Big Data-Based Predictive Policing and the Changing Nature of Criminal Justice

– Consequences of the extended Use of Big Data, Algorithms and AI in the Area of Criminal Law Enforcement –

von Prof. Dr. Carsten Momsen and
*Cäcilia Rennert, Attorney at Law**

Abstract
This text[1] contains considerations on the appearance and effects of the use of mass collected and networked data ("Big Data"), their processing for the purpose of analysis, decision preparation and partly already decision substitution by algorithm-based tools ("Algorithms") up to manifestations of artificial intelligence ("AI") in the field of police, security and criminal justice. The result of our considerations is not that the use of new technologies would have to be abandoned, which is not only unrealistic. They can also make the prevention of danger and the detection of crimes more effective.

However, new technologies harbor specific risks. These risks can be identified by the key words lack of understanding of the processes, lack of transparency, lack of individual fairness, promotion and reinforcement of existing inequality, lack of valuation and trust-based decisions, and a variety of individual and structural biases by the people involved in the design, process and evaluation of data processing. In the field of security and criminal justice, they can lead to serious misinterpretations and misjudgments, such as the surveillance and prosecution of innocent people or the violation of elementary principles, e.g. the presumption of innocence.

In addition, there is a tendency to mix up the tasks of the police - which are historically and constitutionally separate, at least in Germany: preventing danger and prosecution of crimes. If the same tools and data are used in both areas, then only potentially dangerous persons and groups will automatically become suspects when corresponding crimes are committed. The overlaps are evident in the area of "Predictive Policing", which we analyze in more detail. This has an impact on central elements of criminal proceedings, which – one might call it that – are becoming "policed". This applies to the concept and function of suspicion as well as to the concept, function and legal status of the accused, for example. These changes may have a direct impact on the structure of criminal proceedings. On the one hand, it may lead to a more adversarial structure, because the individual himself must ensure that his rights are respected, and on the other hand – and this seems even more important - it strengthens an authoritarian structure in criminal proceedings, at least in the area of preliminary proceedings, which are becoming more important compared to the main proceedings. These issues are addressed in the present text. In the context of our research we continue the considerations about the specific consequences of the use of AI and algorithm-based evaluation and prognosis systems. Finally, we will try to develop a framework of human rights as safeguards against a security policy which otherwise might not only undermine privacy.

I. Introduction

Given, the algorithm comes to the conclusion that five persons match all the characteristics that make up the perpetrator type of a certain offence in a certain committing modality in a certain district at a certain time with a certain victim category – just as the algorithm is fed with the learning data.[2] Is everybody of that group now becoming a person who has the right to remain silent? Is a criminal investigation against "unknown", which uses data pools created as part of the threat analysis to substantiate potential suspects, "Predictive Policing", i.e. danger prevention or criminal prosecution? Does everyone to whom a certain combination of characteristics applies after algorithmic evaluation become an accused? Is the evaluation of DNA traces in the context of "Forensic DNA Phenotyping" a search for risk factors or potential perpetrators or even suspects? Where does criminal prosecution begin with the analysis of mass stored data, where does preventing danger and policing end? How high are the risks of discrimination as long the learning data and modes of operation of the algorithm are not transparent and comprehensible for legal decision makers? Does the system produce its own perpetrators according to - possibly politically – predeter-

* Prof. Dr. *Carsten Momsen* heads the Department of Comparative Criminal Law and Procedural Law at Free University Berlin, Faculty of Law and visiting professor at The Center for International Human Rights (CIHR) at John Jay College of Criminal Justice, CUNY – as well he works as a criminal defense attorney. *Cäcilia Rennert* is Assistant Prof. at the Berlin School of Economics and Law, adjunct at the Free University Berlin, Faculty of Law and a criminal defense lawyer and member of the Board of the Berlin Association of Defense Lawyers.

1 The text is a first paper from an ongoing research project at Freie Universität Berlin Faculty of Law and the Center for International Human Rights, John Jay College of Criminal Justice (CUNY). Changes in some aspects may occur in the course of further analyses within the project.

2 *Flynn Coleman*, A Human Algorithm, 2019 (Berkeley) p. XIX, *Nick Bostrom*, Are you living in a computer simulation? Philosophical Quarterly (2003) Vol. 53, No. 211, pp. 243-255, https://www.simulation-argument.com/simulation.pdf.

minated criteria? Moreover, if we lose the clear benchmarks and definitions of the subject matter of the procedure and the roles of the parties involved, it will become increasingly difficult to safeguard the rights of those concerned. For if it is not clear whether we are in the process of predicting and preventing looming danger or whether we are prosecuting specific crimes that already have been committed, we do not know for whom and at what time which procedural rights can be claimed. These procedural rights are human rights, civil rights and liberties. Whenever a citizen is subjected to a police or prosecution measure, his rights are infringed; the most profound intrusion is when he is deprived of his freedom. Theoretically aside the right to freedom, such fundamental rights as the right to food, the right to health, the right to vote, right to be a person under law, the right to access to social media, freedom of expression and not at least the right to personality might be touched – maybe not as a legal guarantee but in the scope for actual exercise and shaping of. It must be borne in mind that interference with these and other fundamental rights is permissible to varying degrees and under different conditions, depending on whether the authorities intervene to prevent danger or to investigate criminal offenses.

