> Second, the data is analysed using ML algorithms. This process consists of a training and a prediction phase, in which the model first searches for patterns in the available historical data (i.e. linking indicators to the risk of a crime) and subsequently publishes these probabilities as a risk score.<sup>12</sup> Three types of predictive policing can be distinguished, based on the type of predictions the underlying models are able to make: (1) area-based policing, i.e. predicting the time and place in which crimes are more likely to occur, (2) event-based policing, predicting the type of crime that is more likely to occur, and (3) person-based policing, predicting the individual who is most likely to conduct a criminal act.<sup>13</sup>

## 2. THE RELEVANT LEGAL FRAMEWORK

Within the EU, the protection of personal data is viewed as a fundamental right.<sup>14</sup> The General Data Protection Regulation (GDPR) regulates the collection, processing and usage of personal data in the European Economic Area. The Law Enforcement Directive 2016/680 (LED) acts as a special to the GDPR and applies to police and judicial cooperation in criminal matters (including crime prevention) and data processing. Importantly, Art. 27 requires the competent authorities (e.g., the police) to carry out a Data Protection Impact Assessment (DPIA) if the data processing may harm the rights of European citizens. A DPIA must contain a human rights assessment and a proposal on how to mitigate those risks.

In 2021, the EU proposed the Artificial Intelligence Act (AIA), which must become a key piece in the regulation of AI. Its aim is twofold: facilitating innovation by harmonising existing national laws regarding AI, while at the same time protecting fundamental rights in the digital realm.<sup>15</sup>

The AIA proposal has overall been welcomed by experts, as it is the world's first legal framework for the responsible development, deployment and use of AI. The proposal differentiates four risk levels regarding AI applications: (1) unacceptable risk, (2) high-risk, (3) limited risk and (4) minimal risk. Under Article 5, the proposal recommends the prohibition of unacceptable risks. This includes the practice of so-called 'social scoring' (e.g. on the basis of people's social behaviour and/or characteristics) by public authorities, and, with some exceptions, the use of 'real-time' remote biometric identification systems in public spaces (i.e. facial recognition). AIA establishes that AI systems used by law enforcement, including predictive policing models, are 'high-risk' and shall be subject to specific transparency and fundamental rights requirements related to data quality, technical documentation, transparency and information, human oversight, robustness, accuracy and cybersecurity. High-risk applications intended for the biometric identification of natural persons are subject to third party conformity assessment; for all other high-risk systems (including predictive policing) a self-assessment suffices.

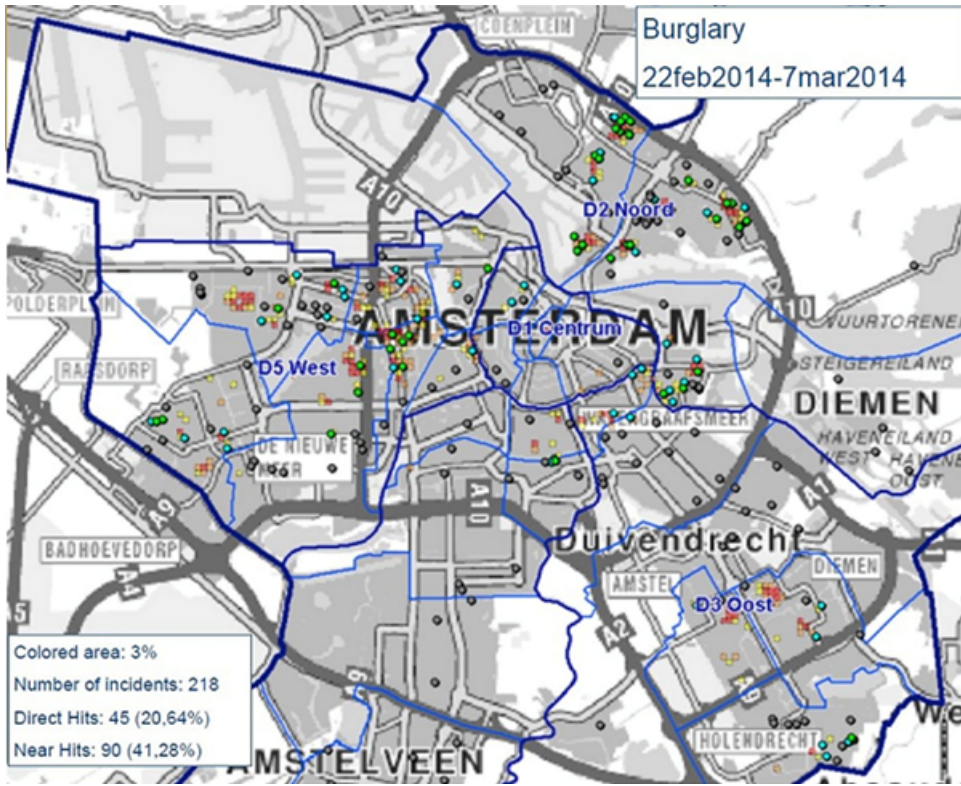
# 3. PREDICTIVE POLICING IN THE EUROPEAN UNION

