EJLT European Journal of Law and Technology

Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity

Plixavra Vogiatzoglou[1]

Abstract

This paper critically examines the judicial regulation of mass surveillance practices undertaken for purposes that include the prevention of serious crime. In essence, this paper assesses the various issues arising from the requirements placed on the private sector, at the behest of security actors, to retain and transfer personal data in bulk for crime prevention purposes. The paper identifies a potential lacuna in the effort of the highest supranational Courts of Europe to delimit this practice and the 'objectivity' criterion established in most recent rulings. It is argued that what are presented as strict requirements may in actuality be significantly more lenient in the context of predictive policing methods.

Keywords: mass surveillance; predictive policing; privacy and data protection

Introduction

As the private sector collects and stores progressively larger amounts of varied data capable of revealing details concerning the personal lives of individuals, new preventive approaches are increasingly employed by security actors, expanding the scope of surveillance measures. In particular, bulk quantities of data are being processed in order to generate useful and reliable correlations, leading to the profiles of potential future suspects. This tendency in fighting crime ties in with the massive accumulation of information within the private sector, as states aspire to get their hands on it.

Private companies are, therefore, being asked to participate in state surveillance en masse by national and European schemes that currently regulate the bulk transfers of personal data from the private sector to security actors. In this paper, the overarching term 'security actors' will be used in order to encompass both law enforcement authorities and intelligence services. As will be discussed further, despite their differences in mandate and competences, several commonalities in intelligence gathering activities and the manner in which bulk personal data transfers are being regulated for the purpose of fight against serious crime, allow for this approach.

Recently, several of the legal instruments regulating private-to-security bulk transfers of data, were placed under the scrutiny of the highest supranational Courts of Europe, i.e. the Court of Justice of the European Union and the European Court of Human Rights. The Courts interpreted the well-established principles of quality of law, including foreseeability, and proportionality in the context of mass surveillance, while their rulings lead to a strict set of criteria that establish a seemingly high threshold of protection for the regulation of private-to-security bulk transfers of personal data.[2]

Nonetheless, questions were raised in relation to the impact and implementation of these criteria. This paper seeks to address the potential problems born by the practical enforcement of the judicial set of criteria vis-à-vis emerging predictive policing methods. More specifically, this paper focuses on a judicial requirement of 'objectivity' that aims at delineating the conditions under which private sector retention of personal data and security agencies' access to private sector databases and further use are allowed. This requirement of objectivity is, however, deemed to clash with the security actors' upcoming practice of searching for the yet unknown suspect.

To that end, this paper is divided in three main sections. The first section of the paper explores modern methods of policing, and in particular predictive policing, and their link to practices of mass surveillance. The judicial regulation and delineation of mass surveillance practices, as extracted by a series of rulings held at a supranational level, are presented in the second section. The third section, then, aims at examining what is referred to as a requirement of objectivity drawn from these rulings, in relation to mass surveillance practices that are being carried out for crime prevention purposes. Finally, this paper reaches the conclusion that the Luxembourg and Strasbourg courts, in regulating private-to-security bulk transfers of personal data, did not give the appropriate consideration to the potential gap born by the application of this requirement in predictive policing methods.

1. Mass surveillance practices in the light of modernisation

1.1. New threats, new rules

During the past two decades, the field of security has been experiencing several changes. Cooperation amongst states, whether EU Member States or third countries, increasingly becomes more intense and more imperative, as crime obtains a more broadly international connotation. New threats to national and public security have risen, while the work of law enforcement on the one hand and intelligence services on the other has growingly been overlapping.[3]

The modern perception of threats shifts the focus towards terrorism, while the separation between the competent security actors has started to blur. Law enforcement authorities turn to tackling external threats and adopt intelligence type of strategies and techniques in fighting crime and increasingly cooperate with intelligence services.[4] In addition, hybrid agencies and organs have emerged in order to facilitate the cooperation and information exchange between security actors. As the threat of terrorism expands outside national frontiers, it encourages the cooperation, exchange of information and adoption of more invasive policies both amongst agents within the same Member State but also amongst EU Member States and with third countries.[5]

Furthermore, a wide range of technological capabilities started to shift the way strategies are being decided on or, in the words of Irion (2015), 'feasibility determines strategies'.[6] Surveillance technologies are becoming faster, smarter, more invasive and more interconnected.[7] Policy makers and security actors push for wider implementation of smart surveillance technologies in the belief that they will increase policing capacities in fighting crime.[8]Increased use of technology is supported under the argument that it will render policing more efficient, whether this statement is eventually proven to be true or not.

In the face of the new threats, new technologies, and their ground-breaking intensity in conjunction with an increasing overlapping of security actors' competences, a new policing prototype started to gain ground. The so-called 'intelligence-led policing' allows for police to employ more invasive, secret-service type of powers, while also resorting to these technologies of

surveillance for the prevention of crime that are more sophisticated than ever. Ratcliffe (2016) defined this notion as a decision-making process that 'facilitates harm and crime, reduction, disruption and prevention through the strategic and tactical management, deployment and enforcement'.[9] More scholars have linked intelligence-led policing primarily to the prevention of crime through information that is gathered into databases around which policing strategies, planning and operations are built.[10] It may, thus, be inferred that intelligence-led policing supports the building up of intelligence through the mass acquisition of data and the formation of large and diverse databases.[11]

1.2. Prevention of crime

Along with the rise of intelligence-led policing, several methods of deterrence of crime have gained a lot of attraction in the recent years, not only in theory but also in practice. While said methods are being referred to as 'predictive', 'preventive', 'pre-emptive' policing and so on, for purposes of coherence and clarification, the term 'predictive policing' will be used in the course of this paper. As implied by the term, predictive policing is defined as the application of 'analytical, particularly quantitative, techniques in order to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions'.[12] Consequently, the aim is not merely to predict future events but also to alter them; in the context of security, this translates in the purpose of deterring crime before it takes place.

