Technology and Regulation

Human rights requirements for person-based predictive policing

lessons from selected ECtHR case law and its limits

Zuzanna Warso*

predictive policing, necessity, proportionality, Rights, AI regulation

zuzawarso@gmail.com

The article addresses human rights requirements for person-based predictive policing. It looks into human rights standards, as elaborated in the selected European Court of Human Rights case law on creating police databases, watchlists and registries, and the police's use of new technologies. The article argues that in the case of new technologies deployed by law enforcement the availability of evidence on the effectiveness and accuracy of a given method should be essential to assess that an interference with a human right using this technology is 'necessary in a democratic society'. The article notes that the Court's unwillingness to assess the claims about the utility of technology critically might suggest that its evaluation of human rights compliance of person-based predictive policing and other experimental technologies would suffer from a severe blind spot.

1. Introduction

Through its research and innovation programs, the European Union is investing in the development of digital tools and methods that will support Law Enforcement Agencies (LEAs) to process vast amounts of heterogeneous data coming from diverse sources. Systems developed for LEAs combine different software components performing various functions, including but not limited to online web crawling, face detection and recognition, behaviour detection, social network analysis and predictive policing. These technologies promise to improve operational effectiveness and efficiency in fighting crime and terrorism. Such promises come, however, with severe risks to the rights and freedoms of individuals and society.

Predictive policing is defined as applying analytical techniques to enable the early identification of potential crime problems.[1] Predictive policing systems use data and algorithmic models to assess the risk that a crime will be committed.[2] They calculate risk scores that are assumed to reflect the likelihood that a person or group will be a victim or perpetrator of a crime (these are referred to as person-based predictive policing), that a specific location will be a future crime scene (place- or area-based predictive policing) or that a particular type of activity might occur (event-based predictive policing).[3] The insights gained from risk scores are used to make further estimations and predictions that may be turned into concrete actions or decisions by the criminal justice system.

This article addresses human rights requirements for person-based predictive policing. It defines 'person-based predictive policing' as attempts by law enforcement authorities to assess a person's risk of committing a crime or becoming a victim of one using algorithms. These attempts can be both for the preventive identification of individuals likely to offend or become a crime victim and for calculating the risk of reoffending. Examples of the first type of predictive policing include the creation by the Chicago Police Department of the list of people it considered most likely to be involved in gun violence,[4] the so-called Strategic Subject List. The algorithm used there remains confidential, however according to some of the available information it used a social network analysis method to calculate the result.[5] Each person's 'risk score' depended not only on their past behaviour (e.g., the number of arrests) but also on information on other people in their social network.[6] An example of a system used to calculate the risk of reoffending is the tool called Correctional Offender Management Profiling for Alternative Sanctions (COMPAS). COMPAS assesses a criminal defendant's likelihood of becoming a recidivist. Trade secrets cover the algorithms implemented in this case. Still, according to the available information, the data used in this case includes, for example, factors such as education level, whether a per-

1 Walter L. Perry and others, Predictive Policing: Forecasting Crime for Law Enforcement (RAND Corporation, 2013) https://www.rand.org/pubs/research_briefs/RB9735.html ((accessed 4 September 2021).

2 Amnesty International, Netherlands: We sense trouble: Automated discrimination and mass surveillance in predictive policing in the Netherlands (2020) https://www.amnesty.org/en/documents/eur35/2971/2020/en/ (accessed 4 September 2021).

3 Tzu-Wei Hung, Chung-Ping Yen, 'On the person-based predictive policing of AI' (2020) *Ethics and Information Technology*.

4 See e.g., https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list

5 David Robinson and Logan Koepke, Stuck in a Pattern: Early evidence on 'predictive policing' and civil rights https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf (2016) (accessed 14 May 2022).

6 The program has been overhauled in 2020. See: https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html (accessed 14 May 2022).)

* Zuzanna Warso is the Director of Research at the Open Future Foundation.

Received 29 Dec 2021, Accepted 7 June 2022, Published: 13 June 2022.

son has a job, or whether one of their parents was ever sent to jail.[7]

The focus on person-based predictive policing in this paper is motivated by the fact that, in this case, the interference with the rights of the person whose risk score is calculated is unrefutable (see the introduction to section 4). The other predictive policing tools (e.g., creating crime heat maps) can operate using only aggregated and non-personal, statistical data. The interference with rights of people affected by results produced by these tools is then less straightforward and might be more difficult to prove. An interference with a right is, however, necessary to proceed with further analysis of the three-step test, which is the core of this paper. Nevertheless, the focus on person-based predictive policing does not mean that the human rights requirements formulated throughout this paper are irrelevant to other instances of predictive policing.

The article proceeds as follows. Section 2 provides information on the distinct characteristics of person-based predictive policing that give rise to human rights concerns discussed in the further sections. Section 3 illustrates some of the risks associated with the development and use of predictive policing. These challenges provide context for the analysis of case law in sections 4 and 5.

Section 4 looks at selected European Court of Human Rights (ECtHR) case law to draw lessons on the conditions and justifiability of using predictive policing under the European Concvention on Human Rights (ECHR). The application of the three-step test in the ECtHR judgments – namely whether the interference with a right was 'prescribed by law', whether it 'pursued a legitimate aim' and whether the interference was 'necessary in a democratic society' is analysed. As there is no ECtHR case law specifically on predictive policing, drawing on jurisprudence from other contexts is needed. In this article, I chose to focus on a selection of case law that is concerned with the two issues discussed in section 2. I take a closer look at judgments related to the processing of personal data and the use of technology by law enforcement. More specifically, the article analyses cases on creating police databases, watchlists and registries. In these judgments, the ECtHR addressed collecting and retaining different types of personal data, including biographical data, photographs, and DNA samples. Other cases analysed in section 4 relate to the police's use of surveillance technologies, particularly GPS devices and bulk interception of communication. The article analyses the application of the three-step test in these judgments to establish criteria that should be considered when setting up or assessing the human rights compliance of a legal framework and procedural safeguards for person-based predictive policing.

Section 5 elaborates further on whether and under which conditions the use of person-based predictive policing technologies could be considered 'necessary in a democratic society'. It focuses on whether this criterion should cover the issues of the efficacy of new technologies deployed by law enforcement. The Article concludes with suggestions on how the EU's regulatory plans regarding AI may create the necessary environment for research in this domain and for producing data on the efficacy, or lack thereof, of predictive policing methods in section 6.