The aim of the study is an overarching analysis of possible changes in the relationship between criminal procedural law or criminal prosecution and the public law of danger prevention. The discussion on the so-called "security law" shows that, at least in the field of counterterrorism, the clear separation of security, prevention of crime, precautionary measures and prosecution is eroding.

II. Should there be a Differentiation between Policing and Prosecuting?

In the US and as well in Germany today, in the wake of terrorist or suspected terrorist attacks, police powers have been greatly expanded and the line between security and law enforcement has been blurred, as reflected in the draft new police laws. In some cases, these drafts seek to bring the two areas of law closer together. As well the same measures and tools might become part of police law and criminal procedural law in parallel (e.g. DNA analysis).

1. Protecting Civil Rights and Human Rights

Specific dangers arise in the area of overlap between "Predictive Policing" and criminal investigation, because preassumptions can cloud the unbiased view of actually available evidence against individuals and make their evaluation become more flawed.

The risks are significantly increased if data collected on a massive scale are used multifunctionally as evidence with the claim to objectivity. And once again, if the original data was collected in a different context with a different purpose, for example in health care or social and labor administration. The longer the chain of use becomes, the more likely it is that the criteria for collection, selection or use will per se be based on erroneous assumptions or on assumptions that are incorrect in the originally unintended context of use. Besides the present danger of discrimination against marginal or minority groups, including economically disadvantaged people, specific risks for civil rights arise in the respective context of use, for example in criminal proceedings.[3] An investigation of possible risks to the rights of affected citizens as well as the potential for efficiency gains therefore seems necessary.

2. Biases, Manipulations and Discrimination

Obviously, the problem is more severe when Big Data and AI enter the playfield. This is due to the fact that the same data, databases and processing tools can be used to describe a danger as well as attribute a crime to a citizen, as will be shown in the following. If the same algorithms are used with the same learning data and enriched with other external data, it is not only predictable that the results will be the same. Reinforcement effects, structural loss of rights and discrimination can be the result. However, these effects could be much less serious if one is aware of the inherent risks and weaknesses. Thus, an analysis of modern methods of criminal investigation will be carried out on the following pages compared to those tools already used for "Predictive Policing". The idea is to figure out risks that arise new or increase as a result of using these methods. As will be shown, the greatest risks do not arise from the new technology itself, but from the fact that people who develop and use these tools consciously or unconsciously take over already existing misconceptions into the data analysis. Under these conditions, an algorithm-based analysis of large amounts of data can significantly aggravate already existing biases, such as discriminatory views on certain population groups or persons – without the users in the police and judiciary having to be aware of this.

How does the manipulative and discriminatory use of data occur? Sometimes, but not regularly, it is due to inner attitudes of the programmers or users of Big Data analysis systems. This could lead to the deliberate use of discriminatory criteria, even when designing an algorithm. Users could interpret data according to their biased assumptions. But it is much more likely that the algorithm will tend to confirm tendencies and use more and more data that fit the tendency to sift out the others as irrelevant. In this case, an assumption that is true or at least justifiable in another context can become erroneous due to the migration to another context.

a) The "PredPol"-Tool

This mechanism has been excellently described by *Cathy O´Neil*. She extensively studied the predictive policing tool "PredPol".[4] She isn´t all in all negative to predictive crime models like "PredPol". Compared to the crime-stoppers in Steven Spielberg's dystopian movie Minority Report, the cops do not track down people before they commit crimes. The intent of "PredPol" is to predict

[3] We will discuss the groundbreaking work of *Virginia Eubanks*, Automating Inequality, 2018, in more detail later.

[4] *Cathy O´Neil*, Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, 2018 pp. 84-122.

where and when crimes are likely to be committed. However, if as *Jeffrey Brantingham*, the UCLA anthropology professor who founded "PredPol" argues the model is blind to race and ethnicity gets under scrutiny. True is, that unlike other programs, including the recidivism risk models, which are used for sentencing guidelines, "PredPol" does not focus on the individual. It targets geography. The key inputs are the type and location of each crime and when it occurred. That seems fair enough. And the idea is, if cops spend more time in the high-risk zones, foiling burglars and car thieves, there's good reason to believe that the community benefits.