Predictive policing is currently applied in a number of European police departments, including the Netherlands, Germany, Austria, France, Estonia and Romania. Other EU Member States, such as Luxembourg, Portugal and Spain are currently investigating the possibilities for the implementation of predictive policing.<sup>16</sup>

Currently, predictive policing is primarily used to prevent domestic burglary and car theft. In this field, the Netherlands is viewed as a pioneer as it is the first country in the world deploying predictive policing on a national scale.<sup>17</sup> Its Crime Anticipation System (CAS) initially targeted so-called 'high impact crimes', i.e. domestic burglaries, robberies, and mugging, but now covers also pickpocketing, car burglaries, violent crimes, commercial burglaries and bicycle theft.<sup>18</sup> It combines demographic and socioeconomic data from three sources: (1) the Central Crime Database, (2) the Municipal Administration, and (3) the Central Bureau of Statistics of the Netherlands. Data is displayed in the form of so-called 'heat maps', charting areas of increased crime risk which ultimately drive policing interventions.<sup>19</sup> Precobs in Germany mainly targets residential burglary by means of historical data, usually of the last five years.<sup>20</sup> Austria and France deploy predictive policing to detect residential and vehicle burglary.<sup>21</sup> Austria uses historical crime data (the offence type, time, location, modus operandi and place information). The output is demonstrated on a thematic dashboard showing offences, hotspots, statistics, reports and prevention measures. In France, the input comprises filed complaints, historical crime statistics and geolocations of burglaries and car theft of the last seven to ten years. Data may include meteorology and national statistics in the near future. The output is displayed on a map on which a blue to red gradient indicates where an offence is likely to occur.

Estonia stands out in that it deploys predictive policing to predict event-based, area-based and person-based crimes. Input includes previous crime data (type, time and place), data related to border crossing (place, time, migration status and related documentation) and unnatural deaths (drug related, traffic accidents and homicides). Romania uses predictive policing to predict area-based and person-based crimes.





# 4. IMPORTANT CONSIDERATIONS TO KEEP IN MIND

There are a few caveats when applying AI for the purpose of predictive policing, including problems with transparency and accountability, possible bias, especially automation bias, and positive 'feedback loops'. The following section introduces and discusses these challenges to provide clarity on the existing shortcomings.

- Transparency: the "black-box" problem

The way in which machine-learning models generate results can be opaque.<sup>22</sup> This stems from a number of factors, that often conflate. Algorithms are often very complex and thus difficult to grasp for end users. Additionally, self-learning models may take decisions on the basis of rules it has set for itself. Finally, a degree of opacity may be built in by developers as an intentional form of self-protection.<sup>23</sup> ML algorithms collect and process vast amounts of data and keep learning during the calculations. Steps made by the ML algorithm are too complex to retrace for humans, even for those who designed the algorithm. In other words, it becomes impossible, both in theory and in practice, to unveil the reasons behind a specific result or decision. ML algorithms are therefore often depicted as "black boxes".

