ACTA UNIVERSITATIS LODZIENSIS
FOLIA IURIDICA 97, 2021

https://doi.org/10.18778/0208-6069.97.13



*Donatas Murauskas*[*]
https://orcid.org/0000-0003-2092-2873

# PREDICTIVE ANALYTICS IN CRIME PREVENTION AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS: TACKLING RISKS IN PRIVACY AND FAIR TRIAL FRAMEWORKS

**Abstract.** In this paper I discuss whether the European Convention on Human Rights provides safeguards to individuals affected by predictive analytics in crime prevention. I start with depicting a conceptual issue that worries legal scholars – the trend of law-enforcement authorities to increase their attention to crime prevention rather than traditional criminal investigations. Then I dive into the right to privacy case-law of the European Court of Human Rights looking for the Court's references to the threats of data processing. Lastly, I select concrete cases of the European Court of Human Rights on the right to a fair trial to show that the human rights safeguards are not yet developed to frame predictive analytics in crime prevention.

**Keywords:** right to a fair trial, human rights, European Court of Human Rights, predictive analytics, case-law.

## ANALIZA PREDYKCYJNA W ZAPOBIEGANIU PRZESTĘPCZOŚCI I EUROPEJSKA KONWENCJA PRAW CZŁOWIEKA

**Streszczenie.** W tym artykule omawiam, czy Europejska Konwencja Praw Człowieka zapewnia ochronę osobom, których dotyczą analizy predykcyjne w zapobieganiu przestępczości. Zacznę od przedstawienia zagadnienia koncepcyjnego, które niepokoi prawników – tendencji organów ścigania do zwracania większej uwagi na zapobieganie przestępczości, a nie na tradycyjne dochodzenia. Następnie zagłębię się w prawo do orzecznictwa Europejskiego Trybunału Praw Człowieka w zakresie prywatności, szukając odniesień Trybunału do zagrożeń związanych z przetwarzaniem danych. Na koniec wybrałem konkretne sprawy Europejskiego Trybunału Praw Człowieka dotyczące prawa do rzetelnego procesu sądowego, aby wykazać, że zabezpieczenia praw człowieka nie zostały jeszcze opracowane; aby opracować ramy analiz predykcyjnych w zapobieganiu przestępczości. Stwierdzam, że orzecznictwo Europejskiego Trybunału nie gwarantuje wystarczającej ochrony praw człowieka, zwłaszcza gdy organy ścigania stosują analizy predykcyjne w zapobieganiu przestępczości.

**Słowa kluczowe:** prawo do rzetelnego procesu, prawa człowieka, Europejski Trybunał Praw Człowieka, analizy predykcyjne, orzecznictwo.

[*] Vilnius University Law Faculty; donatas.murauskas@tf.vu.lt

# DUOMENŲ ANALITIKA NUSIKALTIMŲ PREVENCIJOJE IR ŽMOGAUS TEISIŲ IR PAGRINDINIŲ LAISVIŲ APSAUGOS KONVENCIJA: TEISĖS Į PRIVATUMĄ IR TEISĖS Į TEISINGĄ BYLOS NAGRINĖJIMĄ TAIKYMO RIBOS

**Santrauka.** Straipsnyje keliu klausimą dėl Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos potencialo apsaugoti asmenis nuo žmogaus teisių ribojimų, teisėsaugos institucijoms naudojant algoritmus nusikaltimų prevencijos tikslais. Pirmiausiai pristatau teisėtyroje diskutuojamą konceptualią problemą – tendenciją teisėsaugos institucijoms vis daugiau dėmesio skiriant nusikaltimų prevencijai, o ne nusikalstamų veikų tyrimui. Toliau pristatau Europos Žmogaus Teisių Teismo praktiką privataus gyvenimo gerbimo srityje, ieškodamas Teismo nuorodų į rizikas dėl duomenų tvarkymo. Galiausiai aptariu konkrečius Teismo sprendimus (pirmiausiai Didžiosios kolegijos sprendimą *de Tommaso v. Italy*), abejodamas dėl juose pateikiamų teisės į teisingą bylos nagrinėjimą taikymo gairių pakankamumo nusikaltimų prevencijos, naudojant algoritmus, kontekste.

**Raktiniai žodžiai:** teisė į teisingą bylos nagrinėjimą, žmogaus teisės ir technologijos, Europos Žmogaus Teisių Teismas, algoritmai nusikaltimų prevencijoje, EŽTT praktika.

## 1. INTRODUCTION

Imagine your name is the same to a well-known criminal. This coincidence makes you a high-risk person in the eyes of law-enforcement: your behaviour is now monitored extensively; the police may stop you more frequently, asking to provide documents; your cell phone use may be monitored.

Mr Angelo de Tommaso has experienced even more. The courts have restricted his movement and communication. Mr de Tommaso appealed and after more than 6 months the courts quashed the restrictions. Later, the European Court of Human Rights found a very limited violation due to the lack of a public hearing in national courts (ECtHR 43395/09).

The recent case of the European Court of Human Rights *de Tommaso v. Italy* highlights perils of crime prevention. The experts also alert us about changing nature of the criminal justice model. Law-enforcement tends to rely more on crime prevention. This trend is worrisome due to emerging technologies used in law enforcement – bringing possibilities to tackle crimes efficiently, doing it before a crime happens. The criminal justice model becomes prospective, based on aggregated data, yet impersonal and distanced (Marks 2017, 708).

In this paper I search for the human rights safeguards available to individuals targeted by algorithmic decision systems in crime prevention. I focus on the case-law of the European Court of Human Rights applying the right to a fair trial and the right to privacy, i.e. Articles 6 and 8 of the Convention. Considering the broad effect algorithmic decision systems could imply, I deliberately exclude analysis of other Convention rights.

I review the conceptual issue in the first part of the paper, asking about the emerging trend to rely on algorithmic decision making in crime prevention. I provide insights on predictive policing tools used by law enforcement. In the second part of the paper I look whether the European Court of Human Rights refers to the threats of Big Data analytics in its privacy case-law. In this part I focus on the Court's case-law, looking for legal reasoning acknowledging threats of future use of collected data.

In the third part of the paper I look for more concrete cases applied in crime prevention – the stage in crime control where predictive analytics bloom. I focus on the right to a fair trial because this right is among the most affected rights by predictive analytics. The European Convention on Human Rights contains two parts of the fair trial guarantees – criminal and civil – that I discuss in turn.

This paper does not claim to tackle systemic risks of Artificial Intelligence Systems in criminal justice (it seems to be too ambitious to offer a holistic analysis of such conundrum in one scholarly paper). It does not offer a comprehensive analysis of how legal frameworks should be adjusted. Many experts wrote great papers on those conceptual questions that inspired my contribution, including Broeders and others (Broeders et al. 2017), Zavirsnik (2018a; 2018b; 2019), Ferguson (2017; 2018); Marks and others (Marks et al. 2017) and others. I concentrate on the limits of the European Convention to curb risks associated with predictive policing based on the case-law of the European Court of Human Rights. This is a doctrinal paper, looking at selected judgments of the European Court of Human Rights and reviewing them in the context of an allegedly shifting paradigm of the criminal justice system.

## 2. HOW IS THE CRIMINAL JUSTICE CHANGING?

### 2.1. Increasing focus on crime prevention in criminal justice

We are witnessing how law-enforcement authorities are emphasising the data driven approach and crime prevention. States enshrine the imperatives of economy, efficiency and effectiveness, following business model ideals. The criminal justice associated with retribution and rehabilitation now focuses more on prevention means. The authorities seek to identify potential criminals before they commit offences (Marks 2017, 708). This is the outcome of increasing reliance on preemptive predictions in criminal justice, used to diminish a person's range of future options (Kerr, Earle 2013).