First problem: Most crimes are not as serious as burglary and grand theft auto, and that is where serious problems emerge. When police set up their "PredPol" system, they have a choice. They can focus exclusively on so-called Part One crimes. These are the violent crimes, including homicide, arson, and assault, which are usually reported to them. But they can also broaden the focus by including so-called Part Two crimes, including vagrancy, aggressive panhandling, and selling and consuming small quantities of drugs. Many of these "nuisance" crimes, as *O´Neil* describes them, would go unrecorded if a cop were not there to see them. This of course leads to the fact that neither an individual has a previous entry in his records nor that the area is marked as unsafe.

O´Neil further argues, these nuisance crimes being endemic to many impoverished neighborhoods. In some places police call them antisocial behavior, or ASB. Unfortunately, including them in the model threatens to skew the analysis. Once the nuisance data flows into a predictive model, more police are drawn into those neighborhoods, where they are more likely to arrest more people. After all, even if their objective is to stop burglaries, murders, and rape, they are bound to have slow periods. It is the nature of patrolling. And if a patrolling cop sees a couple of kids who look no older than sixteen guzzling from a bottle in a brown bag, he stops them. These types of low-level crimes populate their models with more and more dots, and the models send the cops back to the same neighborhood.[5] This creates a pernicious feedback loop. The policing itself spawns new data, which justifies more policing. And our prisons fill up with hundreds of thousands of people found guilty of victimless crimes. Most of them come from impoverished neighborhoods, and most are black or Hispanic. So even if a model is color blind, the result of it is anything but. In our largely segregated cities, geography is a highly effective proxy for race.[6]

b) Indirect Effects

It is crucial to recognize that discrimination or racism need not necessarily to be the result of an appropriate selection of data or criteria. It is much more likely that apparently objective criteria, such as income or education, apply primarily to indirectly certain groups or ethnic groups, with the consequence that in the perception of human users the algorithm, as a result of its analysis, classifies the groups in question as directly exposed to a high level of crime or as being at risk. This erroneous perception could, for example, result in a tendency to regard group members as (probable) suspects against whom investigative measures can be taken, even if the evidence is otherwise insufficient.[7]

O´Neil further examines, if the purpose of the models is to prevent serious crimes, why nuisance crimes are tracked at all. Her answer is that the link between antisocial behavior and crime has been an article of faith since 1982, when a criminologist named *George Kelling* teamed up with a public policy expert, *James Q. Wilson*, to write an essential article in the Atlantic Monthly on so-called "broken-windows policing".[8] The idea was that low-level crimes and misdemeanors created an atmosphere of disorder in a neighborhood. This scared law-abiding citizens away. The dark and empty streets they left behind were breeding grounds for serious crime. The antidote was for society to resist the spread of disorder. This included fixing broken windows, cleaning up graffiti-covered subway cars, and taking steps to discourage nuisance crimes. This thinking led in the 1990s to zero-tolerance campaigns, most famously in New York City – leading to the meanwhile (formally) abandoned "stop-and-frisk tactics. Cops would arrest kids for jumping the subway turnstiles. They were supposed to apprehend people caught sharing a single joint and rumble them around the city in a paddy wagon for hours before eventually booking them. Some credited these energetic campaigns for dramatic falls in violent crimes. Others disagreed. The authors of the best-selling book "Freakonomics" went so far as to correlate the drop-in crime to the legalization of abortion in the 1970s. And plenty of other theories also surfaced, ranging from the falling rates of crack cocaine addiction to the booming 1990s economy. In any case, the zero-tolerance movement gained broad support, and the criminal justice system sent millions of mostly young minority men to prison, many of them for minor offenses."[9]

But zero tolerance actually had very little to do with *Kelling* and *Wilson's* "broken-windows" thesis.[10] Their case study focused on what appeared to be a successful policing initiative in Newark, New Jersey. "Cops who walked

5 *Cathy O´Neil*, Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, 2018 pp. 84-122.
6 *Cathy O´Neil*, Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, 2018 pp. 84-122.
7 *Cathy O´Neil*, Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, 2018 pp. 84-122.
8 *George Kelling and James Wilson*, "Broken Windows: The Police and Neighborhood Safety", Atlantic Monthly, March 1982, www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/.
9 *Cathy O´Neil*, Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, 2018 pp. 84-122.
10 *George Kelling and James Wilson*, "Broken Windows: The Police and Neighborhood Safety", Atlantic Monthly, March 1982, www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/.

the beat there, according to the program, were supposed to be highly tolerant. Their job was to adjust to the neighborhood's own standards of order and to help uphold them. Standards varied from one part of the city to another. In one neighborhood, it might mean that drunks had to keep their bottles in bags and avoid major streets but that side streets were okay. Addicts could sit on stoops but not lie down. The idea was only to make sure the standards didn't fall. The cops, in this scheme, were helping a neighborhood maintain its own order but not imposing their own. (…)"[11] *O´Neil´s* point is that police make choices about where they direct their attention. Today they focus almost exclusively on the poor. That's their heritage, and their mission, as they understand it. And now data scientists are stitching this status quo of the social order into models, like "PredPol", that hold ever-greater sway over our lives.