## What is the "black box"?

The "black box" metaphor has been evoked by academics in discussing AI. Due to its high complexity and extensive data input, we often cannot understand, even in hindsight, why an algorithm has made a certain decision. The "black-box" phenomenon in this context symbolises a system in which we can only observe its input and output, with the decision-making itself remaining secret.

Another factor that negatively affects transparency is the fact that developers may keep the initial data input and algorithms hidden from users, for reasons of self-protection or in pursuit of a competitive advantage: secrecy, the argument goes, can get you ahead of your commercial opponents.<sup>24</sup> For instance, Predpol, the pioneer in predictive policing software from the US, makes use of secretive proprietary algorithms.<sup>25</sup> Limited transparency makes it exceedingly difficult, for policy-makers and citizens alike, to comprehend and appreciate AI-induced predictions.

- Accountability: the “Many hands” problem

The “black-box” problem feeds into the second issue relating AI, sometimes referred as the “many hands” problem, referring to a scenario in which a range of individuals and organisations are involved in the development and deployment of complex systems. As this is often the case with AI products in general and predictive policing in particular, it is often impossible to unambiguously identify who is to blame for the harms and fundamental rights violations resulting from the AI implementation in predictive policing.<sup>26</sup> A pertinent example is the risk assessment tool “COMPAS” used in the US court system, which the non-profit ProPublica has revealed to be not only ineffective in predicting criminal behaviour but also discriminatory against black defendants. ProPublica demonstrated that the application wrongly considered black defendants to be twice as likely to commit crimes than white defendants.<sup>27</sup> COMPAS disputed ProPublica’s interpretation of the results, leaving the issue unresolved to this day.<sup>28</sup>

- Bias

The third issue of AI is its potential for bias. We can generally identify two sources of bias when it comes to AI systems: (a) Algorithmic bias and (b) Big Data bias. The former refers to the bias of the algorithm developers, builders and engineers. Whether consciously or unconsciously, the (predominantly male and white) developers’ views and beliefs may ring through in the algorithm.<sup>29</sup> The latter refers to the bias in the data itself, which even in the age of Big Data may not be representative.<sup>30</sup> In the context of predictive policing, so-called “gender-neutral” risk assessments can overstate the recidivism risk of women because women tend to reoffend less often than men.<sup>31</sup> Datasets can also disproportionately target minority groups in this scenario. If minority neighbourhoods have been overpoliced in the past, more crime would have been found there than in other areas.<sup>32</sup>

What this means in practice is that skewed datasets combined with algorithms that propagate existing biases can yield false positives. Racial profiling—illegal in the EU—becomes entrenched in the predictive policing.<sup>33</sup>

Some researchers have, for instance, reported that PredPol was more likely to target low-income, black communities compared to affluent, white communities with similar rates of drug crimes in the United States.<sup>34</sup>

- Automation bias & positive 'feedback loops'

A side effect of AI is the phenomenon of automation bias, in which humans tend to rely uncritically on computer-generated solutions. This is largely because humans have a superior view of in automated systems.<sup>35</sup> Even when contradictory information is available, humans tend to defer to automated decisions either because they ignored or failed to verify that information.<sup>36</sup> The automation bias is even stronger in case of doubt.<sup>37</sup> It goes without saying that this might lead to false positives.