Zavrsnik explores the ways big data analytics affects criminal justice and crime control. He notices a fundamental change in linguistics discussing law enforcement activities (Zavrsnik 2019). Traditional criminal justice concepts have direct link with human rights safeguards. The law-enforcement authorities modify

the long-standing crime control concepts "to limit the executive power to legal procedures" (Zavrsnik 2019, 5). Emerging concepts of crime prevention such as 'meaning extraction', 'sentiment analysis', 'opinion mining' and 'computational treatment of subjectivity' fall into the grey zone between criminal procedure and crime prevention, blurring the boundaries in the security and crime control (Zavrsnik 2019, 5).

Law enforcement authorities depart from the traditional criminal justice model partly because they want to cure its subjectivity. Economist Daniel Kahneman summarised a good deal of researches: "humans are incorrigibly inconsistent in making summary judgments of complex information" (Kahneman 2013, 224). The criminal justice systems are shifting towards complete de-subjectivation in the decision-making process (Zavrsnik 2018a, 7). Given the accelerating progress of data analytics and data mining capabilities, less and less effort is needed to identify a person from scattered pieces of data. Such pieces do not tell much on their own, but they can be revealing and used to identify a person if taken at the aggregate level (Zavrsnik 2018a, 9).

Predictive data analytics is one of the big data revolution trends (Broeders 2017, 312). It allows law enforcement to predict people's behaviour with a degree of probability. A person qualifies as a suspect before the criminal act and the authorities prevent the criminal act from happening – the general public safety concerns are satisfied. Yet, the predictive data analytics contains risks related to limitations of big data analytics (Broeders 2017, 314).

What are these limits? Computers can only be tasked with making inductive predictions based on past experiences. The future they predict is a continuation of the past data. Actual behaviour of an individual is neglected in such calculations. Zavrsnik underlines the importance of information that can never be properly encompassed by the algorithms (Zavrsnik 2018a, 12). Broeders and others emphasise limited number of crime patterns that can be analysed by algorithms in a meaningful way (Broeders et al. 2017, 314).

### 2.2. Predictive policing and its risks

Predictive policing is one of the fastest growing data analytics tools in criminal law (Isaac 2018, 546). Walter and others define predictive policing as applications designed to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions (Isaac 2018, 546). Predictive analytics shifts law-enforcement towards more transparency, pragmatics, and data-driven policymaking (Isaac 2018, 547).

Experts distinguish between different types of predictive policing tools: some predictive analytics are used in the form of place-based predictive policing, others in person-based targeting (Ferguson 2018, 505). An example of a place-based tools

is the *Baden-Württemberg pilot project P4*.[1] This system uses statistical analysis to identify areas where burglaries of apartments, business premises and car theft are likely to occur.[2] An example of a person-based targeting is the *Hessen-Data* system in Germany. This system combines data from social media with entries in various police databases, data from telephone surveillance to identify potential offenders; the system also helps to identify potential terrorists.[3]

Predictive policing suffers from similar limits and risks as associated with other data analytics. Broeders and others identify the following limits of data analytics (Broeders et al. 2017, 314):

1) Limited data quality or absence of it;
2) Limited technical possibilities of algorithms to meaningfully consider certain complex questions;
3) Lack of causality implication regarding person's activities;
4) The existence of errors in statistical analysis.

The application of data analytics is associated with risks summarized by Broeders and others (Broeders et al. 2017, 314–315), including:

1) The data is based on history which reinforces past biases, magnifying social and economic inequalities;
2) The data analysis violates privacy of people who are not involved in crimes;
3) Uncertain secondary use of data (known as 'function creep');
4) The effect on people behaviour by making them to avoid surveillance (known as 'chilling effect').

Other experts frame these issues differently. For example, Ferguson gives an argument on "black data" problem in Big Data policing (Ferguson 2017, 3). He indicates that there are three overlapping concerns related to "black data": big data policing lacks transparency, because the solution is provided using mathematically complex algorithms; big data policing is racially encoded; big data policing faces legal uncertainty as old constitutional doctrines built on small data principles no longer work in the new big data age (Ferguson 2018, 504).

Ferguson's third point underlines inadequacy of current legal frameworks to regulate big data policing. He suggests that the uncertainty created by old constitutional doctrines driven by "small data principles" applied to solve challenges of Big Data world. Even though Ferguson writes about the issues in the United States, similar challenges are relevant in the European context.

[1] See more details: https://csl.mpg.de/de/forschung/projekte/predictive-policing/ [Accessed: 12 February 2020].

[2] See more details: https://atlas.algorithmwatch.org/report_en/security-and-surveillance/ [Accessed 1 March, 2020].

[3] Ibid.

The shift from traditional criminal investigations to predictive policing implies, on one hand, the possibility to effectively prevent criminal acts from happening, on the other hand, risks undermining personal autonomy, by assigning criminal tendencies to individuals before they actually commit crimes. This diminishes the subjective side of a criminal act, relying on objectively identified risks, using statistical methods. At the same time, prediction may lead to conclusion as to the need to take necessary preventive measures to curb possible crime. This leads to restriction of individual liberties beyond the criminal investigation stage:

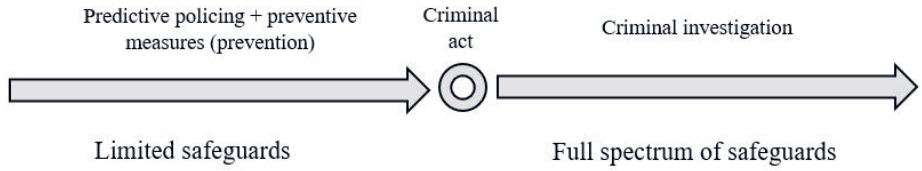


**Fig. 1. Legal safeguards before and after the criminal act – discussing the focus shift of law-enforcement from criminal investigation to crime prevention (created by the author)**

### 2.3. Is the regulatory framework in Europe limited?

The short answer is yes. Current European legal framework is "mainly concerned with the initial data collection phase" (Broeders et al. 2017, 316). Predictive policing is a further step after the collection and retention of data – it concerns the use of such data. The safeguards regarding predictive policing in the European Union falls under the Police and Criminal Justice Authority Directive.[4] Article 1 of the Directive defines that it is applied in crime prevention. This Directive is rather limited tool if compared with the more known General Data Protection Regulation (Marquenie 2017, 338).

One of the practical issues with the Directive is its scope. The decision-making by law-enforcement authorities typically combines both statistical analysis tools and the officer, working with the tool and verifying the conclusion. The participation of an officer in decision-making implies that the decision-making is not considered as "automated processing" in the Directive sense (Brkan 2019, 100). It may limit the application of the Directive to rather unrealistic situations when predictive analytics used without monitoring.

[4] 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 (OJ L 119, 4.05.2016, pp. 89–131).

The Directive also leaves wide discretion to national governments to regulate the use of predictive policing. The absence of strict standards necessitates to look for substantive provisions on more abstract constitutional level. One of prevailing constitutional human rights settings in Europe is the European Convention on Human Rights. The Convention sets basic principles (minimum human rights standards) and the Strasbourg court derives the relevant meaning of them in developing social contexts. This task troubles the Court when emerging technologies are considered.

Emerging technologies fall under existing legal settings that accommodate new reality to a limited extent. The tension grows when courts confront emerging technologies using legal frameworks created in the past without any thought about future challenges. Ferguson identifies this issue as the uncertainty created by old constitutional doctrines driven by "small data principles" to solve challenges of Big Data world (Fergusson 2018). The limits of old constitutional standards could lead to a casuistic case-law on emerging issues. Ziemele underlines the case-law of the European Court of Human Rights on the right to privacy as an example (Ziemele 2020, 2–3).