In this sense, "PredPol", even with the best of intentions, empowers police departments to zero in on the poor, stopping more of them, arresting a portion of those, and sending a subgroup to prison. The automated evaluation of data mountains (data mining) in police operations would be / is problematic if it were used not only in the context of security policing but also in the context of criminal prosecution, in order to generate suspicion regardless of any connection to the crime.[12]

Problem occurring to the image of data as "objective evidence" it is presumable that police chiefs, in many cases, if not most, think that they are taking the only sensible route to combating crime. That is where it is, they say, pointing to the highlighted ghetto on the map. And now they have cutting-edge technology (powered by Big Data) reinforcing their position there, while adding precision and "science" to the process. The result is that we criminalize poverty, believing all the while that our tools are not only scientific but fair. (…) „So, fairness isn't calculated into weapons of math destruction. And the result is massive, industrial production of unfairness. If you think of a weapon of math destruction as a factory unfairness is the black stuff belching out of the smokestacks. It's an emission, a toxic one", convincingly concludes.[13]

c) Efficiency or Fairness

The crucial question is whether we as a society are willing to sacrifice a bit of efficiency in the interest of fairness. Should we handicap the models, leaving certain data out? It's possible, for example, that adding gigabytes of data about antisocial behavior might help "PredPol" predict the mapping coordinates for serious crimes. But this comes at the cost of a nasty feedback loop. So, *O´Neil* argues to discard the data. (…) Although the recidivism model used mostly for sentencing guidelines the biased data from uneven policing funnels right into this model. Judges then may often "look to this supposedly scientific analysis, crystallized into a single risk score. And those who take this score seriously have reason to give longer sentences to prisoners who appear to pose a higher risk of committing other crimes". In a perfect vicious circle that has impact on future "Predictive Policing".

d) Implicit Racism

The problem is that the mass of data has to be cleaned and structured in order to obtain usable information. This process can never be performed in a value-free and completely objective manner.[14] Already the language used in the "learning" of the algorithms transfers possible prejudices of the persons involved.[15] However, the question is why are e. g. nonwhite prisoners from poor neighborhoods more likely to commit crimes? According to the data inputs for the recidivism models, it is because they are more likely to be jobless, lack a high school diploma, and have had previous run-ins with the law. And very likely their friends have, too. Another way of looking at the same data, though, is that these prisoners live in poor neighborhoods with terrible schools and scant opportunities. And of course, they are highly policed. So, the chance that an ex-convict returning to that neighborhood will have another brush with the law is no doubt larger than that of a tax fraudster who is released into a leafy suburb. In this system, the poor and nonwhite are punished more for being who they are and living where they live.

III. Predictive Policing – Overview

Before getting deeper into possible effects by using the modern requisites of "Predictive Policing" we will have a very short overview on the idea and practicing of "Predictive Policing". One of the pioneers among the Western democracies is the United States. From the point of view of public surveillance with CCTV, however, no less the United Kingdom. Interest is also growing in Germany. Predominantly, tools developed in the two countries mentioned above are used. Adaptation to the sometimes significantly different legal framework conditions does not seem to occur frequently.[16]

---

11 *Cathy O´Neil*, Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, 2018 pp. 84-122.

12 *Sabine Gless*, Predictive Policing and operational crime fighting, in constitutional criminal procedure and civil rights, memorial publication for Edda Weßlau, Schriften zum Strafrecht, Volume 297, ed.: Felix Herzog, Reinhold Schlothauer, Wolfgang Wohlers, Duncker & Humblot Berlin 2016

13 *Cathy O´Neil*, Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, 2018 pp. 84-122.

14 *Aleš Završnik*, Big Data, Crime and Social Control (Routledge Frontiers of Criminal Justice), 2018, p.3.

15 *Aleš Završnik*, Big Data, Crime and Social Control (Routledge Frontiers of Criminal Justice), 2018, p.3

16 *Andrew Guthrie Ferguson,* The Rise of Big Data Policing, New York University Press 2017; *Matthias Monroy*, Predictive Policing, in CILIP 113 (September 2017), S. 55 ff.; *ders*. Soziale Kontrolle per Software: Zur Kritik an der vorhersagenden Polizeiarbeit, Cilip, 11 Oktober, 2017, https://www.cilip.de/2017/10/11/soziale-kontrolle-per-software-zur-kritik-an-der-vorhersagenden-polizeiarbeit/; *Vanessa Bauer*, Predictive Policing in Germany. Opportunities and challenges of data-analytical forecasting technology in order to prevent crime, 2019, https://www.researchgate.net/publication/338411808_Predictive_Policing_in_Germany_Opportunities_and_challenges_of_data-analytical_forecasting_technology_in_order_to_prevent_crime; The Cambridge Handbook of Surveillance Law, Hg.: *David Gray, Stephen E. Henderson*, Cambridge University Press 2017.