False positives are furthermore susceptible to "positive feedback loops" which can further exacerbate existing biases and exclusions. This occurs, for example, when the system is (unconsciously) trained to recognise people of a certain age, skin colour or from a certain neighbourhood as potential criminals. When this occurs, the system blindly labels this bias as the ground truth. Now, a positive feedback loop is established, whereby not only the personal biases of the operator are reinforced, but also those of the machine-learning system.<sup>38</sup> Similarly, it can indicate certain areas as crime-ridden, resulting in increased police visits and subsequent arrests. This, in turn, teaches the algorithms that these are areas the police should be concentrating on, regardless of the actual crime rate. Its effects are twofold. First, it pushes the police to focus on the wrong priorities, leading to significant security misses. Second, the algorithm learns that it is "correct" in associating race, ethnicity and/or socio-economic status with criminality, and will therefore rely more heavily on this association in subsequent predictions. This can ultimately lead to the wrongful stigmatisation and discrimination of individuals, environments, and community areas.

### **Positive feedback loops: an example**

An example of this limitation was Microsoft's very short-lived experience in creating "Tay", an artificial intelligence chatbot, designed to interact with humans. Users could follow and interact with the bot @TayandYou on Twitter and it would tweet back, learning as it went from other users' posts. As soon as people understood how Tay worked, they started tweeting the bot hateful content. Not long after, the bot started to repeat and produce racist, anti-Semitic, and sexist hate speech. In less than 24 hours after the launch, Microsoft shut Tay down and put out a statement that it was "deeply sorry" for the bot's racist and sexist tweets.<sup>39</sup>

# RECOMMENDATIONS

---

There are significant risks associated with the application of AI in predictive policing. Banning predictive policing would help little to solve these problems: prejudice and bias existed long before the emergence of AI and Big Data. We should aim for a more nuanced perspective. AI should not be viewed as a 'panacea' in crime prevention, yet at the same time, its potential benefits should not be ignored either. A productive use of AI in predictive policing with beneficial outcomes is dependent on a human rights compliant use of AI which keeps in mind the critical areas broken down above: transparency, accountability and bias.

## **1) Avoid the transparency problem**

To boost transparency, practitioners should assure that their algorithms are explainable as well as accessible. This starts with the citizens' right to know that they might be subjected to algorithms in their area. Citizens should have access to information about the data collection, data processing, the purpose of the data collection and processing, the developer and user of the algorithm. Publishing contact information should allow citizens to ask questions and receive more information. Promising practices in this regard have been put forth by The City of Helsinki, Finland, and the City of Amsterdam in the Netherlands, who have been the first cities in the world to launch open AI registries. These online registries offer an overview of existing artificial intelligence systems and the algorithms used by the municipal government. For example, the Amsterdam Algorithm Register contains information on applications ranging from automated parking control to illegal holiday housing. The registries' central aim, according to the two municipalities, is to "be open and transparent about the use of algorithms".<sup>40</sup> Besides outlining the data collection and processing, the registries specifically state how their algorithms avoid discrimination, the risks and safeguards, and how human supervision is implemented.

To further facilitate transparency, it is imperative to rely on in-house software developers rather than commercial companies in the development of predictive policing software. France and Estonia implemented promising practices in this regard, as they already deploy in-house software developers.<sup>41</sup> Hiring specialised personnel with a background in computer science may be costly and time consuming, but at the same time allows to keep control of the entire development process and the resulting algorithm, and thus avoid the black box problem. If the employment of commercial parties cannot be avoided, developers must be required to make the data and code available for critical scrutiny, if necessary through regulatory means.

## **2) Avoid the accountability problem**

To address the accountability problem, independent oversight bodies must be established. These bodies should be adequately funded and staffed. The United Kingdom has implemented a

promising practice in this respect, as their oversight bodies strengthened and increased trust in the police. The body's responsibility extends beyond the examination of algorithms to all aspects of data usage by the police, including the means of data collection, the purpose, the data processing and storage, and use of the results (including secondary use).<sup>42</sup> Most Member States already have oversight bodies in place; when necessary their mandates should be expanded to cover all forms of data collection and processing in the framework of predictive policing and they should be provided with the necessary tools, resources and expertise.