In practice emerging technologies transformed the right to privacy to a 'fit-for-all' cure. Collection and processing of personal data is traditionally viewed as part of privacy related abuses of human rights. Privacy is the primary concern when we discuss how information technologies may affect us. The privacy principle encompasses "any IT-based processing of personal data, subjecting such processing to the informed determinations of the data subject concerned" (Sartor 2017, 442).

Privacy clauses are the backbones of human rights frameworks addressing information technologies. Unsurprisingly, emerging technologies entered the European Court of Human Rights case-law through the privacy clause. Article 8 § 1 of the European Convention prescribes that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8 § 2 of the Convention reads:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The privacy related case-law of the European court is developing rapidly. Even though there are no cases directly related to predictive policing, it is useful to search for clues on potential risks of further data use in the European Court of Human Rights cases. The analysis of the Court's case-law on privacy may provide an outlook on how does the Strasbourg court approach risks of such data use, implying its approach on tackling threats of predictive analytics.

## 3. THE COURT'S CASE-LAW: THE POTENTIAL OF THE RIGHT TO PRIVACY

Data gathering and its retention preconditions data processing be it predictive policing or other. Ferguson underlines that "growing data collection capabilities have provided incentives to create new search technologies to interrogate the information" (Ferguson 2018, 507). Law-enforcement authorities seek extensive data gathering tools and aims for longer data retention to analyse it later. The right to private life of the European Convention covers data processing.

### 3.1. Early surveillance cases

*Klass and others v. Germany* of 1978 (ECtHR 5029/71) is one of the most important cases of the European court on secret surveillance. In this case the Court held that where a state institutes secret surveillance, individuals could be deprived of their Article 8 rights without being aware and without being able to obtain a remedy. The Court did not find a violation in this case, indicating a wide margin of appreciation of member states in dealing with intelligence activities. The conclusion was based on two factors: the technical advances made in the means of espionage and surveillance; and the development of terrorism in Europe.

The Court dealt with the importance of precise laws regulating interception of telephone conversations in *Kruslin v. France* (ECtHR 11801/85) and *Huvig v. France* (ECtHR 11105/84) of 1990. The judges indicated in both judgments that

> [t]apping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.

The Strasbourg court reiterated the importance of clearly prescribed laws associated with sophistication of technologies in *Kopp v. Switzerland* of 1998 (ECtHR 23224/94). This case concerned surveillance measures adopted in on-going criminal investigation – monitoring of a law firm's telephone lines on prosecutor's orders. The Court held that Switzerland violated Article 8 of the Convention.

Judge Pettiti issued his enlightening concurring opinion in *Kopp*. He underlined that

> the legislation of numerous European States fails to comply with Article 8 of the Convention where telephone tapping is concerned. States use – or abuse – the concepts of official secrets and secrecy in the interests of national security. Where necessary, they distort the meaning and nature of that term. Some clarification of what these concepts mean is needed in order to refine and improve the system for the prevention of terrorism.

Judge Pettiti addressed the broadening scope of law-enforcement authorities using sophisticated tools in criminal justice. He pointed out an obscure distinction between criminal investigation and intelligence activities; and a flexible use of "national security" considerations in interception. Unclear definition of "national security" and a wide discretion of law-enforcement create the potential to gather and retain data in large quantities (which is, again, an important precondition for effective predictive policing).

Judge Pettiti's concurring opinion is relevant today. It took a long time for the European Court to acknowledge that the distinction between individual oriented criminal investigation and intelligence activities – allowing much broader margin of appreciation to the states in the latter – is unclear.

In *Kopp* and, most importantly, the Grand Chamber judgment *Amann v. Switzerland* (ECtHR 27798/95) the Court ruled on the scope of analysis of Article 8 violations in data storing context. The Court indicated that the storing of information by a public authority relating to an individual's private life amounts to an interference within the meaning of Article 8 and the subsequent use of the stored information has no bearing on that finding. This rule disincentivised the Court to expand its analysis into the potential data use, making the use unimportant for the deliberation.

### 3.2. *S. and Marper v. the UK*: Revising the scope of analysis and thinking about the future

The Grand Chamber judgment in *S. and Marper v. the United Kingdom* of 2008 (ECtHR 30562/04) changed the Court's approach about the importance of emerging technologies and data use. The UK authorities retained fingerprints and DNA information when defendants in criminal proceedings were acquitted or discharged. The Strasbourg judges held that the UK violated Article 8 of the Convention. The Court repeated the formula developed in *Leander*, *Kopp* and *Amann* cases as to the limited scope of Article 8 (requiring only the storing fact and disregarding data processing potential) adding that

> in determining whether the personal information retained by the authorities involves any of the private-life aspects […], the Court will have due regard to the specific context in which the information […] has been recorded and retained, the nature of the records, *the way in which these records are used and processed and the results that may be obtained* (italicized by the author).

The Court grounded its approach on another decision *van der Velden v. the Netherlands* (ECtHR 29514/05). This reasoning legitimised individual's concern about the potential use of private information retained by national authorities in future. The Court pointed that

> bearing in mind *the rapid pace of developments in the field of genetics and information technology*, it cannot discount the possibility that in the future the private-life interests bound up with

> genetic information may be adversely affected in novel ways or in a manner *which cannot be anticipated with precision today* (italicized by the author).

Such view is a step towards acknowledging non-linear relationships in technology development applicable in predictive analytics context.

*S. and Marper* case provides an outlook on the actual criminal justice shift occurring in the UK. Arguing for the necessity of the interference the UK Government indicated that law enforcement agencies took full advantage of available techniques of modern technology in the prevention, investigation and detection of crime. The Government added that "the retained material was of inestimable value in the fight against crime and terrorism and the detection of the guilty." The Government provided statistical data to support of their view (paragraph 91 of the judgment). They emphasised the benefits to the criminal-justice system, not only permitting the detection of the guilty but also eliminating the innocent from inquiries and correcting and preventing miscarriages of justice.

The Court observed that the privacy protection 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 pointed out that any state claiming a pioneer role in the development of new technologies bears special responsibility (paragraph 112 of the judgment).

The Strasbourg judges identified stigmatisation of people as a risk of future use of extensive database in criminal justice. They were concerned of "the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons" (paragraph 117 of the judgment).

Predictive policing allows authorities to identify risks before they materialise. For example, data sets allow to indicate that a person is high-risk for certain types of behaviour. Preventive actions taken by authorities based on such information raise doubts as to presumption of innocence – a person's features and circumstances of the situation raise awareness of authorities regardless of actual criminal intent. The Court referred to this risk in *S. and Marper* judgment. The judges also noted that the retention of private data cannot be equated with the voicing of suspicions.

However, the Court started to develop a debatable distinction of people groups justifying different level of privacy intrusion. The Court raised concerns as to presumption of innocence by distinguishing convicts, suspects and non-suspects (as were the applicants in *S. and Marper* case). The Court concluded that the prolonged data retention for non-suspects is unreasonable.

*S. and Marper* case findings re-confirmed in *M.K. v. France* of 2013 (ECtHR 19522/09). In this case the Court analysed the legal framework allowing collection

and retention of fingerprints of non-convicts in France. The Court found a violation of Article 8 of the Convention.

The Court analysed the public prosecutor's peculiar argument rejecting the applicant's request to delete his prints from the police database in *M.K. v. France* judgment. The prosecutor grounded his decision on "the need to protect the applicant's interests by ruling out his involvement should someone else attempt to steal his identity." This argument reflects a motivation of law-enforcement authorities to gather as much data as possible – one of concerns related to the on-going shift of the criminal justice model and the potential of predictive policing.