The development of predictive policing methods finds its basis on criminology, sociology and major theories of criminal behaviour. In particular, Perry et al (2013) present a consolidated version of these theories, which they refer to as the 'blended theory'. According to the blended theory; 'Criminals and victims follow common life patterns, thus overlaps in those patterns indicate an increased likelihood of crime. Furthermore, geographic and temporal features influence the where and when of those patterns. Finally, as they move within those patterns, criminals make rational decisions about whether to commit crimes, taking into account such factors as the area, the target's suitability, and the risk of getting caught.'[13]

Based on the idea that previously unknown patterns and trends in crime data can be identified and predicted, the first generation of predictive policing methods were built around studies of temporal and spatial dimensions of crime by time series and hotspot analysis.[14] In other words, the possible time slot and place where certain crimes are likely to occur may be predicted, using patterns that are extracted from historic data of previously registered criminal offences. It has been confirmed that rather accurate predictions may be made for certain crimes at certain times and in certain areas, a phenomenon referred to as the 'near repeat effect'.[15]

Moreover, studies have moved towards the prediction of potential offenders and at the same time potential groups or even individual victims.[16] In casu, big data analytical techniques, such as machine learning data mining, are being utilised for the analysis of information that leads to the development of profiles of individuals, who either have in the past or are likely to in the future, commit a criminal offence.[17] These types of predictive policing methods do not only use historic data of crime records but they are also in need of increasingly larger amounts of data that include a wide range of personal information.[18] The aim of this bulk accumulation of data is to generate useful and reliable correlations and ultimately to generate suspects.[19]

As a consequence, in focusing on crimes not yet committed, the line of action is reversed. Security actors start from building a database based on which data are mined in order to predict criminal behaviour of individuals.[20] In this way, data are being aggregated, stored, sorted and mined in

order to provide for patterns and probabilities about how an individual in a particular category is likely to act in the future. This predictive analysis is carried out with the ultimate goal of deterring crime, for instance of uncovering plans for potential terrorist attacks, at the earlier possible stage. To this end, the approach is inductive, as more and more data are required for more and more reliable patterns to emerge. Data are gathered not for a specific criminal investigation but rather for an undetermined purpose, serving a mentality of 'nice-to-have' rather than 'must-have' intelligence.

1.3. Surveilling the masses

Serving this mentality of 'nice-to-have', practices of mass surveillance increasingly become the most popular means used by both law enforcement and intelligence services in the fight against serious crime. Interestingly, the defining contour of the concept of mass surveillance is not clear. While this term is being broadly used, it is not subject to a formal definition, but it is mainly linked to a number of characteristics.[21] Most importantly, the individuals subject to mass surveillance are not clearly defined in advance. In particular, mass surveillance is not directed against a specific individual or group of individuals, but it concerns large parts of the population or even the entire population. Furthermore, as opposed to targeted surveillance, which relates to a past crime, mass surveillance in its current dimension may also be used as a pre-emptive measure, aimed at the prevention of future criminal offences and threats to society at large.[22] Mass surveillance, hence, feeds from a pre-crime mentality that "in order for the suspect to emerge, everyone must be subject to surveillance". [23] Therefore, while practices of mass surveillance may serve a multitude of purposes including prevention, detection, investigation and prosecution of serious crime, as will be analysed further on, this paper seeks to focus only on this first purpose of prevention.

Furthermore, modern practices of mass surveillance are developing as the adoption of intelligence-led policing and predictive policing methods by a wide range of security actors ties in with the current phenomenon where massive amounts of data are produced and collected on a daily basis in the hands of the private sector. Either willingly and intentionally or unconsciously, citizens give away large amounts of their personal data and information to companies that use them towards their own benefit.[24] Consequently, the private sector collects progressively larger amounts of varied data that are able to reveal important information concerning the personal lives and profiles of the individuals, forming a pool of information that the states aspire to dive into.

To that end, private companies are asked to participate in government surveillance through national and European regulatory frameworks that oblige them to collect, store and eventually hand in citizens' personal data to national and third country law enforcement authorities and/or intelligence services. In this way, the practices of mass surveillance in question facilitate and support intelligence-led policing, including predictive policing methods, and the overarching concept of big data analytics, through the vast amplification of security actors' databases.

At an EU level, a number of legal instruments establishes the transfers of personal data generated in the sectors of financial and travel information, to security actors both internally amongst Member States and externally to third countries.[25] Financial information contains personal data such as the names of the beneficiary and the ordering customer, while travel information, in this case Passenger Name Records (PNR) data, are the data required by an airline, in order for an airplane ticket to be bought and may include the passenger's full name, date of birth, address, as well as sensitive information, such as details of any special meal requirements.

A third and most common category of private entities' bulk collection, retention and ultimately transfer of personal data to security actors for the purposes of mass surveillance, consists of electronic communications data. In particular, data generated or processed in the context of publicly available electronic communications services include both content data and metadata. Content data refer to the content of the communication, for instance a conversation, while metadata refer to technical, temporal and spatial elements, for instance the where, when and amongst who a conversation took place. The latter category of data is now being regulated at national level,[26] after the failed European attempt, which will be further analysed in the following section.[27]

Several of these legal instruments regulating mass surveillance practices was placed under the scrutiny of the highest supranational Courts of Europe. This paper, therefore, focuses on the judicial regulation of modern manifestations of mass surveillance, as being carried out through the bulk access of security actors to personal data held by the private sector.

2. The judicial criteria delineating mass surveillance

2.1. The CJEU and ECtHR rulings

In recognition of the high risk of abuse and the legal challenges that practices of mass surveillance present against fundamental rights, namely privacy and data protection, the Court of Justice of the European Union (hereinafter the CJEU) and the European Court of Human Rights (hereinafter the ECtHR) held a number of rulings that interpret the conditions under which the bulk access of security actors to private sector databases for the purpose of mass surveillance may be permissible.[28]

The cases in question, although ranging in content, all revolved around national and European frameworks that regulate, for the purpose of prevention, detection, investigation and prosecution of crime, the bulk access of security actors to personal data, namely electronic communications data and travel information, which are obligatorily retained in the databases of the private sector. Despite of the different nature and competence of each Court, which function upon a different supranational basis, these rulings not only are to a large extent aligned but they also culminated in a nexus of criteria that the national and European instruments regulating practices of mass surveillance must meet in order not to illegally interfere with fundamental rights.[29] This paper, however, aims to point out the issues that may present themselves in the application of some of these criteria in light of the aforementioned predictive policing methods.

In principle, according to both the Charter of Fundamental Rights of the EU (hereinafter the Charter) and the European Convention on Human Rights (hereinafter the ECHR), limitations to fundamental rights that are not absolute, must be provided by law, pursue a legitimate aim of general interest and be necessary and appropriate to achieve said aim.[30] In applying this so-called 'three-step test', both Courts accepted the implementation of mass surveillance practices for the purpose of fighting serious national, transnational and international crime, including terrorism, as a legitimate objective of general interest in a democratic society. They then proceeded in interpreting the well-established principles of foreseeability and proportionality in the context of mass surveillance.

The following paragraphs constitute an effort to present a concentrated and consolidated version of the criteria formulated by the Courts under these principles, before delving into a discussion around a generated requirement of objectivity found within.