### **3) The results of AI are conjecture in the realm of probability**

To further ensure maximum accountability, full automation of predictive policing should effectively be ruled out. Humans must always be the ultimate decision-makers with respect to intervention. Algorithmic output should not be read as conclusive 'facts', but rather as constructed probabilities which can, and sometimes must, be overridden. It is important to consider that probabilities are just that: probabilities, not to be confused with certainties. AI is most definitely not a future-predicting oracle, and especially in light of false positives, critical reflection must be embraced and promoted. AI can discover correlations that are not apparent at first sight, which can support policing frameworks by presenting probabilities. Predictive policing must thus remain a complementary law enforcement tool in crime prevention strategies, and never replace long-term programmes that address the root causes of crime.

### **4) Measure effectiveness**

Another way to boost accountability is by investing in detailed comparative studies on the use and implementation of predictive policing. The effectiveness is one of the most understudied aspects of the application of predictive policing. Moreover, the lack of uniform criteria makes it difficult to translate evaluation results to different settings. Evaluation studies may include or exclude different variables, e.g. the type of predictive policing (area-based, event-based and person-based), the type of data used (e.g. with or without facial recognition), the objective of the application (i.e. risks assessment or risk reduction), and circumstantial conditions (e.g. trust in the police and business interests of developers). A programme can be highly accurate in risk assessment but perform poorly in overall risk reduction. There are thus many potential confounding factors that inhibit the establishment of clear cause-and-effect relationships. This makes it difficult to determine whether AI applications in predictive policing are ultimately effective and serve the purpose of rendering policing more efficient and legitimate, or fails to do so and instead contribute to disproportionate surveillance. Transparent evaluations and detailed comparative studies are needed to create an evidence base regarding the costs and benefits of

AI applications in predictive policing.

### **5) Addressing the problem of Big Data Bias**

It goes without saying that the quality of data determines the quality of the output. A data collection and quality strategy can mitigate many problems. Monitoring the data quality and collection is paramount to avoiding bias and discriminatory applications. In this respect, inspiration can be taken from Austria and Estonia, who assess their data quality on a regular basis.<sup>43</sup> Estonia, for instance, has dedicated a special analysis unit to monitor data collection and to make proposals for the improvements of the software and data quality. Police personnel and software operators who enter the data, manipulate it or interpret the results should be adequately trained, and such training should be institutionally embedded. The training should devote specific attention to the limitations of the algorithms, particularly the possibility of false positives and automation bias, as well as to the individual and institutional responsibilities in interpreting the results. A promising practice in this regard can be found in Austria, which offers crime analysis courses to police personnel. Finally, it is promising that, according to the EUCPN questionnaire, European law enforcement agencies are generally aware of the risks involved in predictive policing and the need to act responsibly.



# GLOSSARY OF TERMS

Algorithm -Sequence of formal rules (logical operations, instructions) applied to input data in order to solve a problem.

Artificial intelligence (AI) -A set scientific theories and techniques whose purpose is for a machine (a computer) to reproduce the cognitive abilities of a human being with the aim of supporting decision-making processes or making predictions.

Artificial Neural Network (deep learning) -Algorithmic system design based on neurons in the human brain. Neural nets are characterised by the presence of one or several hidden layers of interconnected nodes (neurons) between the input and the output, the output of each of which may serve as input for the others. This creates very smart but potentially opaque AI systems.

Big Data-The term "big data" refers to a large heterogeneous data set (open data, proprietary data, commercially purchased data), as well as the possibilities offered by AI to handle such datasets.

Machine Learning -Machine learning is a subfield of AI concerned with applications that become "smarter" more accurate as they are being used (hence "learning"). The applications will process the input in ways that are not explicitly programmed to produce the output.

Personal Data -Any information relating to an identified or identifiable natural person. In the EU, any data, even when encrypted, that could lead to the identification of a person is considered personal data and falls within the scope of the GDPR.

Personal Data Processing -Any operation or set of operations applied to personal data or sets of data, including collecting, recording, structuring, storing, modifying, retrieval, consulting and sharing personal data.