The Court discussed uncontrollable scope of such approach. The judges found that accepting this argument would justify "the storage of information on the whole population of France" (paragraph 40 of the judgment). This point is interesting in the light of the Court's argument made in an earlier inadmissibility decision in *van der Velden v. the Netherlands* in 2006 (ECtHR 29514/05). In *van der Velden* case the Court noted that the inclusion of DNA profile of the applicant in the national database is beneficial for the applicant as "he may thereby be rapidly eliminated from the list of persons suspected of crimes in the investigation of which material containing DNA has been found." The development enhances protection of human rights afforded by the European Convention.

### 3.3. Collecting data from the convict v. non-convict

The Strasbourg judges pointed out that the retention of fingerprints and DNA information of defendants who are acquitted or discharged violates the Convention in *S. and Marper v. the UK*. The question remained as to the extent the rights of suspects or convicts could be restrained. A few cases clarify this aspect.

The Court analysed taking and retention of DNA profiles of convicted criminals for the use in possible future criminal proceedings in Germany in *Peruzzo and Martens v. Germany* of 2013 (ECtHR 7841/08). The law in Germany allowed the authorities to collect DNA samples and to retain DNA profiles of persons who committed criminal offences of certain gravity and who have negative criminal prognosis. The Strasbourg court declared application inadmissible as manifestly ill-founded. German courts based their finding to take DNA samples and to retain DNA profiles on the gravity of committed offences. Strasbourg judges found reasons sufficient, including the assumption that criminal investigations with respect to similar offences were to be conducted against the applicants in the future (paragraph 48 of the decision).

The Court noted that domestic courts' decisions referred to the applicants' past convictions and their future criminal prognosis without implying allegations that they would be suspected of reoffending (paragraph 53 of the decision). The Court did not address the stigmatisation and biases risks this data retention could have on the applicants if predictive policing tools are used.

In another case *Aycaguer v. France* of 2017 (ECtHR 8806/12) the Court found a violation of Article 8 of the Convention when the legal framework in France prescribed fixed period for retention of DNA samples of convicted offenders irrespective of gravity of offence with no possibility to seek the destruction of such data. The legal framework in France did not differentiate offences, indicating maximum retention period 40 years. The Strasbourg judges treated this period as indefinite.

In 2020 the data retention saga in the UK continued with *Gaughran v. the United Kingdom* (ECtHR 45245/15). In this case the Court reaffirmed the principles laid down in *S. and Marper* judgment. In *Gaughran* case the Court dealt with the law allowing indefinite retention of DNA profile, fingerprints and photograph of persons convicted of a minor offence. The Court found a violation of Article 8 of the Convention in this case.

In the *Gaughran* case the UK Government argued that indefinite retention of biometric data and photograph of a convicted person "is of value in fighting crime, in particular statistics for Northern Ireland show that a significant percentage of convicted adults are re-convicted of a further offence within one or two years. Also, awareness that such data is being retained can deter offenders" (paragraph 62 of the judgment).

### 3.4. Addressing mass surveillance in criminal contexts

Mass surveillance tools allow to gather data required to use predictive analytics. Some of the European court cases deal with mass surveillance and contain references to future data use. The Court analysed surveillance regimes in Russia and Hungary in two cases touching upon the distinction between targeted surveillance in criminal cases and bulk interception.

The Grand Chamber judgment in *Roman Zakharov v. Russia* of 2015 (ECtHR 47143/06) stands out as one of the guiding cases in applying Convention standards for surveillance activities (Spano 2018, 487). Mr Zakharov complained about covert interception of mobile telephone communications in Russia. He argued that the national law permitted the authorities to intercept any person's communications without obtaining prior judicial authorisation. The Court found a violation of Article 8 of the Convention.

The Strasbourg judges' analysis focuses on features of national legislations allowing for intercepting communications. The judges, following earlier inadmissibility decision *in Weber and Seravia v. Germany* of 2006, identified six requirements for the national legislation such as the importance of notification of a person whose communication is being intercepted and the list of potential offences allowing interception. The Court was rather modest in its consequentialist reasoning regarding potential use of collected data in future.

*Szabó and Vissy v. Hungary* (ECtHR 37138/14) judgment of 2016 was exceptional in that regard. This case was again about the quality of national legislation allowing to intercept communications. The Court found a violation of Article 8 of the Convention because of the broad scope of interception measures. The Court underlined crucial insights on potential threats of further use of collected data by law enforcement authorities in this judgment.

The Court indicated the remarkable progress of the techniques applied in monitoring operations which is hardly conceivable for an average citizen (paragraph 68 of the judgment), adding that it must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards. The judges noted that if the governments can acquire a detailed profile of the most intimate aspects of citizens' lives it may result in particularly invasive interferences with private life. The Court underlined that this threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention, pointing out the need to enhance the guarantees under the Convention in the light of technology development (paragraph 70 of the judgment).

**3.5. Addressing national security grounds for mass surveillance**

*Roman Zakharov v. Russia* and *Szabó and Vissy v. Hungary* represent how do national governments expand criminal investigation by giving more discretionary powers to law-enforcement authorities. If national security is at stake, the Convention affords wider margin of appreciation to national authorities in comparison to criminal investigations. But the tension is growing in intelligence related cases as well.

The Court already acknowledged the need to unify safeguards of targeted and mass surveillance, even if margin of appreciation is different when the national security interest is involved. Here we come to Grand Chamber cases of 2021: *Big Brother Watch and Others v. the United Kingdom* and *Centrum för rättvisa v. Sweden*.

In *Big Brother Watch and Others* case the applicants complained about the scope and magnitude of the electronic surveillance programmes operated by the Government and with regard to the intelligence sharing regime. The case *Centrum för rättvisa* concerned a public interest law firm complaint about legislation permitting the bulk interception of electronic signals in Sweden for foreign intelligence purposes.

In these cases the Court referred to developed case-law on minimum requirements that should be set out in a national legal order to avoid abuses of power in interception cases (see, among others, *Weber and Seravia v. Germany* and *Roman Zakharov v. Russia* [GC]). Yet, the Court indicated that despite the fact that the test was equally applied to targeted and bulk interception regimes (compare *Roman*

*Zakharov* and *Weber and Seravia* cases in this regard), "in the intervening years technological developments have significantly changed the way in which people communicate. Lives are increasingly lived online, generating both a significantly larger volume of electronic communications, and communications of a significantly different nature and quality, to those likely to have been generated a decade ago" (paragraph 341 of *Big Brother Watch and Others*). The Court, therefore, decided to develop the minimum safeguards test for bulk interceptions regime to reflect the specific features of it, considering its primarily preventive nature.

The applicants in *Big Brother Watch and Others* case argued that the Court should update existing requirements for interception regimes. They suggested to include requirements for objective evidence of reasonable suspicion, prior independent judicial authorisation of interception warrants, and the subsequent notification of the surveillance subject. This is important because recent technological developments, according to the applicants, made more potential for communications interception *to paint an intimate and detailed portrait of a person's private life and behaviour* (italicised by the author).

Although the Court developed existing requirements for interception regimes, it did not include "reasonable suspicion" criterion, considering the nature of bulk interception:

> the requirement of "reasonable suspicion", which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence (paragraph 348 of the judgment).

The Grand Chamber underlined the importance of the procedures to be followed for selecting, examining, and using intercept material; the precautions to be taken when communicating the material to other parties; the procedures and modalities for supervision by an independent authority; and the procedures for independent ex post facto review, among others.