2.2. Quality of law

The quality of law implies that the interfering measure must be provided for by national legislation, which, in its turn, must be accessible to the citizens and foreseeable in its application. Foreseeability in the special context of measures of mass surveillance does not compel States to enact legal provisions listing in detail an exhaustive enumeration of situations that may prompt a decision to launch such surveillance operations.[31] The domestic law must rather be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions under which security actors are empowered to access private sector databases. Consequently, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

In particular, the domestic law must set out objective criteria that establish a connection between the transferable data and the objectives pursued.[32] In this way, the scope of the data to be transferred must be delineated clearly and precisely. Moreover, it is important to indicate in a concrete manner the nature of the offences for which data are being collected and transferred from the private sector to law enforcement authorities, while in the context of mass surveillance criminal offences may only be included insofar as they are considered to be 'serious'. Even more so, in the matter of sensitive data, the EU regulatory framework requires a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime.[33]

2.3. Proportionality

According to the principle of proportionality, derogations and limitations in relation to the protection of privacy and personal data must apply only insofar as strictly necessary. Minimum safeguards must be in place, providing the individuals with sufficient guarantees to effectively protect their rights against the risk of abuse. In assessing the proportionality of measures of bulk transfers of data from the private sector to security authorities for purposes of mass surveillance, the Courts singled out several crucial factors. First, the access of the competent national authorities to the private sector databases should, as a general rule, except in cases of validly established urgency, be subject to a prior review or authorisation carried out either by a judicial or in any case by an independent authority. What is more, the decision of that court or body should be made following a reasoned request by those authorities, submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.[34]

Objective criteria must be laid down delimiting the access of the competent national authorities to the data for example through a pre-defined number and position of persons with access authorisation, as well as for the subsequent use of such data clearly and strictly restricted to the purposes for which access was granted. The use of the data by the competent authorities must similarly be strictly restricted and capable of justifying the interference that the use of the specific data entails.[35] It should, nonetheless, be noted here that the latest judgement by the CJEU, i.e. regarding the Passenger Name Records (hereinafter PNR) Agreement between the EU and Canada, presents a differentiation in so far as it allowed for the data of all air passengers indiscriminately to be accessed and processed by the competent authorities. This access and processing are justifiable in the opinion of the Court, as they are intended to 'identify the risk to public security that persons, who are not, at that stage, known to the competent services, may potentially present, and who may, on account of that risk, be subject to further examination'.[36]

Moreover, the implementation of such measures must be supervised, preferably by a judicial body or in any case by an independent authority that is vested with sufficient powers and competence to exercise an effective and continuous control.[37] Onward transfers of the said personal data to other public authorities should be similarly conditional to oversight by an independent supervisory body.[38] During the period of time that the data are stored within the databases of the competent authorities, appropriate organisational and technical measures must be implemented in order to ensure the security and protection of the data.[39] Furthermore, rules must be set out for the erasure or destruction of the transferred personal data when they are no longer necessary.[40]

In addition to the aforementioned, it is also affirmed by the Courts that the individuals subject to these measures should be notified of the access and process of their data by the corresponding authorities, as soon as such notification no longer jeopardises the purpose aimed being served.[41] Lastly, any legislation imposing such measures must also provide for the possibility of an individual to seek effective remedy in order to obtain information and/or access to the data relating to her or him.[42]

2.4. The purpose of prevention

In interpreting the principles of foreseeability and proportionality and analysing the minimum safeguards that materialise them, the Courts do not distinguish between the different purposes for which personal data may be used by the security actors, as provided for by the scrutinised legal instruments. In particular, the potential use of the collected data for the purpose of carrying out predictive policing practices has but once been discussed throughout these rulings by CJEU and ECtHR. It was in its ruling regarding the EU-Canada PNR Agreement, that the CJEU made, for the first time, a specific reference to the use of mass surveillance for the purpose of prevention of serious crime by the Canadian security actors.

More specifically, the Court acknowledged the predictive analysis taking place by automated means of these massive amounts of data, based on pre-established models and criteria for the purpose of identifying individuals that may present risks to public security.[43] In recognising the need for pre-emptive mass surveillance, the Court stated that the pre-established models and criteria should similarly be specific and reliable, making it possible to arrive at results targeting individuals who might be under a reasonable suspicion of participation in terrorist offences or serious transnational crime and should be non-discriminatory.[44] The Court added a final line of protection, requiring that in the case of a positive result obtained following the automated processing of that data and before an individual measure adversely affecting the air passengers concerned is adopted, it must be subject to an individual re-examination by non-automated means.[45]

3. Objective, mass and predictive

3.1. The judicial requirement of objectivity

As may be observed, the usage of the adjective 'objective' is abundant throughout the line of argumentation of both Courts. Objectivity, more specifically, should characterise the conditions of retention within private sector databases as well as the access and use of the acquired personal data within security agencies. Nevertheless, when delving deeper into these elements and how this judicial requirement of objectivity may be materialised, a lacuna seems to present itself.

As regards the conditions on data retention, the CJEU states that retention must be 'targeted for the purpose of fighting serious crime and limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary'.[46] The Court continues on by shedding more light into how data retention may be considered to be limited to what is strictly necessary, by clarifying the manner in which the persons concerned may be delineated. In particular, in deciding which persons should be affected, there must be 'objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.'[47]

In this way, retention may be considered to be limited and targeted, when objective criteria are being used, for instance to describe the persons to be affected. The opinion of the Court, however, seems to be that data retention is objective, and thus targeted, insofar as the public concerned is likely to reveal a link, any kind of link, to a crime or even a threat.

In the same vein, in order to define when access to the personal data retained may be allowed according to the ECtHR, 'a connection, of one way or another, must be made between the person affected and the suspected subjects or objects of planned serious criminal offences, e.g. terrorist attacks'.[48] The vagueness of the language used in casu was even criticised by Judge Pinot de Albuquerque, in his concurring opinion, as being 'indicative of an illusory conviction of global surveillance'.[49] Similarly, in the words of the CJEU, 'in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities'.[50] Therefore, despite the argument that access must be restricted to what is strictly necessary, words like 'might' and 'effective' seem to broaden the scope, weaken the rigidity proclaimed and thus to open the way to looser interpretations.

An indicative example of this wider margin of interpretation may be drawn from a working document published by EUROPOL (2017), which provides for an analysis of this case law in relation to the requirements on data retention and access.[51] According to this document, a data retention measure that is 'targeted', as CJEU provides in the Digital Rights Ireland and Tele 2 Sverige rulings, is practically impossible, since the 'potential relevance amongst data and the purposes pursued cannot be foreseen in advance'. In this way, EUROPOL seems to provide for an interpretation that would 'fit for law enforcement reality', where 'restricted' data retention may still be considered to abide by the CJEU requirement as discussed above, since, in the opinion of EUROPOL, the subsequent access to the retained data must always be 'targeted'. This wordplay portends to the confusion that may be born in relation to the interpretation and implementation of the judicial criteria and the surrounding requirement of objectivity on measures ordering data retention within private databases and access to the data by security actors in general, and for the purpose of prevention of crime in question.