Although a detailed analysis of EU laws is not the focus of this article, it is essential to mention two pieces of EU secondary legislation that form the main building blocks of the emerging EU regulatory framework for the development and use of person-based predictive policing systems by the LEAs: the Law Enforcement Directive[8] and draft AI Regulation.[9] The Law Enforcement directive lays down rules on the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The relevance of this directive is significant, as the collection and further processing of data, including personal data, is the 'fuel' of predictive policing systems. In addition, at the time of writing this paper, the proposal for an EU Regulation on AI was published. The proposal presented by the EC lists in Annex III AI systems classified as high-risk, some of which fall under the definition of predictive policing quoted in previous paragraphs.[10]

Through the AI regulation, the EU will shape the legal landscape for predictive policing in Europe. Considering these developments, there is an urgent need for clarity about what human rights standards apply to these tools. As human rights standards set in the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention of Human Rights, ECHR) constitute general principles of the EU law,[11] this article looks into these standards, as elaborated in the European Court of Human Rights (ECtHR) case-law on the right to respect for private life, to address the issue of human rights conditions and requirements. This approach is rooted in the conviction that human rights standards constitute anchor points and a general legal environment that can promote and guarantee responsible advances in science and technology.[12] Therefore, the regulatory challenges posed by new technologies, including predictive policing systems, should be situated in the overarching principles that constitute the sphere of rights and freedoms.[13]

7 https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

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

9 Proposal for a Regulation of the European Parliament and of the Council Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Brussels 21.4.2021).

10 These would be: "AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences" (point 6a) as well as in point 6e: AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 (the Law Enforcement Directive) or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups. In the Draft report on the proposal for the AI regulation two European Parliament Committees (the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs) propose to add predictive policing to prohibited practices as it "violates the presumption of innocence as well as human dignity" (see Amendments 16, 76, 293, 294). The draft report is available at https://www.europarl.europa.eu/doceo/document/CJ40-PR-731563_EN.pdf)

11 Article 6 of the Treaty on the European Union.

12 Erica Palmerini and others, D6.2 Guidelines on Regulating Robotics (RoboLaw project, 2014) http://www.robolaw.eu/RoboLaw_files/documents/robolaw_d6.2_guidelinesregulatingrobotics_20140922.pdf (accessed 4 September 2021).

13 Ronald Leenes and others, 'Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues' (2017) 9 *Law, Innovation and Technology* 1; Theresa Murphy, Gearoid O Cuinn, 'Works in Progress: New Technologies and the European Court of Human Rights ' (2010) 10 *Human Rights Law Review* 601

2. Distinct features of person based predictive policing

For this article, it is worth to highlight two specific features of person-based predictive policing systems that give rise to human rights concerns. First are questions about the data - what types of personal data are collected and kept, how long is the data stored, how it is collected etc. The second category of questions relates to the reliability and validity of the science behind the system, since, as noted by Ferguson, '[b]eyond the fuel of data, the engine of predictive technologies lies in its methodology'.[14]

Processing data and using statistics, forecasting and risk assessment are not new in policing. As noted by Berk,[15] sophisticated research on crime trends began already in the nineteenth century. In the early twentieth century, the interest in trends was extended to include forecasts. Compared to these previous efforts, what is distinct about the attempts by law enforcement authorities to assess a person's risk of committing a crime or becoming a victim of one is the specific focus on an individual and the amount and scope of personal data that might 'fuel' the algorithms. The new predictive tools often bring together data from databases across the public sector previously kept in silos (e.g., data held by local authorities, data stored by social services etc.). Various other data sources, such as information available online, e.g., shared on social media websites, might be further integrated into one surveillance and risk assessment system.

The other feature concerns the science behind the technology that is used. Predictive policing models vary considerably – they might use simple algorithms[16] which are interpretable and easy to understand in terms of how a forecast is produced, or black-box machine learning[17] models which are too complicated for any human to comprehend[18]. In the case of the latter, as pointed out by Oswald and others, it is difficult to explain to non-computer scientists and non-statisticians how a machine learning forecasting model arrives at its outcomes, which increases the potential for misunderstanding and even intentional misrepresentation[19]. Depending on the level of technical sophistication, the corresponding ethical and human rights concerns and proper ways of addressing them might vary. In all cases, however, the prevalence of secrecy and lack of transparency around the models used for predictive policing impedes the review of deployed methodologies and assessments of the scientific validity of the technologies in question (e.g., the relevance of the criteria considered to produce a 'risk score').

3. Why is there a problem?

Before moving on to the case law analysis, it might be helpful to illustrate some of the significant concerns raised against the development and premature deployment of person-based predictive policing. There are numerous reasons why it is problematic. Scholars from various disciplines including mathematicians, computer scientists, political scientists, and lawyers, have discussed these concerns in literature at length.[20] This section is not meant to be exhaustive, but instead serves as a reminder of some of the basic challenges related to development and use of predictive policing.[21]

From the perspective of human rights, the most fundamental argument against the use of person-based predictive policing systems found in literature seems to be that subjecting someone to computer-made assessments and decision leads to their objectification. As such, it is an insult to and cannot be reconciled with the human rights requirement for protecting human dignity. The argument pertaining to human dignity was raised in a joint opinion of the European Data Protection Board and the European Data Protection Supervisor on the EU Regulation on AI proposal (the Opinion).[22] It has been pointed out there that it "affects human dignity to be determined or classified by a computer as to future behaviour independent of one's own free will". The Opinion notes that the AI predictive policing systems listed in the Annex III to the AI Regulation used according to their intended purpose will lead to "pivotal subjection of police and judicial decision-making, thereby objectifying the human being affected". The Opinion concludes that these AI systems should be prohibited.[23] In

14 Andrew Ferguson, 'Policing Predictive Policing' (2017) 94 *Washington University Law Review* 1109

15 Richard Berk, Forecasting Methods in Crime and Justice (2005) Annual Review of Law and Social Science 220

16 An algorithm is a computational process or set of rules that are performed to solve some problem. A computer is typically used to carry out complex algorithms, but a human could also follow an algorithmic process, such as by following a recipe or using a mathematical formula to solve an equation. David Leslie and others, Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe (Council of Europe, Alan Turing Institute 2021). https://www.turing.ac.uk/research/publications/ai-human-rights-democracy-and-rule-law-primer-prepared-council-europe (accessed 4 September 2021).