1. Introduction

In 2011 Time Magazine described "Predictive Policing" as one of the best 50 inventions of the year. Thwart crime before it happens. Know in advance where a crime is about to be committed. What sounds like an ideal seems to have already become reality with "Predictive Policing". And simple data are already sufficient for this. Big Data and their analyses are seen as a great hope in the fight against crime. What "Predictive Policing" means, how it can be used and what problems and questions can arise in this context is explained in the following sections.

2. Definition

"Predictive Policing" refers to the analysis of case data to calculate the probability of future crimes in order to control the deployment of police forces. "Predictive Policing" is based on various aspects of statistics and/or social research.[17] Such systems have become particularly popular in the USA since the beginning of the 2010s, and for some years now they have also been used in Germany or are being tested in pilot projects. The aim is to use this data as a basis for appropriate police measures to prevent potential crimes (preventive) or to better investigate crimes (repressive). This should enable police forces to be deployed in a resource-efficient manner.

3. Applications

According to a study by the Research and Development (RAND) Corporation, there are four categories of application of PPs:

- methods for predicting crimes, to determine places and times when there is an increased risk of crime occurring
- methods for predicting offenders, to determine individuals who are at risk of committing crimes in the future
- methods for predicting offenders, to determine the risk of committing crimes in the future. Methods for predicting perpetrators´ identities, to develop perpetrator profiles in relation to past specific crimes
- methods for predicting victims of crime, to identify groups or individuals who are at increased risk of becoming victims of crime

The idea behind this is that software-supported linking and evaluation of different, large amounts of data makes it possible to make predictions about impending crimes or offences.

4. Predictive Policing and Big Data

It is no coincidence that "Predictive Policing" is often associated with the keyword and subject area Big Data, because Big Data is also about the technological possibilities of processing and evaluating a high volume of data in order to achieve action-leading results. In the case of "Predictive Policing", the aim is thus to achieve strategic and targeted police work that identifies emerging hot spots early on the basis of known crime-related factors.

There are basically two forms of "Predictive Policing". On the one hand, those procedures that relate to future risk locations and times (spatial procedures). On the other hand, those that refer to potential perpetrators and victims (personal procedures).

Within the framework of spatial forecasting procedures, three basic analytical and technical approaches can be distinguished: Hot-spot methods, near-repeat approaches and risk terrain analysis. "Predictive Policing" using personalized data refers to personalized procedures that relate to future perpetrators or victims of crime, i.e. they attempt to determine a crime risk on both the perpetrator and the victim side and to make this risk available to the police. This involves creating a risk profile for individual persons on basis of the data evaluation. As a basis for this, in addition to previous convictions, other police data, e.g. the place of residence or the social environment of the person, which is determined by the evaluation of social media, also serve as a basis. Here, on basis of certain risk factors, probabilities are calculated for individual persons with which these persons will commit crimes or become involved in capital crimes and, if necessary, this information is entered on so-called danger lists. A well-known example is the "Chicago Strategic Subject List". The decisive factor in this context is the thesis that persons whose circle of acquaintances and relatives includes victims or perpetrators of violent crimes have a high risk of also being involved in such crimes in the future.

IV. Foundational Aspects of the Legal Framework

How is "Predictive Policing" to be legally classified and what legal consequences and problems may arise by using certain tools considering the distinction from criminal law?

1. The Preventive Nature of Predictive Policing

"Predictive Policing" is factually located at the borderline between police law and criminal law on the one hand and brings considerable innovations for both fields. However, legally it is part of preventive police law. From the perspective of police law, "Predictive Policing" seems less innovative at first glance. The imminent commission of an

[17] *Sabine Gless*, Predictive Policing and operational crime fighting, in constitutional criminal procedure and civil rights, memorial publication for Edda Weßlau, Schriften zum Strafrecht, Volume 297, ed.: Felix Herzog, Reinhold Schlothauer, Wolfgang Wohlers, Duncker & Humblot Berlin 2016, p. 165.

offence has always been a police offence and allows police action to be taken. However, the preventive fight against crime is also part of the police's canon of tasks (see e. g. § 1 para 3 Berlin Police Law).