3.2. Objectivity in predictions

More specifically, the question that inevitably arises is how to reasonably implement objective criteria when security actors employ practices of mass surveillance for the purpose of predictive policing, precisely on the grounds that these criteria have not yet been revealed to them. In fact,

this line of thinking is used by the CJEU, when it sets down the rules regarding data retention and access of PNR data, as an argument in favour of widening the scope of persons concerned and subsequently of accepting the need for all air passengers to be affected.[52] In this case, hence, objectivity is translated into ubiquity. This last ruling is claimed to be more restricted in its effect than rulings concerning, for instance, electronic communications data, due to the nature, narrow scope and limited amount of PNR data in relation to the latter.[53] It is, thus, argued that a wider rationale would not be similarly applicable to a vast category of personal data like electronic communications data.

In allowing, however, for a more intensive interference to privacy and to data protection as regards a specific category of data, which, nonetheless, includes special categories of personal data, for the purpose of safeguarding security against the vague threat of terrorism, a precedent is set. What may now be perceived as restricted to a category of personal data, may potentially become widespread in the future, as threats and technological capabilities evolve. Furthermore, as the specific purpose of prevention of crime as well as the analytical technologies employed for that purpose have not been given any other consideration by the Courts, their positioning in the matter remains unclear. Therefore, the applicability of the judicial criteria in the context of mass surveillance for the purpose of prevention of crime is worth further analysis.

3.2.1. Looking for patterns

As discussed in the first section, methods of predictive policing are built around the quest for valuable patterns. Patterns lead to information, for instance profiles of potential criminal offenders, through the probabilistic processing of data.[54] Results, in this case, are based on correlation rather than causality. Correlation has been considered to provide adequate argumentation in favour of characterising these methods and techniques as objective.[55] Nevertheless, instead of accepting correlation as objective per se, I would like to further examine the separate elements of the process that eventually leads to the desired result of correlation.

In order for big data analytics to be effective and result in patterns from which valuable information may be extracted, the raw material must consist of the right quality and quantity of data.[56] Opting for the right quantity of data depends on various subjective factors, such as the accuracy and up-to-dateness as well as the potential human bias.[57] As regards the quantity then, 'objective evidence of contribution in one way or another' may be interpreted as what big data analytics require in order to provide for valuable results. As aforementioned, some predictive policing methods require only historic criminal data, hence data that exist already in the databases of law enforcement and intelligence services. However, this discussion does not address historic data, in the sense of criminal records, but rather the data deriving from the private sector for the purpose of enriching the security actors' databases as raw material.

Following a purely predictive rationale, a lot of confusion is created in relation to which data need to be collected.[58] In particular, defining the amount of data that is sufficient to render big data analytics for predictive policing effectiveness may prove to be quite the brain teaser, especially in light of the fact that the elements capable of producing relevant results may not be known beforehand, as also pointed out by EUROPOL (see supra). Even more so, there seems to be no guidance on how to draw the line between the amount and volume of data that leads to any connection or have any kind of link to a crime or a threat and the one that does not. However, assessing effectiveness may prove to be even more vague and arbitrary than establishing objectivity. As the use of larger datasets is claimed to make it possible to detect correlations and patterns that might otherwise have been missed, effectiveness may be achieved with more rather

than less data.[59] It may deemed, therefore, logical to conclude that, insofar as data make an effective contribution, and, in this case, the more data the more effective the contribution, this requirement of objectivity is fulfilled. In the words of Andrejevic (2014), "populational", i.e. mass, surveillance only works if it is normalised and ubiquitous.[60]

3.2.2. Objectivity and bias

Another aspect not given consideration by the Courts, relates to the potential bias created or perpetuated by modern analytical techniques. Numerous scholars have long identified the manifestation of bias in big data analytics and systems of decision-making automation.[61] While the mathematics behind the analytical techniques may be neutral, their design, development and application may often lead to results that are biased against a group of persons.[62]According to Johnson (2006) 'development is not neutral; there is no objectively correct choice at any given stage of development, but many possible choices'.[63] More specifically, bias may be generated or implemented, even inadvertently, at different stages of development. Bias may be coded into a machine learning system, through the rules, input, hypotheses or assumptions introduced by the human designing the algorithm. Furthermore, bias may occur through the selection of datasets used to train and further feed the algorithm, while technical defects or errors may also lead to biased results.[64]

In predictive policing methods, bias may similarly be built in or generated at various stages, for instance in the technical design, in specifying the predictive algorithms and in determining the datasets subject to analysis.[65] What is of most relevance for this paper is the high risk of bias being born, perpetuated or even enhanced through the selected datasets, including data stemming from past crime records as well as data transferred from the private sector to security actors. In past crime records, certain characteristics, like racial or ethnic origin, might statistically correlate with outcome variables of interest, such as propensity to crime.[66] Furthermore, different data attributes, for instance racial or ethnic origin and geographic location, may not be independent from each other but instead they may be highly related one to the other.[67] For example, a postal code may be highly correlated with racial or ethnic origin, and by extension, with an aforementioned propensity to crime. In this way, clearly identifying which attribute contributes to what extent to the final predictions becomes a difficult task. Moreover, these statistical correlations, albeit mathematically true at some point in time, will provide for results that define future neighbourhoods and persons of criminal interest, which will, however, be likely biased against a specific racial or ethnic origin, community and/or area.[68] In addition, these results will logically lead to a higher demand on behalf of security actors of data transferred from the private sector that relate to this specific racial or ethnic origin, community and/or area.