The Court adopted a procedural approach in *Big Brother Watch and Others* and *Centrum för rättvisa* cases. This approach was already critised by scholars (see, among other, Milanovic 2021; Zalnieriute 2021). Yet, it seems rather difficult to substantially raise minimum requirements for mass surveillance regime by not undermining its essence (see paragraph 424 of *Big Brother Watch and Others* judgment).

For the first time the Court set mass surveillance on an equal foot with targeted surveillance. In paragraph 363 the Court concluded that "the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content". This is an important development considering the potential of big data in crime prevention and the shift to predictive analytics. Even more so, the Court emphasised the gradual steps of uneven intrusion into privacy of a person – depending on a particular

stage of bulk interception the level of intrusion may differ. If during the initial interception stage there may be only limited links to individuals, the final stage (e. g. the use of a report) may include some higher intrusion of privacy – "the degree of interference with privacy rights will increase as the process moves through the different stages" (paragraph 331 of *Big Brother Watch and Others* judgment).

Although critically received the judgments *Big Brother Watch and Others* and *Centrum för rättvisa* shed a light upon mass surveillance and provided an initial legal framework for legal regimes that consider potential of algorithmic decision making in crime prevention. By making a reference to different types of data collected by public authorities the Court underlines a development made in *S. and Marper* that is a turning point, proving the Court's serious attention to data processing potential.

**3.6. What is and what is not a "sensitive data"?**

The Strasbourg court gives much attention to the type of data discussing the proportionality of interference in surveillance cases. A variety of data collected by state authorities was summarised in recent *Breyer v. Germany* case of 2020 (ECtHR 50001/12). This includes the use of surveillance via GPS, telecommunications, retention of fingerprints, cell samples and DNA profiles, metering and other.

Predictive analytics could use all data disregarding its type. The algorithm is used to analyse dataset, looking for correlations. Its success is determined by the precision of the result. One data could be proxy for another. For example, the fact that the person is sleeping could be determined by observing a person, by measuring temperature of his residence, or by looking at his cell phone activities and comparing it with the history trends, and myriads other ways. Sometimes, the combination of seemingly unrelated data could lead to important conclusion.

The logic of linear relationships is not applicable to complex data analytics. Arbesman discusses the complexity permeating our world, noting that "we are unable to fathom the structure and dynamics of huge and complex systems themselves – the way the different pieces interact as a whole" (Arbesman 2011, 71). Selecting the data which is a threat for human rights is risky itself considering uncertainty of predictive analytics potential. But this approach is typical in today data rights legal framework. The GDPR requires more rigorous approach to handle sensitive data. The European Court follows this idea.

The Strasbourg judges flagged DNA data in *S. and Marper* case. In recent *Breyer v. Germany* case the Court analysed legal obligation on service providers to store personal data of users of pre-paid mobile-telephone SIM-cards, making them available to German authorities. The Court did not find a violation, considering personal data of pre-paid mobile-telephone SIM-cards users as insensitive.

The Court concluded that a list of users of pre-paid SIM-cards with names, surnames and addresses did not include any highly personal information; nor did it allow the creation of personality profiles or the tracking of the movements of mobile-telephone subscribers. The Court took a linear approach in this case deciding which type of data may be sensitive in future use. Not even data experts would claim that such conclusion could be certain. The strength of predictive analytics lies in the combination of available data, searching for possible correlations.

The dissenting opinion of judge Ranzoni in this case underlines the risks of the Court's approach. He indicated that the Court's majority "overlooked the fact that the data serves as the key to (sensitive) telecommunications data and enables a person to be linked up to a phone number or a phone number to be connected to a person. It thus facilitates the identification of the parties to every telephone call or message exchange and the attribution of possibly sensitive information to an identifiable person." The judge referred to another case *Benedik v. Slovenia* (ECtHR 62357/14), where the Court considered that it is possible to identify an internet user by obtaining the subscriber information associated with a dynamic IP address.

In yet another *Catt v. the United Kingdom* case of 2019 (ECtHR 43514/15) the Court found a violation of the right to private life due to retention of peaceful campaigner's data on police database. In this case the Court referred to future implications of retention of sensitive data referring to the case-law on surveillance. The Court indicated that the decisions to retain the applicant's personal data did not take into account the heightened level of protection it attracted as data revealing a political opinion, and that in the circumstances its retention must have had a "chilling effect."

### 3.7. The Court is thinking about the future

The European Court develops a cautious approach about the data use under the privacy clause. When data gathering and retention is considered, the Court is starting to consider the potential of the use of data in future, looking into the context of a situation and acknowledging uncertainty about the scope of data use. The prove of this are groundbreaking judgments in cases *S. and Marper, Big Brother Watch and Others* and *Centrum för rättvisa*.

The Court restrictevely approaches future data use under the privacy clause, with the exception of *Big Brother Watch and Others* that included Article 10 (Freedom of Expression) due to the fact that under the bulk interception regime confidential journalist material could have been accessed by the intelligence services. Although the Court lacks non-linear outlook on predictive policing potential indirectly legitimising future use of such tools, it develops a framework potentially capable to deal with such matters. The Convention privacy clause

safeguards individuals from their data collection and retention but the effect on the use of data is still ambiguous. In *Big Brother Watch and Others* and *Centrum för rättvisa* judgments the Court underlines importance of data use by referring to gradual steps of data processing in intelligence activities. Combining this with *S. and Marper* exposure of sensitive data indicates the Court's turn into complicated matters of data processing that is the core of algorithmic decision-making. The recent jurisprudence reveals that the Court becomes sensitive not only to the fact of data collection and its retention but also to its potential use.

The next question is following. What if a person is affected by predictive policing? Should he appeal the use of predictive analytics under the privacy provisions or refer to presumption of innocence under the fair trial safeguards? Although the European Court is aware about the threats of data use to privacy the effects of predictive policing go beyond privacy into the realm of a fair trial. The reasoning in *S. and Marper* shows that the Court is looking for the interlink between privacy and the factual presumption of innocence through stigmatisation concept (Galetta 2013).

Predictive policing helps law enforcement to prevent crime. This may deprive individuals from fair trial safeguards, including the presumption of innocence. I would like to look how does the European Court case-law approaches crime prevention in this regard and what does this imply to predictive policing.

## 4. THE ECTHR CASE-LAW: THE RIGHT TO A FAIR TRIAL

### 4.1. Crime prevention and the European Convention

Fair trial rights under the European Convention sets general principles applicable to the two basic categories of trials in modern justice systems – civil/administrative and those that are criminal in nature (Schabas 2012, 270). These categories are called, accordingly, civil and criminal limbs of the right to a fair trial in the Convention system. Let us discuss the criminal limb first.

Predictive policing is a part of the prevention framework in criminal justice. International human rights obligations are rigorous regarding criminal justice in its traditional sense. Article 6 of the European Convention sets a clear line when fair trial rights could be considered, that is "in determination […] of any criminal charge." Crime prevention formally falls beyond the scope of fair trial, leaving the states broader discretion in this area – "Article 6 is applicable to the preliminary investigation stage of criminal prosecution" (Schabas 2012, 280) but not to preventive measures.

The subsection on stages of criminal proceedings in the Court's guide on the criminal limb of fair trial rights (Guide 2020) begins with the basic rule that crime prevention is not perceived as a stage of criminal proceedings within the meaning of

Article 6 of the Convention. The authors of the guide ground this statement on two cases against Italy: *Raimondo v. Italy* of 1994 and *de Tommaso v. Italy* of 2017.

In *Raimondo v. Italy* (ECtHR 12954/87) the Court ruled that if national authorities restrict the applicant from using its property as a special measure of preventive nature, this is not a criminal sanction because it is designed to prevent the commission of offences (paragraph 43 of the judgment). The context changed from 1994. Authorities rely on crime prevention more than ever. Did the Court develop its case-law after more than 20 years to tackle present challenges?