# ENDNOTES

1. Preamble of the Montréal Declaration for Responsible AI: <https://www.montrealdeclaration-responsibleai.com/>
2. S. Egbert and M. Leese, *Criminal Futures: Predictive Policing and Everyday Police Work*, London: Routledge, 2020, 242.
3. W.L. Perry, B. McInnis, C.C. Price et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Washington DC: RAND Corporation, 2013.
4. W. Hardyns and A. Rummens, Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges, *European Journal on Criminal Policy and Research* 24:3 (2018), 201-18, <https://dx.doi.org/10.1007/s10610-017-9361-2>.
5. C.-P. Yen and T.-W. Hung, Achieving Equity with Predictive Policing Algorithms: A Social Safety Net Perspective, *Science and Engineering Ethics* 27:3 (2021), art. no. 36, <https://dx.doi.org/10.1007/s11948-021-00312-x>.
6. T.-W. Hung and C.-P. Yen, On the Person-Based Predictive Policing of AI, *Ethics and Information Technology* 23:3 (2021), 165-76, <https://dx.doi.org/10.1007/s10676-020-09539-x>.
7. T.Z. Zarsky, Governmental Data Mining and Its Alternatives, *Dickinson Law Review* 116:2 (2011), 285-330.
8. Hayward & Maas (2021)
9. R. van Brakel, Pre-Emptive Big Data Surveillance and Its (Dis)Empowering Consequences: The Case of Predictive Policing, in: B. van der Sloot, D. Broeders, and E. Schrijvers (Eds.), *Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press, 2016, 117-41.
10. A.G. Furgeson, Policing Predictive Policing, *Washington University Law Review* 94:5 (2017), 1109-89, <https://journals.library.wustl.edu/lawreview/article/id/3851/>; A. Rummens and W. Hardyns, The Effect of Spatiotemporal Resolution on Predictive Policing Model Performance, *International Journal of Forecasting* 37:1 (2021), 125-33, <https://dx.doi.org/https://doi.org/10.1016/j.ijforecast.2020.03.006>.
11. EUCPN Questionnaire.
12. Hardyns and Rummens, Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges.
13. Yen and Hung, Achieving Equity with Predictive Policing Algorithms: A Social Safety Net Perspective.
14. European Union, Charter of Fundamental Rights, Brussels, 2012, [http://data.europa.eu/eli/treaty/char\\_2012/oj](http://data.europa.eu/eli/treaty/char_2012/oj).
15. On the proposed Artificial Intelligence Act, see the following website maintained by the Future of Life Institute; <https://artificialintelligenceact.eu/>
16. EUCPN Questionnaire.
17. L. Strikwerda, Predictive Policing: The Risks Associated with Risk Assessment, *The Police Journal* 94:3 (2020), 422-36, <https://dx.doi.org/10.1177/0032258X20947749>.
18. Hardyns and Rummens, Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges.
19. I. Mugari and E.E. Obioha, Predictive Policing and Crime Control in the United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing, *Social Sciences* 10:6 (2021), 234, <https://dx.doi.org/10.3390/socsci10060234>.
20. Ibid.
21. EUCPN Questionnaire.
22. D. Castelvecchi, Can We Open the Black Box of AI?, *Nature* 538:7623 (2016), 20-3, <https://dx.doi.org/10.1038/538020a>.
23. J. Burrell, How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms, *Big Data & Society* 3:1 (2016), 1-12, <https://dx.doi.org/10.1177/2053951715622512>.
24. Ibid.
25. K. Blair, P. Hansen, and L. Oehlberg, "Participatory Art for Public Exploration of Algorithmic Decision-Making" (paper presented at the Companion Publication of the 2021 ACM Designing Interactive Systems Conference, Virtual Event, USA2021), 23-6, <https://doi.org/10.1145/3468002.3468235>.
26. K. Yeung, A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework, Strasbourg: Council of Europe, <https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdb>.
27. S. Buranyi, Rise of the Racist Robots – How AI Is Learning All Our Worst Impulses, 8 Aug. 2017, <https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses> (Accessed 2 Aug. 2022).
28. R. Rieland, Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?, 5 Mar. 2018, <https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/> (Accessed 2 Aug. 2022).
29. S. Dillon and C. Collett, AI and Gender: Four Proposals for Future Research, 2019, <https://dx.doi.org/10.17863/CAM.41459>.
30. K. Crawford, K. Miltner, and M.L. Gray, Critiquing Big Data: Politics, Ethics, Epistemology, *International Journal of Communication* 8 (2014), 1663-72.
31. Dillon and Collett, AI and Gender: Four Proposals for Future Research.
32. A. Christin, Predictive Algorithms and Criminal Sentencing, in: D. Bessner and N. Guilhot (Eds.), *The Decisionist Imagination: Sovereignty, Social Science and Democracy in the 20th Century*, New York: Berghahn, 2018.
33. W.D. Heaven, Predictive Policing Algorithms Are Racist. They Need to Be Dismantled, 17 July 2020, <https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/> (Accessed 2 Aug. 2022).