Therefore, seemingly objective and lawful, under the discussed case law, criteria, such as geographical location, that may be utilised to define the personal data to be transferred from the private sector to security actors for the purpose of carrying out predictive policing methods, may lead to biased results. This issue has only been lightly touched upon by the CJEU in its ruling on the EU-Canada PNR Agreement, where the Court stated that the pre-established models, criteria and databases should be non-discriminatory.[69] Besides the lack of analysis on this topic, this single-sentenced reference to non-discrimination law may also prove inadequate for the protection of citizens' fundamental rights in this context of big data analytics and predictive policing methods. As explained above, in such correlative analyses, it may not always be clear that a final outcome is directly and unlawfully discriminating on the grounds of a protected characteristic, like racial origin.[70] On the contrary, challenges from contextual dependencies might be generated or

brought forth by the algorithms employed, leading to biased or unfairly differential treatment that lays outside the realm of non-discrimination legislation.[71]

3.2.3. Right to a fair trial

Finally, the question that seems inevitable but was never discussed by the Courts, relates to the effect of mass surveillance practices for the purpose of predictive policing on the fundamental right to a fair trial and the principle of presumption of innocence found within. Even though the rights to effective remedy and to fair trial have been invoked in some of the discussed cases, both Courts found that any further analysis on these rights would be redundant, since a violation on the rights to privacy and data protection had already been declared. Indicatively, the ECtHR in its most recent ruling declared the complaint under article 6 of the ECHR (right to a fair trial) to be manifestly ill-founded, by arguing that the right to a fair trial does not apply to 'proceedings relating to a decision to place a person under surveillance'.[72] The Court supports its argument by referencing, first, to the 1978 Klass v. Germany ruling, where the claimants' arguments revolved around notification and remedy, and, second, to the Kennedy v. the United Kingdom ruling, where the ECtHR provided for an analysis solely on the principle of equality of arms found within the right to right to fair trial.[73]

Perhaps more relevant and interesting in cases of mass surveillance, nonetheless, is the potential interference with the principle of presumption of innocence, as established by the right to fair trial. According to this principle, an individual that has been charged with a criminal offence has the right to remain silent and not to discriminate her or himself, any doubt should benefit the accused and the burden of proof of guilt falls with the accuser.[74] The act of charging an individual with a criminal offence has been defined by the ECtHR, as the 'official notification given to an individual by the competent authority of an allegation that he is suspected of having committed a criminal offence'.[75] From that moment on, hence, even in advance of any formal charges, said individuals must be able to enjoy all the guarantees provided by their right to fair trial, while law enforcement agents and prosecutors must respectively respect and allow the exercise of these guarantees. [76]

In the case of personal data being transferred in bulk and then analysed by predictive policing methods, the act of charging an individual may not yet take place. Nonetheless, the individual's criminal procedural rights, as derived from the principle of presumption of innocence, may already become affected.[77] More specifically, mass surveillance forces a shift in the burden of proof, as there is no crime to start from and hence individuals are surveyed before they, if ever, commit any crime. In this way, information referring to a specific individual that may have no knowledge of the content of this information or even the existence of such practice, as the notification requirement rarely takes effect,[78] is collected and may be used as evidence against them. Furthermore, in the words of Ramirez (2013) 'individuals may be judged not because of what they've done, or what they will do in the future, but because inferences or correlations drawn by algorithms suggest they may behave in certain ways'.[79] It is, however, practically impossible to contest any predictive determination about one's future behaviour based on past personal data that have been collected by private companies and transferred in bulk to security actors.[80]

Therefore, a re-examination of the boundaries of the right to a fair trial, including the principle of presumption of innocence, is perhaps warranted in this context. Furthermore, it becomes doubtful that the judicial criteria and the requirement of objectivity, as analysed by the Courts, will suffice to safeguard the citizens' criminal procedural rights. While further analysis, research and active judicial discussion would be essential in order to clarify this matter and provide for legal certainty,

the fear, that the aforementioned vague wording would not meet the threshold of protection of the principle of the presumption of innocence, is born.

3.3. Secondary EU law

For the purpose of completeness, the data quality principles deriving from secondary EU law, namely purpose limitation and data minimisation, as well as the permissible derogations to those principles, must certainly also be taken into consideration in the context of bulk transfers of personal data from the private sector to security actors. [81] The relation between the fundamental right to data protection as enshrined in article 8 of the Charter and the secondary EU legal framework regulating data protection, i.e. the General Data Protection Regulation (hereinafter the GDPR) and the accompanying Directive (EU) 2016/680 on the processing of personal data in the context of criminal justice, is a complex one, while it also extends beyond the scope of this paper. Nonetheless, it is worth clarifying that, in this case, primary and secondary EU law are intensively intertwined in the sense that article 8 of the Charter is inspired by the piece of secondary EU legislation formerly regulating data protection, i.e. the Directive 95/46/EC, [82] and the currently in force GDPR, is a procedural tool enabling the fundamental right to data protection enshrined in article 8 of the Charter. [83] In this way, the GDPR, the Directive (EU) 2016/680 and the legal rules they provide must be informed by the Charter and its interpretation by the CJEU.

To start with, according to the purpose limitation principle, personal data may only be processed for a predefined specified purpose. As a derogation, the processing of personal data for a purpose other than the one for which they were initially collected, is allowed insofar as it is based on law, which constitutes a necessary and proportionate measure in a democratic society, and aims to safeguard the objectives of, inter alia, national security, public security and prevention of criminal offences. [84] In addition, according to the data minimisation principle, the personal data processed by private companies (in the GDPR) and by law enforcement authorities (in Directive (EU) 2016/680) must be adequate, relevant and not excessive in relation to the purpose for which they are collected. [85] In this particular case, personal data that are collected by the private sector for one purpose, for instance in the context of traveling or communicating via publicly available electronic communication services, are transferred in bulk to security agencies for the purpose of prevention of crime. In this way, both principles of purpose limitation and data minimisation are affected and the conditions for the permissible derogations to these data quality principles, as established in the secondary EU law, must be similarly examined.

As aforementioned, the interpretation of secondary law, here the EU data protection framework and the principles established within, must in principle be made in the light of primary law, in casu the Charter and the CJEU case law discussed in this paper, and the analysis of the safeguards stated within. [86] In this way, the conditions of necessity and proportionality, allowing for a derogation to the data quality principles established in the secondary EU data protection framework, may, arguably, be equally assessed as widely or as narrowly as the judicial criteria and respective requirement of objectivity analysed in this paper allow for. In other words, insofar as a legal lacuna is presented in primary EU law, as suggested in this paper, it will be respectively reflected in secondary EU law. Furthermore, the purpose limitation principle is also established in primary EU law, i.e. article 8(2) of the Charter, as one of the elements constituting the fundamental right to data protection. Therefore, any restriction to the purpose limitation principle found within the fundamental right to data protection, must additionally respect the essence of said fundamental right. [87] However, the CJEU has held that the generalised retention of metadata and PNR data for their subsequent transfer to law enforcement authorities do not

adversely affect the essence of fundamental rights to data protection, insofar as organisational and technical measures safeguarding the security, confidentiality, integrity and lawful processing of the personal data are in place.[88] This legal constraint to the conditioned respect to the purpose limitation principle, as established in the Charter is, hence, dissolved.