At the intervention level, it would now be necessary to clarify which measures can be linked to probability statements by means of "Predictive Policing" software. In the USA, we see this in the example of the so-called "Heat List", where surveillance or hazard warnings are carried out on people who are considered to have a high-risk profile. What is therefore permissible in Germany if police officers are sent to an area where an increased probability of committing a crime is predicted? Striping, simple observations and other measures without intervention character are allowed. On the other hand, different rules would have to apply to intervention measures, which therefore affect the fundamental rights of the person concerned. The stopping and searching of persons, the prolonged observation of certain persons or even a dismissal require a legal basis as fundamental right interventions, the conditions of which must be fulfilled. The basic principle is that interventions are only permitted if there is a sufficient concrete reason for them. In police law, the danger forms this intervention threshold, in criminal procedure law it is basically the suspicion or probable cause requirement that fulfils this function. Sufficiently for a suspicion or probable cause is concrete fact-based evidence that a crime has been committed (by a certain individual). If a crime is suspected, the police can carry out a wide range of fact-finding measures, from telecommunication inspections to apartment or online searches. "Predictive Policing" prognosis, however, only says something about abstract probabilities in the future, whereas the precondition of suspicion of a crime asks for a concrete event in the past. Thus, only an increased risk of committing burglary is stated. Regarding to criminal law, these innovations consist mainly in the prevention orientation.

2. The Retrospective Nature of Criminal Justice

It is precisely the nature of criminal law that it deals with completed life facts and judges them in retrospect. It is true that criminal law is also familiar with the idea of prevention - for example, in the prevention of danger without respect to the offender´s ability and capacity. However, these can hardly be described as such comprehensive and direct preventive action as the "Predictive Policing". Whereas he backbone of criminal responsibility is still guilt - the individual's reprehensibility and blameworthiness. But this is measured by the offense, not by the offender.

3. Basic Distinctions

Other than this reviewing legal assessment, "Predictive Policing" tries to calculate the risk of coming up offenses. Moreover, by substituting the criterion of proofed subjective guilt for that of a calculated objective risk, it is conceivable that criminal intervention will take place before the accused know that they will be committing an infringement of a legal right. Thus, the distinction of police action into preventive (police-law averting of danger) and repressive (criminal procedural criminal prosecution) is becoming increasingly blurred. Self-manifesting in a steady advancement of procedural powers of investigation and is accompanied by a non-excludable loss of rights of the accused.

4. Basic Arguments

The former international Secretary General of Amnesty International, Salil *Shetty*, saw the presumption of innocence from Article 6 II ECHR, Article 20 III in conjunction with Article 28 I 1 GC threatened by "Predictive Policing". He warns that discrimination against ethnic and religious minorities can be increased through "Predictive Policing".

For when the police patrol a "risk area" mentioned by the project appraisal, they usually have the sole information about the location and size of the area in question. Since these trips are also used to look for suspicious events or persons, the question arises as to who is considered suspicious. Stigmatizing indicators such as foreign appearance or a kind of police "typecast" can often be used. There is thus also the fear that not only potential criminals will be targeted, but also other persons, with the consequence that police measures and associated encroachments on fundamental rights will be directed against persons who do not pose a danger. In this context, the question also arises as to the responsibility for forecasts that turn out to be incorrect. Especially if police measures have already been taken against persons affected by it. Can the police (or manufacturers) exculpate themselves by saying that the software has made a false prediction?

In addition, displacement effects or exploitation effects can also occur. There is a risk that "Predictive Policing" does not reduce crime, but possibly only displaces it. Especially with simple systems, it can happen that experienced perpetrators take advantage of the way the systems work. If you know that a burglary will lead to the police patrolling this area more in near future, you are more likely to turn to other areas during this time.

5. The Promise of Effectivity and Prospect

Before we start thinking about the possible development, we first must be aware of how effective "Predictive Policing" actually is. The quality of the data collected is crucial for the quality of the probability statements. The performance therefore depends decisively on what data is used for the probability calculation.

Completeness, correctness, reliability, accuracy and topicality of the processed information are essential. This is particularly important because data errors inevitably lead to misinterpretations. Such misinterpretations are sometimes not even noticed because they may correspond to stigmatizing or conventional patterns of thought. However, algorithms are only as objective as the programmers who created them; as the criminological assumptions on

which they are based; as the data they use.[18] This is particularly true where the techniques are based on crime statistics, because crime statistics do not necessarily reflect the reality of crime, but rather police registration behavior. "Predictive Policing"[19] is the attempt to calculate the probability of future crimes based on the "near-repeat theory" or the assumption of "repeat victimization". Similar to the "Broken Windows" theory it is assumed that past delinquent actions are likely to be followed by others. Data on crime scene and time, prey and approach are processed and weighted according to a specific procedure (scoring). With the help of data mining, patterns are to be recognized and serial offenders are to be tracked down.