17 Machine learning is a type of computing used to find data patterns and predict an outcome for a particular instance. 'Learning' is a bit misleading, as the computer does not learn in the same way as humans do. Instead, the computer is able to find similarities and differences in the data through the repetitious tuning of its parameters (often called 'training'). When the input data changes, the outputs also change accordingly, meaning the computer learns to detect new patterns. This is accomplished by applying a mathematical formula to large amounts of input data to produce a corresponding outcome. Leslie and others (n 16).

18 For more on the challenges posed by black box machine learning models see: Cynthia Rudin, 'Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead' (2019) 1 *Nature Machine Learning* 206

19 Marion Oswald, Jamie Grace, Sheena Urwin, Geoffrey C. Barnes, 'Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality' (2018) *Information & Communications Technology* Law 223. That being said, it is important to acknowledge the significant growth of the Explainable Artificial Intelligence over the last years. For a review of these efforts see e.g. Giulia Vilone, Luca Longo, 'Explainable Artificial Intelligence: a Systematic Review', (2020), available at: https://arxiv.org/abs/2006.00093

20 See, e.g., Cathy O'Neil, *Weapons of Math Destruction: How big data increases inequality and threatens democracy* (St Ives, Allen Lane, 2016); Richardson, Rashida, 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* 192; Danielle Ensign, Sorelle A. Friedler, Scott Neville, Carlos Scheidegger, Suresh Venkatasubramanian, 'Runaway Feedback Loops in Predictive Policing' (2018) *Proceedings of Machine Learning Research* 1; Dylan J. Fitzpatrick, Wilpen L. Gorr, Daniel B. Neil, 'Keeping Score: Predictive Analytics in Policing (2019) 2 *Annual Review of Criminology* 1; Kristian Lum, William Issac, 'To predict and serve?' (2016) 13 Significance 14

21 Other issues not elaborated on here are the secrecy and lack of transparency around how the technologies work and are used, the problems with oversight when the methods are implemented, the absence of accountability, detecting and dealing with false positives and false negatives, and the impact of predictive technologies on how people think and understand the role of law enforcement.

22 European Data Protection Board, European Data Protection Supervisor, DPB-EDPS Joint Opinion 5/2021). on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2021).) https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021).-proposal_en (accessed 4 September 2021).

23 European Data Protection Board, European Data Protection Supervisor, DPB-EDPS Joint Opinion 5/2021). on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2021).) https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021).-proposal_en (accessed 4 September 2021).

the same vein, the draft report of the EP committees published in April 2022 asserts that predictive policing should be prohibited as it violates human dignity.[24]

The reference to 'free will' in the joint EDPS and EDPB Opinion is somewhat troubling, as the concept's meaning in the legal context is far from clear. Nevertheless, the mention of human dignity and free will highlights that person-based predictive policing systems entail evaluating people not based on their unique characteristics but on the attributes of the groups they are members of. Implementing such methods would neglect that person's decisions on what course of action to pursue in their life, and in consequence violate their human dignity. This line of reasoning may be, however, undermined by claiming that there is no automatism and the assessment carried out by the computer systems merely assists and offers insights in reaching a decision, rather than being its sole basis. Furthermore, while over-reliance on risk assessment in the operation of criminal law is a valid critique that applies to ex-ante prevention methods in general,[25] different forms of risk assessment in crime prevention are already present in the justice system and seem to be accepted as part of how the criminal law routinely operates.[26] Therefore the argument against person-based predictive policing pertaining to human dignity might need to be fleshed out otherwise it can be easily dismissed.

A reference to 'free will' might also suggest that the Opinion authors link the problem to the right not to be subject to a decision based solely on automated processing enshrined in Article 22 of the General Data Protection Regulation (GDPR) and Art. 11 of the LED. If this is the case, the permissibility of the discussed AI systems would depend on whether the persons 'determined or classified by a computer' gave their consent. However, the GDPR and LED provisions allow the EU or the Member States to authorise a decision based solely on automated processing, including profiling if the law provides appropriate safeguards. The subject's explicit consent is referenced in Art. 22 (2) (c) GDPR, but not in LED, which is justified bearing in mind the inherently unequal power relations in the law enforcement context.

3.1 Suspicion instead of trust and the chilling effect

One of the other critical concerns about predictive policing is that it may impact how suspicion and trust operate in society and affect the role of probable cause, reasonable doubt, and the presumption of innocence.[27] Predictive policing tools consider a wide range of information sources to identify unknown dangers or threats[28] and, as a result, may elevate many people, who would not usually be considered a threat or placed under police surveillance, into the realm of being suspicious. In such circumstances, 'suspicion does not precede data collection, surveillance is not initiated based on 'reasonable suspicion'. Rather, it is generated by analysis of the data itself'.[29]

Data collection based on a generalised suspicion might, in turn, have a 'chilling effect'. It has been shown that individuals refrain from engaging in certain forms of activity if that activity is observed, because of the perceived consequences.[30] Individuals may refrain from lawfully exercising their democratic rights, such as freedom of expression (Art. 10 ECHR) and the right to freedom of assembly and association (Art. 11 ECHR), due to a fear of the consequences that may follow. Existing research indicates that those most vulnerable to a chilling effect are opposition movements, minority groups and those with the fewest resources to challenge the status quo.[31]

3.2 The bias of data and risk of discrimination

Another strand of critique of predictive policing is related to bias of input data and the consequences this might have.[32] Mathematical models or algorithms should quantify relevant traits to produce reliable results, but in the case of predictive policing the systems may have harmful outcomes and reinforce inequality. First of all, statistical inferences require the data from which the model learns to be representative of the data on which it is applied.[33] However, police databases are not a complete record of all crimes, and neither do they constitute a representative sample.[34] For example, data sets may omit information about certain types of crime (e.g., white-collar crimes and cases of domestic violence are under-investigated).[35] While some efforts offer insight into how much crime remains unrecorded, the representativeness of data in police databases is difficult to estimate as there exists no 'ground truth' data set containing a representative sample of crimes for comparison.[36] Moreover, predictive policing systems rely heavily on historical data held by police, which can reflect discriminatory practices of over-policing specific communities or groups. As systems are built on data produced during 'documented periods of flawed, racially biased, and sometimes unlawful practices and policies'[37], machine learning and AI might 'hardwire' a system based upon historical data that often is emblematic of reflect racial, ethnic or class prejudice. Reliance on imperfect data leads to vicious cycles that perpetuate discriminatory practices.