4. Conclusions

The conundrum of achieving the right balance between security and fundamental rights has spawned a seemingly perpetual discussion that should continue to evolve according to institutional and technological developments. In the face of modern practices of mass surveillance, the highest supranational Courts of Europe took a firm and coordinated stance that is bound to have a great impact on all legal instruments establishing practices of mass surveillance for the wider purpose of the fight against serious crime. In doing so, however, the Courts set outside of their scope of consideration the particular challenges that may arise by the purpose of crime prevention. In this way, the Courts interpreted the conditions on the lawful interferences with the fundamental rights to privacy and to data protection in a seemingly strict manner that may prove insufficient when applied in the specific context of predictive policing methods, a trend that is increasingly growing and evolving amongst security actors at a national, European and international level.

The aim of this paper was to raise the questions concerning the remaining width of the States' margin of appreciation, in delineating the magnitude of personal data that may be lawfully transferred from the private sector to security actors for the purpose of carrying out methods of predictive policing. It was argued that, as rigorous as these judicial criteria may seem to be at first glance, there is still enough room for implementing surveillance practices that are no less mass than before. More specifically, the requirement of objectivity, as formulated in the discussed rulings, may be rendered void in defining the quality and quantity of data to be processed via big data analytics for the determination of profiles and persons susceptible to criminal behaviour. Equally, this judicial criterion neglects the potential for bias in predictive policing methods, as well as the problematic born by the potential interference with the principle of presumption of innocence.

Therefore, the particularities of modern methods of policing and intelligence gathering should be acknowledged and further researched by the Courts. Preventive and predictive processing activities employed by security actors in the context of the fight against serious crime should be considered separately from the reactive and post factum activities. The Courts should consider updating the conditions under which an interference with the fundamental rights to privacy and to data protection may be lawful, according to the ECHR and to the Charter, in light of the issues and factors discussed in this paper. In interpreting and assessing the principles of quality of law, including foreseeability, and proportionality, the risks potentially generated or enhanced by big data analytics, including predictive policing methods, should be explicitly taken into account. As regards the Charter in particular, insofar as it provides for a separate provision on the fundamental right to data protection, further light should be shed on the features constituting the essence of this right. In addition, the interaction between the different elements determining a lawful interference with the fundamental right to data protection, i.e. article 8 paragraphs 1, 2 and 3 and article 52 paragraph 2 of the Charter, and the interaction between the respective primary and secondary EU law, should be further clarified. Finally, the discussion concerning the impact of modern policing practices on the fundamental right to effective trial, and in particular on the principle of presumption of innocence, should be opened.

Acknowledgement

Part of this article is based on and inspired by the author's LL.M thesis prepared in the context of the KU Leuven Advanced Master of Intellectual Property and IT Law in Brussels.

The text has been revised, updated and enriched through further research conducted in the context of the SAURON project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740477.

---

[1] Legal Researcher in the KU Leuven Centre for IT and IP Law (CiTiP). For correspondence: plixavra.vogiatzoglou@kuleuven.be

[2] CJEU: C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014; C-362/14 Maximillian Schrems v Data Protection Commissioner, 06 October 2015; C-203/15 and C-698/15 Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, 21 December 2016; Opinion 1/15, 26 July 2017. ECtHR: Case of Roman Zakharov v. Russia, App. No 47143/06, 04 December 2015; Case of Szabó and Vissy v. Hungary, App. No 37138/14, Final Text 06 June 2016.

[3] Vervaele, JA (2014) 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?', in Gutwirth, S, Leenes, R and de Hert, P (ed) Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges (Springer Netherlands), p.121-122.

[4] Završnik, A (2013) 'Blurring the line between Law Enforcement and Intelligence: Sharpening the gaze of Surveillance?', Journal of Contemporary European Research 9(1), p.182, 186-187.

[5] Brown, I and Korff, D (2009) 'Terrorism and the Proportionality of Internet Surveillance', European Journal of Criminology 6(2), p.125.

[6] Irion, K (2015) 'Accountability unchained: bulk data retention, preemptive surveillance and transatlantic data protection' in Rotenberg, M, Horwitz, J and Scott, J (ed) Privacy in the Modern Age, The search for solutions (The New Press), p.80.

[7] Klitou, D (2014) Privacy-Invading Technologies and Privacy by Design, Safeguarding Privacy, Liberty and Security in the 21st Century (Springer), p.50-51.

[8] van Brakel, R and de Hert, P (2011) 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', Cahiers Politiestudies Jaargang 3(20), p.170-171.

[9] Ratcliffe, J (2016) Intelligence-Led Policing (Routledge, Second Edition).

[10] De Busser, E (2016) 'Private Companies and the Transfer of Data to Law Enforcement Authorities: Challenges for Data Protection', Maastricht Journal 3, p.480-481; Langheinrich, M, Finn, R, Coroama, V and Wright D (2014) 'Quo Vadis Smart Surveillance? How Smart Technologies Combine and Challenge Democratic Oversight', in Gutwirth, S, Leenes, R and de Hert, P (ed) Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges, (Springer Netherlands); Directorate General for Internal Policies Policy Department C (2014) 'Citizen's Rights and Constitutional Affairs, National Security and Secret Evidence in Legislation and before the Courts: Exploring the Challenges', Study for the LIBE Committee, p.18.

[11] Coudert, F (2015) '"Precrime police" is not for 2054, it's for now: how to regulate "data intensive policing"?', Submission to the Amsterdam Privacy Conference 2015; Van Brakel, R and de Hert, P (2011) 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', Cahiers Politiestudies Jaargang 3(20), p.168.

[12] Perry, WL, McInnid, B, Price CC, Smith, SC, Hollywood, JS (2013) 'Chapter One', Predictive Policing - The role of Crime Forecasting in Law Enforcement Operations (RAND Corporation), p.1-2.

[13] Perry, WL, McInnid, B, Price CC, Smith, SC, Hollywood, JS (2013) 'Chapter One', Predictive Policing - The role of Crime Forecasting in Law Enforcement Operations (RAND Corporation), p.3.

[14] Rummens, A, Hardyns, W and Pauwels, L (2018) 'BIG DATA - A scoping review for predictive analysis techniques for predicting criminal events', in Vermeulen, G and Lievens, E (ed) Data Protection and privacy under pressure: Transatlantic tensions, EU surveillance and big data (Maklu - Antwerp), p.254-257.

[15] Fergusson, AG (2017) 'Policing Predictive Policing', Washington University Law Review 94(5), p.1128-1129.

[16] Fergusson, AG (2017) 'Policing Predictive Policing', Washington University Law Review 94(5), p.1137-1143; Perry, WL, McInnid, B, Price CC, Smith, SC, Hollywood, JS (2013) 'Chapter One', Predictive Policing - The role of Crime Forecasting in Law Enforcement Operations (RAND Corporation), p.8-11.