According to this logic, the limit of predictability is not determined by the algorithms, but by the computing power of the computers or the data sources that are included in the analysis. Indeed, a study commissioned by the State Office of Criminal Investigation (LKA) of Lower Saxony points out that "Predictive Policing" is ultimately a further development of the crime mapping with which police authorities used to digitize their pins on the map.[20]

6. Basic Critique

One source of uncertainty may be, above all, the possible incorrect legal classification of crimes or too late reporting of the victim, especially in the case of burglaries, which would make the data-based prediction inaccurate and even wrong. Moreover, measuring the effectiveness of the project appraisal is a major problem. If a spatio-temporal prognosis of a software does not apply, i.e. there is no break-in in the room mentioned, then it is basically unclear at first whether the prognosis is wrong or whether the police have been successful in deterring offenders on their behalf. It also means more police operations in a certain area, usually more frequent documentation of crimes.

a) Amplifying Existing Prejudices and Discrimination

"Predictive Policing" can act as an amplifier for existing prejudices and discrimination: For example, if the police patrol more frequently in districts defined as "hotspots", they will record more crime reports there - which in turn will be incorporated with greater weight in future forecasts.

With the use of increasingly digitally generated and retained data, the police is often operating close to the limits of what is permitted in the digital domain under European data protection law.[21] The automation of police security through the introduction of forecasting software should reinforce this trend. Already more than two years ago, the conference of German federal and state data protection commissioners warned against a "further shift of the police intervention threshold in the forefront of dangers and crimes".[22] It is completely unclear today which crimes will be automatically detected in the future and which data sources will be included. With digital investigations, the rule of thumb is that the haystack has to be enlarged in order to find the needle. There is also a risk of incorrect prognoses, which, according to the data protection officers, is to be expected especially with the increasing number of preliminary analyses and is associated with significant consequences for the persons suspected in this process.

In the states of Bavaria and North Rhine-Westphalia, the purpose of the software is to be extended to include other crimes in public places, with car theft or robbery being discussed. The data sources will also be expanded. Currently, weather, traffic data or expected events can be processed. However, from a police perspective, these data are hardly relevant. More meaningful are, for example, the connection of an area to motorways or local traffic, or information on building development. The criminal investigation offices also want socio-economic data on income distribution, purchasing power and creditworthiness or the value of buildings to be used. Some authorities are already obtaining such data from statistical companies. Current water and electricity consumption can also be used to draw conclusions about criminal offences, as this indicates the absence of the occupants. In the state of Baden-Wurttemberg, the Institute for Pattern-Based Forecasting Technology is testing whether the "Precobs" software can be improved with information on the proportion of foreigners or immigrants in a residential area.[23]

b) Privatizing Surveillance through Social Networks

Finally, publicly available information from social networks can also be integrated. Corresponding, already prefiltered data could be supplied by the police authorities themselves. A modern police operations-room nowadays has functions for evaluating trends on Twitter, Facebook or Instagram.[24] This would enable the police to track

---

18 *Aleš Završnik*, Big Data, Crime and Social Control (Routledge Frontiers of Criminal Justice), 2018, p.3

19 *Matthias Monroy*, Soziale Kontrolle per Software: Zur Kritik an der vorhersagenden Polizeiarbeit, Cilip, Oktober, 2017, https://www.cilip.de/2017/10/11/soziale-kontrolle-per-software-zur-kritik-an-der-vorhersagenden-polizeiarbeit/.

20 Predictive Policing – eine Bestandsaufnahme, abrufbar unter https://netzpolitik.org/wp-upload/LKA_NRW_Predictive_Policing.pdf.

21 *Matthias Monroy*, Soziale Kontrolle per Software: Zur Kritik an der vorhersagenden Polizeiarbeit, Cilip, Oktober, 2017, https://www.cilip.de/2017/10/11/soziale-kontrolle-per-software-zur-kritik-an-der-vorhersagenden-polizeiarbeit/ – „Examples are the rapid use of radio cell queries or the sending of silent SMS as a standard measure in investigations".

22 *Matthias Monroy*, Soziale Kontrolle per Software: Zur Kritik an der vorhersagenden Polizeiarbeit, Cilip, Oktober, 2017, https://www.cilip.de/2017/10/11/soziale-kontrolle-per-software-zur-kritik-an-der-vorhersagenden-polizeiarbeit/ – https://datenschutz-berlin.de/attachments/

23 *Matthias Monroy*, Soziale Kontrolle per Software: Zur Kritik an der vorhersagenden Polizeiarbeit, Cilip, Oktober, 2017, https://www.cilip.de/2017/10/11/soziale-kontrolle-per-software-zur-kritik-an-der-vorhersagenden-polizeiarbeit/.