34. K. Lum and W. Isaac, To Predict and Serve?, *Significance* 13:5 (2016), 14-9, <https://dx.doi.org/https://doi.org/10.1111/j.1740-9713.2016.00960.x>.
35. A. Završnik, Algorithmic Justice: Algorithms and Big Data in Criminal Justice Settings, *European Journal of Criminology* 18:5 (2019), 623-34, <https://dx.doi.org/10.1177/1477370819876762>.
36. L.J. Skitka, K. Mosier, and M.D. Burdick, Accountability and Automation Bias, *International Journal of Human-Computer Studies* 52:4 (2000), 701-17, <https://dx.doi.org/10.1006/ijhc.1999.0349>.
37. L.J. Skitka, K.L. Mosier, and M. Burdick, Does Automation Bias Decision-Making?, *International Journal of Human-Computer Studies* 51:5 (1999), 991-1006, <https://dx.doi.org/https://doi.org/10.1006/ijhc.1999.0252>.
38. S.D. Ramchurn, S. Stein, and N.R. Jennings, Trustworthy Human-Ai Partnerships, *iScience* 24:8 (2021), <https://dx.doi.org/10.1016/j.isci.2021.102891>.
39. A. Kraft, Microsoft Shuts Down Ai Chatbot after It Turned into a Nazi, 25 Mar. 2016, <https://www.cbsnews.com/news/microsoft-shuts-down-ai-chatbot-after-it-turned-into-racist-nazi/> (Accessed 2 Aug. 2022).
40. Helsinki and Amsterdam First Cities in the World to Launch Open Ai Register, 20 Sept. 2020, <https://news.cision.com/fi/city-of-helsinki/r/helsinki-and-amsterdam-first-cities-in-the-world-to-launch-open-ai-register.c3204076> (Accessed 2 Aug. 2022).
41. EUCPN Questionnaire.
42. K. Macnish, D. Wright, and T. Jiya, Predictive Policing in 2025: A Scenario, in: H. Jahankhani, B. Akhgar, P. Cochrane, and M. Dastbaz (Eds.), *Policing in the Era of Ai and Smart Societies*, Cham: Springer International Publishing, 2020, 199-215.
43. EUCPN Questionnaire. [1] For a more extensive glossary, see the Council of Europe Glossary on Artificial Intelligence: <https://www.coe.int/en/web/artificial-intelligence/glossary>

## Contact details

EUCPN Secretariat

Email: [eucpn@ibz.eu](mailto:eucpn@ibz.eu)

Website: [www.eucpn.org](http://www.eucpn.org)

[twitter.com/eucpn](https://twitter.com/eucpn)

[facebook.com/eucpn](https://facebook.com/eucpn)

[linkedin.com/company/eucpn](https://linkedin.com/company/eucpn)