[17] Perry, WL, McInnid, B, Price CC, Smith, SC, Hollywood, JS (2013) 'Chapter Two', Predictive Policing - The role of Crime Forecasting in Law Enforcement Operations (RAND Corporation), p.37.

[18] Rummens, A, Hardyns, W and Pauwels, L (2018) 'BIG DATA - A scoping review for predictive analysis techniques for predicting criminal events', in Vermeulen, G and Lievens, E (ed) Data Protection and privacy under pressure: Transatlantic tensions, EU surveillance and big data (Maklu - Antwerp), p.264-267; Fergusson, AG (2017) 'Policing Predictive Policing', Washington University Law Review 94(5), p.1145.

[19] Andrejevic, M (2014) 'Surveillance in the Big Data Era, Chapter 4, Emerging Pervasive Information and Communication Technologies (PICT)', Law, Governance and Technology Series 11, p.55-56.

[20] Fura, E and Klamberg, M (2012) 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA', Freedom of Expression - Essays in honor of Nicolas Bratza - President of the European Court of Human Rights (Wolf Legal Publishers, Oisterwijk), p.464-465.

[21] Dubuisson, F (2016) 'La Cour Européenne des droits de l'homme et la surveillance de masse', Revue Trimestrielle des Droits de l'Homme 108, p.857.

[22] Milaj, J and Bonnici, JPM (2014) 'Unwitting subjects of surveillance and the presumption of innocence', Computer Law & Security Review 30, p.423.

[23] Andrejevic, M (2014) 'Surveillance in the Big Data Era, Chapter 4, Emerging Pervasive Information and Communication Technologies (PICT)', Law, Governance and Technology Series 11, p.55-56.

[24] Schustera, S, van den Bergb, M, Larruceaa, X, Sleweb, T and Ide-Kostic, P (2017) 'Mass surveillance and technological policy options: Improving security of private communications', Computer Standards & Interfaces 50, p.76.

[25] With regard to financial data: Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73-117. The so-called Fourth Anti-Money Laundering Directive is currently under revision. A compromised text of the Proposal for Directive has been adopted by the European Parliament, for more information see:http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm (accessed on 5 December 2018)

With regard to traveling information: European Commission, Transfer of Air Passenger Name Record (PNR) Data and Terrorist Financing Programme (TFTP), available at the official website: http://ec.europa.eu/justice/data-protection/international-transfers/pnr-tftp/pnr-and-tftp_en.htm (accessed on 5 December 2018)

[26] Indicatively, see Report by EUROJUST (2017) 'Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15', 10098/17, 6 November 2017.

[27] Annulment of the Data Retention Directive in CJEU: C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014.

[28] Cases: CJEU: C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, 8 April 2014; C-362/14 Maximillian Schrems v Data Protection Commissioner, 06 October 2015; C-203/15 and C-698/15 Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, 21 December 2016; Opinion 1/15, 26 July 2017. ECtHR: Case of Roman Zakharov v. Russia, no.47143/06, 04 December 2015; Case of Szabó and Vissy v. Hungary, no.37138/14, Final Text 06 June 2016; Case of Centrum för Rättvisa v. Sweden, no.35252/08, 19 June 2018.

[29] The latest, at the time when this paper was being drafted, relevant ruling by the ECtHR, however, i.e. the Big Brother Watch and others v. the United Kingdom, includes elements that imply a deviation between the two Courts. Whether the two Courts will continue their, thus far, aligned stand or follow separate lines of argumentation in the

future remains to be seen. Case of Big Brother Watch and Other v. the United Kingdom, nos.58170/13, 62322/14 and 24960/15, 13 September 2018.

[30] Charter of Fundamental Rights of the European Union, art.52(1); European Convention on Human Rights, art.8(2).

[31] Zakharov v. Russia, para 228; Centrum för Rättvisa v. Sweden para 101.

[32] C-698/15 Tele2 Sverige, para 119; Zakharov v. Russia, para 260.

[33] Directive 1995/46/EC, art.8; Regulation (EU) 2016/679, art.9; Framework Decision 2008/977/JHA, art.6; Directive (EU) 2016/680, art.10; Charter of Fundamental Rights of the European Union, art.7, art.8 and art.21; Opinion 1/15 para 165.

[34] C-698/15 Tele2 Sverige, para 120; Opinion 1/15, para 202-208; Zakharov v. Russia, para 249; Szabó v. Hungary, para 73.

[35] C-362/14 Schrems, para 93; Opinion 1/15, para 191; Zakharov v. Russia, para 253.

[36] Opinion 1/15, para 187.

[37] C-698/15 Tele2 Sverige, para 123; Opinion 1/15, para 229-230; Szabó v. Hungary, para 79.

[38] Opinion 1/15, para 215.

[39] C-293/12 Digital Rights Ireland, para 66-68; C-698/15 Tele2 Sverige, para 122.

[40] C-362/14 Schrems, para 90; C-698/15 Tele2 Sverige, para 122; Zakharov v. Russia, para 231. It should be pointed out, however, that according to the CJEU, in its latest relevant ruling, an extension of the period of time of retention is justifiable by the average lifespan of international serious crime networks and the duration and complexity of investigations relating to those networks (Opinion 1/15, para 205-209).

[41] Opinion 1/15, para 220-225; Szabó v. Hungary, para 86.

[42] C-698/15 Tele2 Sverige, para 121; Opinion 1/15, para 226-227; Zakharov v. Russia, para 287; Szabó v. Hungary, para 86.

[43] Opinion 1/15, para 130-132, 168-178.

[44] Opinion 1/15, para 172-174.

[45] Opinion 1/15, para 173.

[46] C-698/15 Tele2 Sverige, para 108.

[47] C-698/15 Tele2 Sverige, para 111.

[48] Szabó v. Hungary, para 79.

[49] Szabó v. Hungary, Concurring Opinion of Judge Pino de Albuquerque, para 20.

[50] C-698/15 Tele2 Sverige, para 119.

[51] EUROPOL (2017) 'Proportionate data retention for law enforcement purposes', WK9957/2017 INIT, 21 September 2017.

[52] Opinion 1/15, para 187.

[53] Hijmans, H (2017) 'PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidelines to Negotiators', European Data Protection Law Review 3, p.410-411.

[54] Broeders, D, Schrijvers, E, van der Sloot B, van Brakel, R, de Hoog, J and Hirsch Ballin, E (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, p.314; van Brakel, R and de Hert, P (2011) 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', Cahiers Politiestudies Jaargang 3(20), p.173.

[55] Fergusson, AG (2017) 'Policing Predictive Policing', Washington University Law Review 94(5), p.1124.