*De Tommaso v. Italy* (ECtHR 43395/09) tells us a story about Mr de Tommaso who was investigated by Italian law-enforcement authorities. Based on the investigation findings Italian court acknowledged that the applicant had "active criminal tendencies." The national court applied preventive measures justified by these findings. The preventive measures included obligations not to change his place of residence, not to return home later than 10 p.m. or to leave home before 6 a.m.; not to go to bars, nightclubs, amusement arcades or brothels and not to attend public meetings, and not to use mobile phones or radio communication devices among others. The appeal court quashed the measures after 7 months of their application.

Even though *de Tommaso* case does not consider the use of predictive analytics in crime prevention, its implications are applicable in this context. The Court repeated its case-law that the criminal aspect of Article 6 of the Convention should not be applied to crime prevention. The Strasbourg judges observed that "special supervision" in Italy did not involve the determination of a "criminal charge" within the meaning of Article 6 of the Convention (paragraph 43 of the judgment).

Judge Pinto de Albuquerque and Judge Egidijus Kūris addressed flaws related to the Court's majority approach not to apply the criminal fair trial aspect in their dissenting opinions. Some of their arguments point towards the threats of predictive policing.

#### 4.2. What does the criminal limb of a fair trial provision allow?

Before delving into the dissenting opinions in *de Tommaso* case I would like to clarify why is it so important to apply the criminal aspect of a fair trial in predictive policing. Predictive policing touches upon sensitive elements of human autonomy. When law-enforcement authorities identify a person as a "suspect" they increase attention to his activities, including further collection of personal data. Depending on the legal regime, if law-enforcement authorities perceive a person as "high-risk" they can restrict his life using prevention measures as is the case in Italy.

The criminal aspect of a fair trial ensures that the standard of administration of evidence is higher in criminal cases. The presumption of innocence implies that the burden of proof is on the prosecution (ECtHR 10590/83). The actual use

of surveillance technologies shifts the burden of proof to the suspect as it gathers data before the actual criminal proceedings are instituted (and, accordingly, presumption of innocence is activated; see more: Galetta 2013). According to the ECtHR, if authorities obtain evidence by violating privacy clause of the Convention a trial is considered as unfair. This includes situations when law-enforcement uses unlawful secret surveillance (ECtHR 4378/02).

The expectation of publicity is higher in criminal cases in comparison to civil cases. Exceptions to this rule help protecting witnesses' safety or privacy; or promote the free exchange of information and opinion in the pursuit of justice (ECtHR 36337/97). Classified information is not itself an argument for closing a trial from a public in criminal cases. Courts must find that closure is necessary to protect a compelling governmental interest and must limit secrecy if it is necessary to preserve such an interest (ECtHR 28617/03).

The Convention protects individuals by requiring that anyone accused of a criminal offence has the right to remain silent and not to contribute to incriminating himself (ECtHR 19187/91). This requirement evaporates if law-enforcement authorities target a person in crime prevention. For example, when authorities use predictive analytics to identify a person as "high-risk" the Convention does not provide safeguards to this person to refuse giving evidence against himself or his family members.

Moreover, preventive activities could imply negative impact on a person, similarly to criminal prosecution. Take Article 4 § 1 of Protocol No. 7 (right not to be tried or punished twice) of the European Convention extending to the right not to be prosecuted or tried twice. If a person is a "suspect" in crime prevention context, law-enforcement may "supervise" him permanently.

*De Tommaso v. Italy* judgment is worrisome because the Strasbourg court disregarded the effect preventive measures had on applicant's autonomy. Judge Pinto de Albuquerque reasoned why does the severity of measures applied to the applicant is a reason to classify them as "criminal." He analysed the nature of preventive measures in Italy identifying the links with a criminal procedure in many ways. For example, a breach of preventive measures was punishable by a sentence of up to five years' imprisonment. The application of such measures was considered as an aggravating factor in sentencing for criminal offences under the Italian Criminal Code.

This judgment is worth attention in yet another aspect. The majority of the Grand Chamber ignored the fact that the applicant was mistakenly considered dangerous by Italian authorities. The authorities errored but the applicant received neither compensation nor apology from them. In his dissenting opinion Judge Egidijus Kūris regretted that the Court did not find this circumstance sufficient to conduct a proportionality analysis instead of an abstract discussion on the quality of Italian legislation. It is hard to imagine that misidentification of a person

and application of such severe restrictions as in Mr de Tommaso case would be tolerated in criminal proceedings.

The risk of error is one of the major issues in predictive analytics and other forms of algorithmic decision making. For example, experts suggest that DNA analysis software contains codes leading to erroneous conclusions and inaccurate probabilities regarding individual participation in criminal acts. Non-disclosure of the code of such software may hamper the defence just because there is no objective baseline truth against which the software may be evaluated (Lacambra 2018, 32).

Apparently, if national authorities use predictive analytics and apply preventive measures based on their data analysis it does not fall under the criminal aspect of a fair trial of the European Convention. The Convention does not give us adequate safeguards to people affected by predictive analytics today if we accept scholars' warning on threats of expanding scope of crime prevention in criminal justice. Still, in *de Tommaso* judgment the Strasbourg court ruled that the civil aspect of a fair trial might be applied in crime prevention. The Court concluded that some of the restrictions complained of by the applicant "clearly fall within the sphere of personal rights and are therefore civil in nature": the prohibition on going out at night; leaving the district where the applicant lived; attending public meetings or using mobile phones. The Court held that Article 6 § 1 of the Convention had been infringed because the courts did not hold a public hearing.

Perhaps the civil aspect of a fair trial is sufficient to safeguard human rights when predictive analytics is involved? I doubt this for the following reasons.

### 4.3. Why is the civil aspect of a fair trial limited?

The civil aspect of a fair trial does not frame crime prevention in a criminal setting, including burden of proof standards and the presumption of innocence – "[s]tates have greater latitude when their courts are dealing with civil rights and obligations than when criminal matters are concerned" (Schabas 2012, 287). The defendant in criminal proceedings enjoys more safeguards than the party in civil proceedings. Although the requirement of equality of arms applies in principle to civil and criminal cases (ECtHR 8562/79), the civil aspect eliminates safeguards related to the status of a defendant as a party facing the threat of state-based criminal sanctions.

The Convention provides parties with the opportunity to discuss all evidence influencing the court's decision (ECtHR 36515/97). Yet, this right is not absolute. In some cases, it may be necessary to withhold certain evidence from the defence to preserve the fundamental rights of another individual or to safeguard an important public interest. Any difficulties caused to the defence by a limitation on its rights must be sufficiently counterbalanced (ECtHR 35601/04).

But how would the rights be counterbalanced if restrictions are based on predictive analytics conclusions? The law-enforcement may apply an algorithm developed by a private company. The company may have a legitimate interest not to reveal the code entirely. Should the law oblige the companies to reveal their codes? Even so, would this help a "suspect" to argue against complex statistical analysis? The revealed criteria to identify a person as "high-risk" may look objective on the surface but contain proxies for discriminative outcome. Questioning of an algorithm and its results is even more complicated if we consider that the prevention activities (including preventive measures) never shift to criminal investigation by activating fair trial requirements allowing to challenge the evidence.

The civil aspect of a fair trial limits the Strasbourg court possibilities to reject domestically verified algorithm. If national authorities provide a justification for the use of an algorithm, adding their own arguments to explain the outcome of its use, the Strasbourg court would find it difficult to counter their decision.