3.3 Automation bias

Predictive policing tools are often presented as merely decision support systems that inform human decision making and assist human decision-makers rather than replace them. However, people tend to follow automated directives or recommendations, and automation bias is a recognised problem - it occurs in decision-making because humans tend to "disregard or not search for contradictory information in light of a computer-generated solution that is accepted as

24 See justification to Amendment 16 https://www.europarl.europa.eu/doceo/document/CJ40-PR-731563_EN.pdf
25 For a discussion on the use of prevention measures to control crime see for example: Andrew Ashworth, Lucia Zedner, Patrick Tomlin, *Prevention and the Limits of Criminal Law* (Oxford University Press, 2013).
26 See: Frederick Schauer, 'The Ubiquity of Prevention' in Andrew Ashworth, Lucia Zedner, Patrick Tomlin, *Prevention and the Limits of Criminal Law* (Oxford University Press, 2013).
27 For a discussion on the reconfiguration of suspicion in the case of mass surveillance see: Pete Fussey, Daragh Murray, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' (2019) 52 *Israel Law Review* 31
28 Council of Europe, Mass Surveillance (2017) https://rm.coe.int/fact-sheet-on-mass-surveillance-final-rev1august2017/1680735d82 (accessed 4 September 2021).
29 Fussey and others (n 27).
30 Daniel J. Solove, 'A Taxonomy of Privacy' (2016) 154 *University of Pennsylvania Law Review* 477
31 Fussey and others (n 27).
32 Bias in machine learning can take different forms. In this subsection, 'bias of input data' refers to the fact that data used to construct and train predictive policing models does not reflect the 'ground truth' and might encompass social prejudice against certain groups. For a discussion of bias and fairness in AI in general see for example: Eirini Ntoutsi, Pavlos Fafalios and others, 'Bias in data-driven artificial intelligence systems—An introductory survey' (2020), 10 *WIREs*, available at https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1356 (accessed 16 May 2022).
33 https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1356
34 Lum & Issac (n 20).
35 Richardson and others (n 20).
36 Lum & Issac (n 20).
37 Richardson and others (n 20).

correct (...)".[38] The critical assessment of the tools may be hampered when police officers lack the confidence and knowledge to question or override an algorithmic recommendation. In addition, the proliferation of algorithmic decision-making might undermine professionals' skill and decision-making activities, placing over-reliance on information provided by technology (the 'autopilot problem'), which leads to an accountability problem. As pointed out by Tudor, "[u]sing a computer to allocate police attention shifts accountability from department decision-makers to black-box machinery that purports to be scientific, evidence-based and race-neutral".[39]

4. Interference with human rights

As already pointed out, the use of person-based predictive policing tools entails collecting and storing personal data. These activities interfere with Art. 8 of the ECHR that secures the right to respect for private and family life.[40] It is well-established in the ECtHR case law[41] that the protection of personal data is of fundamental importance to a person's enjoyment of their right as guaranteed by Article 8 of the Convention. The Court has ruled on several occasions that the mere storing of personal data by a public authority amounts to an interference with the right to respect for private life as secured by Article 8 par. 1 of the Convention.[42] In Amann v. Switzerland,[43] the Court reiterated that the subsequent use of the stored information had no bearing on the finding that the holding of personal data interfered with Art. 8. It was irrelevant whether the information gathered was sensitive or not or whether the person concerned had been inconvenienced in any way. Even public information can fall within the scope of private life, where it is systematically collected and stored in files held by the authorities.[44] This is all the truer where the information concerns a person's distant past.[45] To evaluate if interference was legitimate, the three-part test is applied. It must be assessed whether the interference is lawful, pursues a legitimate aim and is necessary in a democratic society to achieve that aim. These three criteria will be examined in turn.

4.1 'In accordance with the law'

No interference with a human right can be considered lawful if it does not have a legal basis in domestic law. However, the mere existence of a legal basis is not enough. The notion of 'in accordance with the law' also refers to the quality of the law. More specifically, the law should be (1) accessible to the person concerned and (2) foreseeable as to its effects.[46]

Under Article 8 of the Convention, data protection issues may arise at different stages of handling personal data, including during its collection, storage, use, and communication. The requirement of clear and detailed rules applies to all these stages. In general, the law must be formulated with sufficient precision to enable individuals to regulate and foresee the consequences of their conduct.

For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.[47] That being said:

> The level of precision required of domestic legislation – which cannot, in any case, provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed[48].

Against this background and requirements for the clarity of a legal basis, questions arise on how clear and detailed the law on the use of predictive policing must be. Can the use of predictive policing systems be based on general police powers to detect and prevent crime? Does the law have to provide a legal basis for the deployment of specific technologies? Should the law specify which factors and features could be considered in assessing the risk of criminality posed by an individual? Right now, these questions remain essentially open given the ECtHR case law. Still, some critical guidance on the required level of precision of the legal basis is offered by judgments that concerned the storage of personal data by the law enforcement agencies, the use of technological devices by the police and secret surveillance.

The Court examined the quality of the law on the storage of personal data in *Segerstedt-Wiberg and Others v. Sweden*.[49] The case concerned the storage of personal information in security police records and refusal to impart the full extent of personal information kept in these records. The applicants claimed that the national provisions that allowed for data storage on the grounds of 'special reasons' were not formulated with sufficient precision and were excessively broad. The government disagreed with this assessment but confirmed that a person might be registered in the police database without his or her being incriminated in any way. The Court noted that the security police enjoyed a certain level of discretion in assessing who and what information should be registered. However, the discretion was not unrestricted. The Court listed provisions that set limitations on the police power to record and store data. These included a general prohibition of registration based merely on the person's race or ethnic origin, political opinions, religious or philosophical conviction, membership of a trade union, health or sexual orientation. The Court referred to the provisions that set the purposes of keeping a register and the types of information stored. The relevant domestic law set up procedures to correct and destroy registered data, deal with individual complaints, and remove registered information. As a result, the Court

38 Mary Cumming, Automation Bias in Intelligent Time Critical Decision Support Systems (AIAA 1st Intelligent Systems Technical Conference, Chicago, 2004, 2012), https://doi.org/10.2514/6.2004-6313 (accessed 4 September 2021).

39 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020) www.europarl.europa.eu/doceo/document/LIBE-PR-652625_EN.pdf (accessed 4 September 2021).

40 Interference with a right is, however, not synonymous with a violation of a right. 'Interference' is used when a particular right is brought into play or 'engaged'. Fussey and others (n 27)

41 E.g. S and Marper v UK App nos 30562/04 and 30566/04 (ECHR, 4 December 2008), Gardel v France App no 16438/05 (ECHR, 17 December 2009, final 17 March 2010)

42 E.g. Segerstedt-Wiberg and Others v Sweden App no. 62332/00 (ECHR, 6 June 2006, final 6 September 2006), S and Marper v UK App nos 30562/04 and 30566/04 (ECHR, 4 December 2008).