[56] Broeders, D, Schrijvers, E, van der Sloot B, van Brakel, R, de Hoog, J and Hirsch Ballin, E (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, p.314

[57] Id.

[58] Gonzaler Fuster, G, de Hert, P, Ellyne, E and Gutwirth, S (2010) 'Huber, Marper and Others: Throwing new light on the shadows of suspicion', INEX Policy Brief 8/2010, (Centre for European Policy Studies), p.5.

[59] Bennett Moses, L and Chan, J (2014) 'Using Big Data For Legal and Law Enforcement Decisions: Testing The New Tools', University of New South Wales Law Journal 37(2), p.664.

[60] Andrejevic, M (2014) 'Surveillance in the Big Data Era, Chapter 4, Emerging Pervasive Information and Communication Technologies (PICT)', Law, Governance and Technology Series 11, p.60.

[61] Indicatively, see: Friedman, B and Nissenbaum, H (1996) 'Bias in Computer Systems', ACM Transactions on Information Systems 14(3), p.330-347; Kitchin, R (2013) 'Big Data and human geography: Opportunities, challenges and risks', Dialogues in Human Geography, 3(3), p.262-267; Mittelstadt, BD, Allo, P, Taddeo, M, Wachter, S and Floridi, L (2016) 'The ethics of algorithms: Mapping the debate', Big Data Society July-December, p.1-21.

[62] Zouave, ET and Marquenie, T (2017) 'An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling', 2017 European Intelligence and Security Informatics Conference, p.19.

[63] Johnson, AJ (2006) 'Technology and Pragmatism: From Value Neutrality to Value Criticality' SSRN Electronic Journal, as cited by Mittelstadt et al (2016) 'The ethics of algorithms: Mapping the debate', Big Data Society July-December, p.7.

[64] Bennett Moses, L and Chan, J (2014) 'Using Big Data For Legal and Law Enforcement Decisions: Testing The New Tools', University of New South Wales Law Journal 37(2), p.648; van Brakel, R (2016) Pre-Emptive Big Data Surveillance and its (Dis)Empowering consequences: The case of Predictive Policing in van der Sloot, B, Broeders, D and Schrijvers, E (ed) Exploring the Boundaries of Big Data (Amsterdam University Press), p.125.

[65] Indicatively, see Perry, WL, McInnid, B, Price CC, Smith, SC, Hollywood, JS (2013) 'Chapter Five' Predictive Policing - The role of Crime Forecasting in Law Enforcement Operations (RAND Corporation), p.115-136; Coudert, F (2015) '"Precrime police" is not for 2054, it's for now: how to regulate "data intensive policing"?', Submission to the Amsterdam Privacy Conference 2015; van Brakel, R (2016) Pre-Emptive Big Data Surveillance and its (Dis)Empowering consequences: The case of Predictive Policing', in van der Sloot, B, Broeders, D and Schrijvers, E (ed) Exploring the Boundaries of Big Data (Amsterdam University Press), p.125-126.

[66] Edwards, L and Veale, M (2017) 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for', Duke Law and Technology Review 16(1), p.28.

[67] Calders, T and Žliobaitė, I (2013) 'Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures', in Custers, B, Calders, T, Schermer, B and Zarsky, T (ed) Discrimination and Privacy in the Information Society (Springer), p.47-48.

[68] Bennett Moses, L and Chan, J (2014) 'Using Big Data For Legal and Law Enforcement Decisions: Testing The New Tools', University of New South Wales Law Journal 37(2), p.672; Lum, K and Isaac, W (2016) 'To predict and serve?', Significance 13(5), p.15-16.

[69] Opinion 1/15, para 172-174.

[70] Bennett Moses, L and Chan, J (2014) 'Using Big Data For Legal and Law Enforcement Decisions: Testing The New Tools', University of New South Wales Law Journal 37(2), p.672; Edwards, L and Veale, M (2017) 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for', Duke Law and Technology Review 16(1), p.30.

[71] Vedder, A and Naudts, L (2017) 'Accountability for the use of algorithms in a big data environment', International Review of Law, Computers & Technology 31(2), p.217-218.

[72] Big Brother Watch and Other v. the United Kingdom, paras 506-513.

[73] Case of Klass and others v. Germany, no.5029/71, 6 September 1978, paras 74-45; Case of Kennedy v. the United Kingdom, no.26839/05, 18 August 2010 Final, paras 184-191.

[74] Charter of Fundamental Rights of the European Union, art.27 and 28; European Convention on Human Rights, art.6.

[75] Case of Deweer v. Belgium, no.Deweer v. Belgium, 27 February 1980, paras 42-46.

[76] Mole, N. and Harby C. (2006) 'The right to a fair trial', Council of Europe, Human rights handbooks, No.3, p.19-20.

[77] Hildebrandt, M (2014) 'Criminal Law and Technology in a Data-Driven Society' in Dubber, MD and Hornle, T (ed) The Oxford Handbook of Criminal Law (Oxford University Press Nov.2014), p.18.

[78] See for example the acknowledgment of the fact by the ECtHR in Centrum för Rättvisa v. Sweden para 165.

[79] Ramirez, E (2013) 'The Privacy Challenges of Big Data: A View From The Lifeguard's Chair', Keynote Address at the Technology Policy Institute Aspen Forum, available at:https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf (accessed on 5 December 2018). Similarly in the context of credit scoring see Citron, DK and Pasquale, FA (2014) 'The Scored Society: Due Process for Automated Predictions', Washington Law Review 89, p.1-33; Zarsky, T (2014) 'Understanding Discrimination in the Scored Society', Washington Law Review 89(4), p.1375-1412.

[80] Mitsilegas, V (2014) 'The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance', International Political Sociology 8(1), p.105.

[81] Regulation (EU) 2016/679, art.5(1).

[82] Kranenborg, H (2014) 'Scope and Interpretation of Rights and Principles' in Peers, S, Hervey, T, Kenner, J and Ward, A (ed) The EU charter of fundamental rights: a commentary (London: Hart Publishing), p.224.

[83] Ausloos, J (2018) The Right to Erasure: Safeguard for informational self-determination in a digital society?, KU Leuven Faculty of Law Doctoral Dissertation, p.60-63, 240-241.

[84] Regulation (EU) 2016/679, art.6(4) in combination with art.21(1).

[85] Directive (EU) 2016/680, art.4.1(c).

[86] Jasserand, C (2017) 'Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?', Computer Law & Security Review 34(1), p.158.

[87] Charter of Fundamental Rights of the European Union, art.52(1).

[88] C-293/12 Digital Rights Ireland, para 39-40; C-698/15 Tele2 Sverige, para 101; Opinion 1/15, para 151.