Even more so, the Strasbourg case-law incentivises domestic authorities to use of available crime prevention tools in order to fulfil positive obligations under the Convention. Take an example of *Kotilainen and Others v. Finland* (ECtHR 62439/12). In this case the Court concluded that Finland violated substantive limb of Article 2 (right to life) of the Convention by failing to preventively confiscate a gun from an individual whose internet postings prior to committing school killings cast doubt on his fitness to safely possess firearms. The factual assessment of evidence as to reasonable suspicion that the individual may pose threat to his school community made by the domestic court was not satisfactory in the Strasbourg court's view. The violation implies the importance to use of available preventive measures to tackle possible risks for other members of the society that itself questions the scope crime prevention could employ available technological means to advance its aim. From the psychological standpoint, if an algorithm is verified by experts, there will be less incentives to doubt its results. Even though law-enforcement authorities and national courts can deviate from the algorithm the psychological factor should be considered. Stubbs and Plesničar notes that "a judge deciding against the prediction of an algorithm is seemingly taking a greater risk and greater responsibility, even though her decision would be the same as without the algorithmic analysis" (Stubbs 2018, 168).

But even the normative standpoint of the Convention does not give much hope for individuals affected by predictive analytics. Recall *de Tommaso* case and the measures applied to the applicant – law-enforcement authorities can apply preventive measures based on the conclusion of predictive analytics. Even if national legislation requires to obtain court's order, it would not be problematic from the European Convention standpoint. Predictive analytics in crime prevention could be justified by public safety grounds. The European Convention does not require to reveal all evidence if compelling grounds not to reveal them exist.

Take an analogy of the case concerning the use of classified evidence to limit person's possibility to use firearms. In *Pocius v. Lithuania* case of 2010 (ECtHR 35601/04) the applicant started proceedings against his entry in a law-enforcement database. The authorities revoked his firearms licenses based on this entry. The evidence was neither disclosed to the applicant nor did he have a possibility to respond to it.[5]

The European Court found a violation of Article 6 of the European Convention in *Pocius* case because the courts did not provide reasons at all. The national court "merely mentioned 'written evidence' against the applicant, without any further explanation." What would the European Court consider as sufficient reasoning in such case? What if the authorities revealed a summary of their evidence to the applicant? He would be able (at least, in theory) to argue such information – this revelation would be satisfactory in the light of the Convention fair trial standard. But would it be sufficient to safeguard people's rights in predictive analytics context?

What if we try to find more concrete status of algorithm-based probabilities in procedural realm? Predictive analytics tools help law-enforcement to ascertain data: the collected data remains a factual background for the algorithm conclusion. In other words, the data is "evidence" leading to the conclusion by the "expert" mechanism. McCormick and others note that the probabilities are not themselves evidence. They are numbers ranging from zero to one that may be used in drawing conclusions from the statistical or other evidence (Kaye et al. 2013, 1267). As Galetta warns, intelligence is not always based on evidence – it has a low exposure to dissent. Intelligence-based evidence is not produced by traditional means of evidence gathering that face particular requirements in a criminal legal order (Galetta 2013). This implies that law-enforcement officials become evidence gatherers and the experts – as managers of algorithms – at the same time. Would expert status help in achieving more scrutiny from national courts? Perhaps. Expert evidence is more intensively regulated field than algorithms as a *sui generis* source of information. The rules regulate expert evidence, ensuring certain reliability standard and providing opportunities to contest expert evidence

Does the European Convention help if we frame algorithms as expert evidence? The answer is uncertain. Take an example of *Devinar v. Slovenia* case of 2018 (ECtHR 28621/15): the national courts appointed applicant's opponent as an expert and relied on the expert opinion in their decision; the applicant relied on Article 6 § 1 of the Convention and alleged that the domestic courts' decisions were unfair; the Strasbourg judges did not find a violation. The European court agreed that if an expert is part of authority (which is a party of the proceedings),

[5] Council of Europe Committee of Ministers information on execution of the judgments of the European Court of Human Rights *Užukauskas* and *Pocius*, available at http://hudoc.echr.coe.int/eng?i=001–163069; [Accessed: 13 March 2020].

the person must have the possibility to raise doubts, including requesting opinion by an independent expert. The Court added that when requesting a second opinion by an independent expert, the applicant is required to produce enough material to substantiate the request. The Court agreed with national authorities that the applicant failed to do so.

Judge Pinto de Albuquerque critisised the reasoning of the majority in this judgment. He argued that this reasoning deviates from existing case-law formed in *Korošec v. Slovenia* of 2015 (ECtHR 77212/12). The Judge underlined the Court's arguments indicating that it was not a decisive factor in *Korošec* case that the applicant failed to submit any argument questioning the authority's findings other than disputing them.

Therefore, if law-enforcement relies on predictive policing tools individuals may have difficulties challenging their decisions even if we frame such decision as expert evidence. The use of predictive analytics involves technical experts. But producing sufficient material to substantiate the request for a second opinion of an independent expert might be unattainable.

## 4. CONCLUSIONS

Big data analytics empower law-enforcement authorities to tackle crime in more effective ways. The criminal justice begins prioritising the use of algorithmic decision systems in prevention of crimes over traditional retrospective criminal investigations. This trend challenges existing human rights safeguards created assuming small data processing.

The European Court of Human Rights discusses the future of data use in its right to privacy case-law. Starting with *S. and Marper v. the United Kingdom* case the European court develops a precautionary approach to data collection and retention associated with threats of its use in future. The Court harmonised privacy standards for different types of surveillance activities. It began discussing stigmatisation of individuals and a "chilling effect" on personal choices.

The European Court of Human Rights maintains a linear approach towards data processing threats. The European court allows national authorities to be more restrictive to convicts in data collection and retention – it puts convicts and other restricted groups at higher risk of stigmatisation. The national security is still a wild card to be used extensively by national authorities collecting and retaining data. Yet, *Big Brother Watch and Others v. the United Kingdom* and *Centrum för rättvisa v. Sweden* are cases where the Court introduced the minimum standards framework addressing mass surveillance, including indications on higher attention to data processing stage of surveillance activities.

Still, the European Convention on Human Rights does not provide sufficient protection for individuals affected by predictive policing under a fair trial

clause. The criminal aspect of a fair trial is not applied in crime prevention – the European Court's findings in *de Tommaso v. Italy* case disregards the restrictive nature of preventive measures. The civil aspect of a fair trial allows easy ways of legitimising law-enforcement preventive activities and provide limited grounds to doubt the conclusions based on predictive analytics.

The paper was prepared as part of my Fulbright Research Scholar programme at Wake Forest University School of Law (2019–2020). I am grateful to Wake Forest University professors, researchers, and the School of Law library personnel. Special thanks to the participants of the Tenth Annual Loyola Constitutional Law Colloquium (Loyola University School of Law, 2019) and the Constitutional law forum (Barry University School of Law, 2020) for their comments that helped me to develop the argument I present in this paper. I would like to thank two anonymous reviewers who provided great insights on how to improve the paper. All errors remain my own.

## BIBLIOGRAPHY

Arbesman, Samuel. 2017. *Overcomplicated: Technology at the Limits of Comprehension*. New York: Portfolio.

Brkan, Maja. 2019. "Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond." *International Journal of Law and Information Technology* 1: 13–20

Broeders, Dennis. Erik Schrijvers. Bart van der Sloot. Rosamunde van Brake. Josta de Hoog. Ernst Hirsch Balin. 2017. "Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data." *Computer Law & Security Review* 33(3): 309–323.

Council of Europe. European Court of Human Rights. 2020. *Guide on Article 6 of the European Convention on Human Rights. Right to a Fair Trial (criminal limb)*. Updated on 31 December 2019. https://www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis/guides&c=# [Accessed: 16 March 2020].