43 Amann v Switzerland App no 27798/95 (ECHR, 16 February 2000).

44 E.g. Rotaru v Romania App no 28341/95 (ECHR, 4 May 2000), Segerstedt-Wiberg and Others v Sweden App no. 62332/00 (ECHR, 6 June 2006, final 6 September 2006).

45 Rotaru v Romania App no 28341/95 (ECHR, 4 May 2000), Cemalettin Canlı v Turkey App no 22427/04 (ECHR, 18 November 2008, final 18/02/2009).

46 Bart van der Sloot, 'The quality of law: How the European Court of Human Rights gradually became a European Constitutional Court for privacy cases' (2020) 11 *Journal of Intellectual Property, Information Technology and E-Commerce Law: JIPITEC* 160

47 M.M. v UK App no 24029/07 (ECHR, 13 November 2012).

48 Peruzzo and Martens v. Germany App nos. 7841/09 and 57900/12 (ECHR, 4 June 2013).

49 Segerstedt-Wiberg and Others v. Sweden, App no. 62332/00 (ECHR, 6 June 2009, final 6 September 2009).

found that the interference with the respective applicants' private lives was 'in accordance with the law', within the meaning of Article 8, because the scope of the discretion conferred on the competent authorities and the manner of its exercise was indicated with sufficient clarity to give individual adequate protection against arbitrary interference.

Thirteen years after adjudicating *Segerstedt-Wiberg and Others*, the Court passed a judgment in *Catt*, which concerned creating an 'extremism database'. The data held included the applicant's name, address, date of birth and presence at demonstrations. Most of the records concerned protests organised by a violent protest group but others related to the applicant's attendance at political and trade union events. The Court noted that the data collection had been carried out based on general police powers. There had been significant ambiguity over the criteria used by the police to govern the collection of data in question. As a result, the exact scope and content of the data collected and compiled to form the database were difficult to determine. The Court also noted the loosely defined notion of 'domestic extremism' and that the government did not acknowledge the existence of the database until the domestic proceedings took place in this case. The Court was concerned that the collection of data for the database did not have a more precise and more coherent legal base. Nevertheless, it accepted that it was possible to deduce that the police were likely to be maintaining such a database from the 'information publicly available'.[50] As far as the retention of the data was concerned, the applicant's data could potentially be stored indefinitely if it was considered not excessive, necessary for a policing purpose, and was up to date. After the initial decision to retain, data was kept for a minimum of six years. After that point, it would be reviewed and could be deleted, but the police had a broad discretion to keep storing it. Despite these shortcomings and a lack of legal clarity, the Court decided not to examine the issue from the perspective of lawfulness, but rather assess if it was 'necessary in a democratic society'. The Court did not rule whether the legal basis met the 'quality of law' requirements within the meaning of Article 8 § 2 of the Convention and decided to examine the issues from the perspective of proportionality. Nevertheless, the criticism of vagueness of the legal basis undoubtedly points to the desire for more legal clarity when creating an 'extremist database'.

In MM, a case[51] that concerned the retention of caution on criminal record for life, the Court noted that the statutory regulations pertaining to the retention and of criminal records should be clear and detailed, and set out the rules governing, among other things, (1) the circumstances in which data can be collected, (2) the duration of their storage, (3) the use to which they can be put and (4) the circumstances in which they may be destroyed. The Court also criticised the absence of a mechanism for (5) independent review of a decision to retain or disclose data.

As far as the legal basis for using technological tools in the law enforcement context is concerned, in Khan v. the United Kingdom, the Court found a violation of Article 8 because there was no statutory system to regulate the use of covert listening devices and the guidelines applicable at the relevant time were neither legally binding nor directly publicly accessible[52]. The Court addressed a similar question in Uzun, a case that concerned the use of GPS by the police during an investigation.[53] In this case, the applicant argued that the provision of the Code of Criminal Procedure had not been a sufficient legal basis for the interference. He argued that the term 'other special technical means intended for the purpose of surveillance' contained in the relevant legal provision was not sufficiently clear. With regard to possible technical developments in the future, its content was not foreseeable for the persons possibly concerned. In response to this point, the Court noted that:

> [I]n any system of law, including criminal law, however clearly drafted a legal provision may be, there is an inevitable element of judicial interpretation. There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances.

At the same time, in the context of secret surveillance, the Court noted that '[i]n view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated'.[54] Similarly, in *Big Brother Watch*[55], a case on secret mass surveillance, the Court noted that:

> [E]specially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (...).

Some years earlier, in *Liberty and Others v. the United Kingdom*[56], a case that concerned the interception of external communication of civil liberties groups based on a warrant issued under broad discretionary powers, the Court noted that the law that did not specify the procedures for examining, using and storing the intercepted material failed to satisfy the criterion of 'sufficient clarity'.

It follows from the above that domestic law should provide a clear legal basis for predictive policing systems. The risks of arbitrary interference with the rights safeguarded by paragraph 1 of Article 8 are especially evident where the power of the executive is exercised in secret. It is justifiable to require the laws that mandate such tools and methods precision in language. Even though it may seem impractical (and considering the Courts assessment quoted above, even unnecessary), to expect the law to provide an exhaustive list of all technologies, the law must ensure foreseeability as to its effects to allow individuals to regulate their behaviour. What would that mean exactly in this case? Undoubtedly, to fulfil the foreseeability requirement and protect individuals against arbitrary interference with their rights under Article 8, the legal provision would have to refer explicitly to the purposes of predictive policing. That should be the case even if it would not list the specific technical means and in that way be open-ended as it was in the case of Uzun. In addition, the law should provide an adequate indication of the circumstances in which and the

50 Catt v UK App no 43514/15 (ECHR, 24 January 2019).
51 M.M. v UK App no 24029/07 (ECHR, 13 November 2012).
52 Khan v UK App no 35394/97 (ECHR, 12 May 2000, final 4 October 2000).
53 Uzun v Germany App no 35623/05 (ECHR, 2 September 2010, final 2 December 2010).
54 Uzun v Germany App no 35623/05 (ECHR, 2 September 2010, final 2 December 2010).
55 Big Brother Watch and Others v. UK App nos. 58170/13, 62322/14 and 24 960/15) (ECHR, 25 May 2021).
56 Liberty and Others v. the United Kingdom App no 58243/00 (ECHR, 1 July.2008, final 1 October 2008).

conditions on which public authorities are entitled to resort to the use of predictive policing systems that process personal data. The legislative framework applicable to the use of predictive policing tools should lay down at least the following conditions:

1. the specific circumstances in which law enforcement may deploy such technologies (including the types of offences which may justify the use of predictive policing tools),
2. the kind and types of information that may be collected and stored,
3. the procedures for accessing the data and using the results of the calculations,
4. the procedure to create a new 'risk score',
5. safeguards regarding supervision of the relevant services' activities, noting that the judiciary should typically carry out adequate supervision,
6. the duration of the storage of data,
7. the circumstances and the conditions in which data and records are deleted,
8. procedures for preserving the confidentiality, integrity and availability of data,
9. the persons authorised to consult the files or how this will be determined,
10. the precautions to be taken when sharing the data with other parties.
11. the right to request the disclosure and destruction of the data.

4.2 'Pursue a Legitimate Aim'

Interests that might justify an interference with the exercise of the right to respect for private and family life are listed in Article 8 par. 2 of the ECHR. These include, among others, national security, public safety, prevention of disorder or crime and the protection of the rights and freedoms of others. In none of the analysed cases, the Court disputed that collecting and processing applicants' data pursued a legitimate aim. The Court generally accepted that policing activities pursue the legitimate purpose of preventing disorder or crime, interpreted as a broad category encompassing a diverse range of activities.

In *Segerstedt-Wiberg and Others*, the Court accepted that the storage of the information in question pursued legitimate aims, namely the prevention of disorder or crime and the protection of national security. In *S and Marper*, the Court agreed with the government that the retention of fingerprint and DNA information pursued the legitimate purpose of the 'detection and, therefore, prevention of crime'. The Court did not distinguish between the prevention and the detection of crime or the investigation of future crimes. Instead, it extended the notion of 'preventing disorder and crime' from Art. 8 to cover these activities. In *S. and Marper*, the government presented statistical and other evidence to show that the retention of fingerprints, cellular samples and DNA profiles of unconvicted persons had been indispensable in the fight against crime. The applicants denied this claim. They asserted that the statistics were misleading and referred to the Nuffield Council on Bioethics' report. The report expressed concerns about the lack of satisfactory empirical evidence to justify the practice of retaining indefinitely fingerprints, samples, and DNA profiles from all those arrested for a recordable offence, irrespective of whether they were subsequently charged or convicted. Nonetheless, the Court did not look into the effectiveness of the measures and relied on the claim made by the State. Although ultimately the Court found a violation of Art. 8 because the interference was not 'necessary in a democratic society', the ECtHR generally accepted that the retention of data served a broader purpose of assisting in identifying future offenders of crimes that have not yet been committed. The Court later repeated the reasoning regarding the legitimate aim in other judgments[57].

Similarly, in *Catt*, there was no dispute about whether the creation and maintenance of the database by the police pursued a legitimate aim. The Court again accepted that the retention of the data pursued the legitimate aim of preventing disorder or crime and safeguarding the rights and freedoms of others. In *Big Brother Watch and Others*[58] the Court did not question that the bulk interception of communication pursued the legitimate aims of protecting national security, preventing disorder and crime, and protecting the rights and freedoms of others. Instead, the Court analysed if the interference was proportionate.

The analysis proves that the ECtHR tends to:

> [A]ccept very general and abstract aims, such as the protection of national security or respecting the rights and freedoms of others, as the basis for its examination of the justifiability of interferences with fundamental rights. As a result, there is hardly any opportunity for the Court to distinguish between various (more specific) aims.[59]

By accepting a tenuous link between the rights-restricting measures and a broad aim, the Court denied itself the opportunity to assess the measure's effectiveness. It does not seem that the Court would expect the State to provide any evidence or data on how exactly the action in question contributes to achieving the legitimate aim from Art. 8 par. 2. This is particularly troubling in the case of new policing technologies and methods, such as predictive policing tools, whose legitimacy should be drawn from proven effectiveness. The article will return to this point in section 5.

4.3 'Necessary in a democratic society'

The use of any measure that interferes with human rights cannot be justified unless the interference is 'necessary in a democratic society'. The ECtHR has developed a framework for assessing whether interference with an applicant's Article 8 rights was necessary and therefore justified. More specifically, an interference may be deemed necessary in a democratic society if it corresponds to a 'pressing social need', it is 'proportionate to the legitimate aim pursued',[60] and the reasons given by the national authorities to justify it are 'relevant and sufficient'.[61] The 'pressing social need' requirement concerns the weight and importance of the aims pursued.[62] The formula also seems to contain a requirement of effectiveness.[63]

A margin of appreciation is left to the national authorities in the assessment of the necessity.[64] In Article 8 cases, the Court has generally understood the margin of appreciation to mean that the Court should not substitute its own assessment of the merits, where

57 Gaughran v UK App no 45245/15 (ECHR, 13 February 2020, final 13 June 2020), MK v France App no 19522/09 (ECHR, 18 April 2013, final 18 July 2013).
58 Big Brother Watch and Others v. UK App nos. 58170/13, 62322/14 and 24 960/15) (ECHR, 25 May 2021).
59 Janneke Gerards, 'How to improve the necessity test of the European Court of Human Rights' (2013) 11 *International Journal of Constitutional Law* 466.
60 Dudgeon v UK App no 7525/76 (Report of the Commission, 13 March 1980).
61 Z v. Finland App no 22009/93 (ECHR, 25 February 1997)
62 Gerards (n 59).
63 Idem.
64 Janneke Gerards, Pluralism, Deference and the Margin of Appreciation Doctrine (2011), 17 *European Law Journal* 80

the independent and impartial domestic courts have examined the facts, applying the relevant human rights standards consistent with the Convention and its case-law, and adequately balanced the applicant's interests against the more general public interest in the case.[65] Nevertheless, the Court considered it necessary to assess the merits in some cases even if the above conditions were fulfilled. To justify this approach, the Court recently recalled the importance of "examining compliance with the principles of Article 8 where the powers vested in the state are obscure, creating a risk of arbitrariness especially where the technology available is continually becoming more sophisticated".[66] In *Gaughran*[67], the Court pointed out that the domestic courts made their assessment relating to the retention of the applicant's photograph on the basis that it was held on a local database and could not be searched against other pictures. Technological developments superseded this conclusion. It follows that the States may ultimately enjoy a narrower margin of appreciation if interference with a right is resulting from or is exacerbated by the use of new technologies.