Ferguson, Andrew Guthrie. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.

Ferguson, Andrew Guthrie. 2018. "Illuminating Black Data Policing." *Ohio State Journal of Criminal Law* 15(2): 503–525.

Galetta, Antonella. 2013. "The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?" *European Journal of Law and Technology* 4(2). https://ejlt.org/index.php/ejlt/article/view/221/377 [Accessed: 30 July 2021].

Gorkic, Primoz. 2018. "Judicial Oversight of the (Mass) Collection and Processing of Personal Data." In *Big Data, Crime and Social Control*. Edited by Aleš Završnik. 179–194. London: Routledge.

Isaac, William S. 2018. "Hope, Hype, and Fear: the Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice." *Ohio State Journal of Criminal Law* 15(2): 543–558.

Kahneman, Daniel. 2013. *Thinking Fast and Slow*. New York: Farrar, Straus and Giroux.

Kaye, David H. Kenneth S. Broun. George E. Dix. Edward J. Imwinkelried. Robert P. Mosteller. Ernest F. Roberts. Eleanor Swift. 2013. *McCormick on Evidence*. 7th Edition. St. Paul: Thomaon Reuters.

Kerr, Ian R. Jessica Earle. 2013. "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy." *Stanford Law Review Online* 66(65): 65–72. https://www.stanfordlawreview.org/online/privacy-and-big-data-prediction-preemption-presumption/ [Accessed: 29 July 2021].

Knowles, R. 2014. "National Security Rulemaking." *Florida State University Law Review* (41)4: 883–944. https://ssrn.com/abstract=2511583

Lacambra, Stephanie J. Jeanna Matthews. Kit Walsh. 2018. "Opening the Black Box: Defendants' Rights to Confront Forensic Software." *The Champion*, May: 28–39, 66.

Marks, Amber. Ben Bowling. Colman Keenan. 2017. "Automatic Justice? Technology, Crime, and Social Control." In *The Oxford Handbook of Law, Regulation, and Technology*. Edited by Roger Brownsword, Eloise Scotford, Karen Yeung. London: Oxford University Press.

Marquenie, Thomas. 2017. "The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework." *Computer Law & Security Review* 33: 324–340.

Milanovic, Marko. 2021. "The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa." *EJIL:Talk! Blog of the European Journal of International Law*, May 26, 2021. https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/ [Accessed: 26 July 2021].

Perry, Walter L. Brian McInnis. Carter C. Price. Susan C. Smith. S. John S. Hollywood. 2013. *Predictive Policing: the Role of Crime Forecasting in Law Enforcement Operations*. Rand Corporation.

Sartor, Giovanni. 2017. "Human Rights and Information Technologies." In *The Oxford Handbook of Law, Regulation, and Technology*. Edited by Roger Broownsword, Eloise Scotford, Karen Yeung. London: Oxford University Press.

Schabas, William A. 2015. *The European Convention on Human Rights: A Commentary*. London: Oxford University Press.

Spano, Robert. 2018. "The Future of the European Court of Human Rights – Subsidiarity, Process-Based Review and the Rule of Law." *Human Rights Law Review* 18: 473–494.

Stubbs, Katja Šugman. Mojca M. Plesničar 2018. "Subjectivity, algorithms and the courtroom." In *Big Data, Crime and Social Control*. Edited by Aleš Završnik. Oxon–New York: Routledge.

Zalnieriute, Monika. 2021. "A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence." *EJIL:Talk! Blog of the European Journal of International Law*, June 4, 2021. https://www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence/ [Accessed: 26 July 2021].

Završnik, Aleš. 2018. "Algorithmic crime control." In *Big Data, Crime and Social Control*. Edited by Aleš Završnik. Oxon–New York: Routlege.

Završnik, Aleš. 2018. "Big data. Big Data: What Is It and Why Does it Matter for Crime and Social Control?" *Big Data, Crime and Social Control*. Edited by Aleš Završnik. Oxon–New York: Routlege.

Završnik, Aleš. 2019. "Algorithmic justice: Algorithms and big data in criminal justice settings." *European Journal of Criminology*. https://journals.sagepub.com/doi/10.1177/1477370819876762 [Accessed: 26 July 2021].

Ziemele, Ineta. 2020. "The European Convention on Human Rights: Living Instrument at 70. Science and Technology." *Speech during the opening of the judicial year of the European Court of*

*Human Rights on January 31, 2020.* https://www.echr.coe.int/Pages/home.aspx?p=events/judicial_year&c= [Accessed: 26 July 2021].

**Case Law**

ECtHR decision *Weber and Seravia v. Germany*, 54934/00, 29 June 2006.
ECtHR decision *van der Velden v. the Netherlands*, 29514/05, 7 December 2006.
ECtHR decision *Peruzzo and Martens v. Germany*, 7841/08, 4 June 2013.
ECtHR Grand Chamber judgment *Saunders v. the United Kingdom*, 19187/91, 17 December 1996.
ECtHR Grand Chamber judgment *Amann v. Switzerland*, 27798/95, 16 February 2000.
ECtHR Grand Chamber judgment *S. and Marper v. the United Kingdom*, 30562/04, 4 December 2008.
ECtHR Grand Chamber judgment *Bykov v. Russia*, 4378/02, 10 March 2009.
ECtHR Grand Chamber judgment *Roman Zakharov v. Russia*, 47143/06, 4 December 2015.
ECtHR Grand Chamber judgment *de Tommaso v. Italy*, 43395/09, 23 February 2017.
ECtHR Grand Chamber judgment *Big Brother Watch and Others v. the United Kingdom*, nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.
ECtHR Grand Chamber judgment *Centrum för rättvisa v. Sweden*, 35252/08, 25 May 2021.
ECtHR judgment *Huvig v. France*, 11105/84, 24 April 1990.
ECtHR judgment *Kruslin v. France*,11801/85, 24 April 1990.
ECtHR judgment *Raimondo v. Italy*, 12954/87, 22 February 1994.
ECtHR judgment *Kopp v. Switzerland*, 23224/94, 25 March 1998.
ECtHR judgment *B. and P. v. the United Kingdom*, 36337/97, 24 April 2001.
ECtHR judgment *Fretté v. France*, 36515/97, 26 February 2002.
ECtHR judgment *Belashev v. Russia*, 28617/03, 4 December 2008.
ECtHR judgment *Pocius v. Lithuania*, 35601/04, 6 July 2010.
ECtHR judgment *M.K. v. France*, 19522/09, 18 April 2013.
ECtHR judgment *Korošec v. Slovenia*, 77212/12, 8 October 2015.
ECtHR judgment *Szabó and Vissy v. Hungary*, 37138/14, 12 January 2016.
ECtHR judgment *Aycaguer v. France*, 8806/12, 22 June 2017.
ECtHR judgment *Benedik v. Slovenia*, 62357/14, 24 April 2018.
ECtHR judgment *Devinar v. Slovenia*, 28621/15, 22 May 2018.
ECtHR judgment *Catt v. the United Kingdom*, 43514/15, 24 January 2019.
ECtHR judgment *Breyer v. Germany*, 50001/12, 30 January 2020.
ECtHR judgment *Gaughran v. the United Kingdom*, 45245/15, 13 February 2020.
ECtHR judgment *Kotilainen and Others v. Finland*, 62439/12, 17 September 2020.
ECtHR Plenary judgment*,* 5029/71, *Klass and others v. Germany*, 6 September 1978.
ECtHR Plenary judgment *Feldbrugge v. the Netherlands*, 8562/79, 29 May 1986.
ECtHR Plenary judgment *Barberà, Messegué and Jabardo v. Spain*, 10590/83, 6 December 1988.