4.3.1 Whose data may be stored?

The Court has generally accepted that, with proper safeguards, the State should have the power to retain personal data of persons convicted of offences.[68] The ECtHR did not call into question the preventive purpose of such registers. However, it did point out that the greater the scope of the recording system, the more important becomes the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data.[69]

In *Segerstedt-Wiberg and Others* the applicants were neither convicted nor suspected of a crime. The information regarding the first applicant was kept in the register of the secret police because she had received bomb threats several years earlier. In this case, the Court found that the reasons of preventing disorder or crime justified the storage of her data. What mattered for the Court was that the measure was at least in part intended to protect the applicant. The Court concluded that there was no question of any disproportionate interference with her right to respect for her private life. In the case of two other applicants, the information concerned their participation in a political meeting and a political demonstration in the sixties, respectively. Based on the nature and age of the data, the Court found that its persistent storage was not justified. In the case of two remaining applicants, the information stored by the secret police related to their membership in a political party that advocated the use of violence and breaches of the law to bring about a change in the existing social order. In support of this claim, the government submitted the party programme. What mattered most for the Court in assessing if the interference with the right to privacy was necessary was the fact that the government did not point to any specific circumstance indicating that the radical programme clauses were reflected in actions or statements by the party's leaders or members and constituted an actual or even potential threat to national security. Therefore, the reasons for the continued storage of the information about those applicants, although relevant, were not considered sufficient for the purposes of the necessity test.

In *S & Marper*, the applicants were suspected but not convicted of criminal offences. The Court noted that weighty reasons would have to be put forward by the government before the Court could regard a difference in treatment of the applicants' private data compared to that of other unconvicted people to be justified. The Court highlighted the risk of stigmatisation of persons who had not been convicted of any offence and were entitled to the presumption of innocence. The Court did not consider the retention of data to be proportionate concerning the purpose of collection. The Court acknowledged that the level of interference with the applicants' right to private life might be different for each of the three categories of personal data retained. In *S & Marper*, these remarks concerned the retention of DNA profiles, cellular samples and fingerprints, but similar considerations are relevant concerning other special categories of data. The Court noted the need to consider the age of the suspected offender and that retention could be especially harmful in the case of minors bearing in mind their unique situation and the importance of their development and integration in society. In *S & Marper*, the Court considered that:

> "The protection afforded by [the right to private life] would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. [...] The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard."

As far as a pressing social need is concerned, in *Catt*, the ECtHR distinguished between the need to collect the applicant's data and retain it. The Court did not dispute the conclusions of the domestic Court that the need existed in the case of data collection. In assessing whether the collection of personal data met a pressing social need, the Court considered it relevant that the applicant decided to align himself repeatedly and publicly with the activities of a violent protest group. The Court took a different stance regarding the retention of the applicant's data and considered that no pressing social need existed in this case. While it noted that there is a need for caution before overriding the judgment of the police about what information is likely to assist them in their task, it found that the absence of any rules setting an absolute maximum time limit on the retention of such data made the applicant entirely reliant on the diligent application of the highly flexible safeguards. The Court expressed concern about the unclear scope of data collection and the ambiguity of the State's powers in this domain. The Court moreover considered that the decision to retain the applicant's data failed to consider the heightened level of protection that should be afforded to data revealing a political opinion as its retention may have a 'chilling effect'. The Court highlighted that although the applicant could request the disclosure and destruction of the data, this safeguard had limited impact. The authorities refused to delete his data or explain its retention in the domestic extremism database, despite the conclusion by the police and domestic courts that the applicant was not considered a danger to anyone. The absence of adequate safeguards was of particular concern as the personal data retained by the police were the so-called sensitive data.

A couple of lessons relevant to assessing whether personal data storage for predictive policing might be necessary in a democratic society can be drawn from the above analysis. Some of these lessons overlap with requirements concerning the certainty and precision of

65 McDonald v UK App no 4241/12 (ECHR, 20 May 2014).
66 Catt v UK App no 43514/15 (ECHR, 24 January 2019).
67 Gaughran v UK App no 45245/15 (ECHR, 13 February 2020, final 13 June 2020).
68 E.g. Gardel v France App no 16438/05 (ECHR, 17 December 2009, final 17 March 2010),Peruzzo and Martens v. Germany App nos. 7841/09 and 57900/12 (ECHR, 4 June 2013), Gaughran v UK App no 45245/15 (ECHR, 13 February 2020, final 13 June 2020).
69 M.M. v UK App no 24029/07 (ECHR, 13 November 2012).

the legal framework. These include the requirement that a person must be able to request the disclosure and destruction of the data and the condition that data must be deleted if no longer relevant or sufficient for the initial purpose. These safeguards should be guaranteed by domestic law. Moreover, domestic law must afford adequate guarantees to ensure that retained personal data are efficiently protected from misuse and abuse. The need for proper safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned. Moreover, the law should set up rules on using the database and the range of public authorities with access to it. The right to consult the database should be restricted to authorities under a duty of confidentiality and precisely determined circumstances.

In addition, while it might be justified to collect data based on someone's alignment with groups that use violence, additional rules and effective procedural safeguards need to be put in place if the data is to be stored for more extended periods. A decision about retaining data should consider the character of the information, i.e., its sensitive nature and the chilling effect the storage might cause. Moreover, the storage of personal data in police database should not be deemed 'necessary in a democratic society' solely based on the objectives or intentions of a movement or a political party that a person belongs to if no actions or statements substantiate the assessment that a person poses a threat to national security, public order or rights and freedoms of other people. In such a case, the reasons for continued storage may not be considered sufficient for the necessity test under Art. 8 par. 2 of the Convention.

5. Additional remarks on the necessity

The analysis of the ECtHR case law in this article focused on the conditions and human rights requirements for the collection and storage of personal data in policing and the criminal justice system. The availability of data is a prerequisite for the development and deployment of predictive policing methods and tools. However, to determine if the use of this, or any other new technology, may indeed be considered proportionate to the aim pursued and that the reasons declared by the national authorities are relevant and sufficient, what is needed is data on the performance of the tools or methods in question. As pointed out:

> Effectiveness and accuracy are intrinsically linked to ethics and legality: if it cannot be demonstrated that a particular tool or method is operating effectively and with a reasonable degree of accuracy, it may not be possible to justify the use of such a tool as necessary to fulfil a particular policing function.[70]

It has been noted in the context of the bulk retention of communications data that the:

> [P]rofessed utility of bulk measures should be more clearly demonstrated, and their necessity or – strict necessity - more clearly addressed. Public disclosure of certain activities may legitimately be restricted based on national security considerations, but transparency should be the rule and secrecy the exception.[71]

The exact requirements apply to predictive policing measures.

So far, there has been little data available on the performance of predictive policing systems, in particular the person-based type.

According to Ferguson: 'the hype surrounding property- and place-based predictive policing has been used to justify adoption of violent crime-focused or person-focused technology, despite a lack of equivalent empirical testing to support it'.[72] There is limited empirical evidence that predictive policing can deliver on its multiple promises. As summarised by Sutherland and others, 'predictive judgments are meaningful when applied to groups of offenders. However, at an individual level, predictions are considered by many to be imprecise'.[73] A RUSI briefing paper summarises some of the available empirical evidence regarding the effectiveness and accuracy of predictive policing technology. In short: high accuracy rates at the group level can often conceal very low accuracy rates for specific individuals or groups of individuals within that larger group. All individual predictions are associated with a confidence interval (a margin of error), which is often not considered when reporting the overall 'predictive accuracy' of the tool.[74] This suggests that at this moment, the application of at least some of the person-based predictive policing tools in individual cases could not be considered effective and accurate, and therefore justified.

Algorithmic technologies in general and predictive policing methods in particular are in many ways experimental[75]. Oswald et all note that '[a]n issue for the courts in reviewing the use of a particular algorithm by the police is highly likely to be that some algorithmic tools are so new that the resource benefits have yet to be realised, and it may be too early to judge the benefits and harms with ease'.[76] Moreover, the tools used by law enforcement are often initially trained and evaluated on various datasets coming from different sources, which raises questions about their suitability for the high-stake domain such as policing. As pointed out, '[a] model is unlikely to perform well in the wild if its deployment context does not match its training or evaluation datasets, or if these datasets reflect unwanted biases'.[77] Due to its novelty and the lack of sufficient data on performance, the testing of predictive policing tools should be treated as experimental research. These technologies should not be used in operational circumstances unless and until their effectiveness and accuracy are proven.

The analysis carried out in section 4 shows that ECtHR falls short of considering the question of effectiveness and accuracy when it comes to new technologies. In the analysed cases, the Court did not consider whether implementing a given technology in police work delivers on its promise. For surveillance technologies, the Court accepted the claims made by the governments that their use will decrease the level of crime, despite the availability of evidence showing that this is not always the case. Similarly, the Court disregarded the lack of satisfactory empirical evidence to justify the practice of retaining indefinitely fingerprints and other personal data. The Court's unwillingness to critically assess the claims about the utility of technology when assessing if the reasons for interference with a right provided by the government are 'relevant and sufficient' might suggest that its evaluation of human rights compliance of person-based predictive policing and other nascent, experimental technologies would suffer from a severe blind spot.

70 Alexander Babuta, Marion Oswald, 'Data Analytics and Algorithmic Bias in Policing' (RUSI, 2019).
71 Fussey and others (n 27).
72 Ferguson (n 14).
73 Alan A. Sutherland and others, 'Sexual Violence Risk Assessment: An Investigation of the Interrater Reliability of Professional Judgments Made Using the Risk for Sexual Violence Protocol' (2012) 11 *International Journal of Forensic Mental Health* 119
74 Babuta & Oswald (n 70).
75 Oswald and others (n 19).
76 Idem.
77 Timnit Gebru and others, 'Datasheets for data sets' (2018) https://arxiv.org/abs/1803.09010 (accessed 4 September 2021).

6. Conclusions

Considering the risks to human rights resulting from person-based predictive policing tools and the uncertainty about their effectiveness and accuracy, States should be extremely cautious when allowing their use in operational conditions. The analysed ECtHR case law on the requirement for the impugned measure to be 'in accordance with the law' has general relevance. States should consider the requirements arising from these judgments when setting up the legal framework for person-based predictive policing. As far as the requirement that any interference must be in pursuit of a legitimate aim, the Court tends to accept broad aims and does not examine whether the measure indeed contributes to their achievement, which is unfortunate in the case of new experimental methods whose efficacy has not been proven. This aspect is directly linked to the third requirement from the three-part test, namely whether interference with a right is 'necessary in a democratic society'. More specifically, whether it is proportionate to the legitimate aim and the reasons given by the national authorities to justify it are 'relevant and sufficient'. This article has argued that to assess this aspect, the availability of evidence on the effectiveness and accuracy of a given tool or method is essential. The analysis carried out in previous sections has shown that the ECtHR has not sufficiently addressed the crucial question of the effectiveness of technologies deployed by law enforcement.

With this in mind, it seems crucial to underscore that not only the use but also the development and testing of predictive policing tools require proper regulatory environment and oversight. These are currently lacking. Some relevant provisions on the reuse of data for scientific research are provided in the GDPR and LED, however in practice, this issue lacks the legal certainty required to ensure that the rights of people whose personal data is processed are respected. The 2021 draft of the EU AI Regulation encourages the setting up of regulatory sandboxes to 'provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan' (Art. 53 point 1 of the initial draft). According to Art. 53 point 1 a (i) of the draft further processing of personal data could be performed in the regulatory sandbox if the AI system is developed for the purpose of the 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of the competent authorities'. These points would cover the AI systems used for predictive policing purposes. Art. 54 sets up conditions for the further processing of personal data that were collected for other purposes for the developing AI systems in the public interest. The conditions include the requirement for effective monitoring mechanisms to identify if any high risks to the fundamental rights of the data subjects may arise during the sandbox experimentation, a response mechanism to mitigate those risks promptly and, where necessary, stop the processing (art. 54 1 c), as well as that the processing of personal data in the context of the sandbox does not lead to measures or decisions affecting the data subjects (54 1 f). This proposal would address the current legal gap in the regulatory oversight over the development, testing, and validation of predictive policing technologies to some extent. Still, its relevance would be limited as not all predictive policing tools and methods use AI. Moreover, it remains to be seen how the proposal put forward by the EC will evolve during negotiations. Ultimately it will be up to Member States' competent authorities to establish the regulatory sandboxes and flesh out the conditions included in the EU legislation.

Acknowledgements

This work was supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833115 (PREVISION project). The author was affiliated with Trilateral Research when the research was carried out and the paper was submitted.