24 „Social Media in der aktiven Polizeiarbeit", heise.de v. 28.6.2016, *Matthias Monroy*, Soziale Kontrolle per Software: Zur Kritik an der vorhersagenden Polizeiarbeit, Cilip, Oktober, 2017, https://www.cilip.de/2017/10/11/soziale-kontrolle-per-software-zur-kritik-an-der-vorhersagenden-polizeiarbeit/.

hashtags or geodata on Twitter during an operation. For example, it would be advantageous for the situation assessment to have tweets from soccer fans or demonstrators displayed in a geo-referenced manner, in order to draw conclusions about soon necessary operational measures.[25] The results of "Predictive Policing" in social media also end up the other way round. The Institute for Pattern-based Predictive Policing has developed an Android app for "Precobs", which is used by the Swiss canton of Aargau under the name "KAPO" ("Kantonspolizei"). Under the motto "The police warns", its users can use push messages to be informed about supposedly imminent crimes in their own residential area. By reporting crimes that have not yet happened, everybody is made block warden.

c) Personalized Data

Since the quality and mass of data is so important, this will lead to a quest to make more and more data usable for such software solutions. The development in the USA makes it clear where the journey is heading.

In Germany, however, there are limits to the collection and processing of personal data under the constitution – and the concept of personal self-determination according to Article 2 I in conjunction with Article 1 I GC. The right of informational self-determination is a manifestation of the general right of personality and was recognized as a fundamental right by the Federal Constitutional Court in the so-called census judgement in 1983.[26] The starting point for the Federal Constitutional Court is the so-called general right of personality (APR), i.e. Article 2.1 of the Constitution (Grundgesetz – GG) in conjunction with Article 1.1 GG. Self-determination in the free development of the personality is endangered by the conditions of modern data processing. Those who do not know or cannot influence what information concerning their behavior is stored and kept in stock will adapt their behavior out of caution. This would not only impair individual freedom of action, but also the common good, since a liberal democratic community requires the self-determined participation of its citizens. "A social order and a legal system enabling this would not be compatible with the right to informational self-determination, in which citizens can no longer know who knows what, when and on what occasion about them".[27]

In the view of the European Parliament, the right to informational self-determination also derives from Article 8(1) of the European Convention on Human Rights:

ARTICLE 8 - Right to respect for private and family life

1.Everyone has the right to respect for his private and family life, his home and his correspondence.

2. 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.

"Correspondence" as well covers any IT-, online- or web-based communication.

Hence, the Federal Constitutional Court (*BVerfG*) emphasizes that the use of such systems is basically only permissible for an objectively determined and limited reason, and that they can only be used without any effort if they are used in response to a dangerous or risky action.[28]

7. Differences and Limitations of Prognostic Decisions in Security Law and Criminal Justice

Using Big Data as well for security purposes and in the field of criminal justice the great challenge for the future will be to find a balance between public safety and the personal rights of the individual. Particular attention should be paid to compliance with the threshold to suspicion of a crime and the rights of the accused. In criminal trials fairness is an important issue. The idea of procedural fairness not just means to respect the presumption of innocence but refers to the whole design of the investigation and trial. It is very much related to a balance of powers reflected in several points like the "Brady Rule", the "Miranda Warnings" and same in the GCP or both the German and the US-Constitution and it´s amendments.

Still, it is an unsolved problem how to translate this idea of fairness into mathematical terms. As *Chelsea Barabas* mentioned[29], bias-based conceptions of validity and fairness fail to interrogate the deeper normative, theoretical, and methodological premises of these tools, which often rely on arrest and conviction data in order to predict future criminal activity and dangerousness. These data directly reflect the allocation of law enforcement resources and priorities, rather than rates of criminal activity.[30]

---

25 *Carsten Momsen und Philipp Bruckmann*, Soziale Netzwerke als Ort der Kriminalität und Ort von Ermittlungen – Wie wirken sich Online-Durchsuchung und Quellen-TKÜ auf die Nutzung sozialer Netzwerke aus? KriPoZ 2019, S. 20 ff.

26 German Federal Constitutional Court (*BVerfG*), judgment of the First Senate,15 December 1983, 1 BvR 209/83 and others – Census, BVerfGE 65, 1.

27 *BVerfG*: Judgment of the First Senate of 15 December 1983 (1 BvR 209/83, marginal no. 146). Federal Constitutional Court. 14 December 1983.

28 *BVerfG*, Order of the First Senate of 4 April 2006, 1 BvR 518/02 – dragnet investigation, BVerfGE 115, 320.
BVerfG, Judgment of the First Senate of 27 February 2008, 1 BvR 370/07 and others – Online search/computer fundamental right, BVerfGE 120, 274.

29 *Chelsea Barabas,* Beyond Bias: Re-imagining the Terms of Ethical AI in Criminal Law, 2019, pp. 2-3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3377921.

30 *Delbert S Elliott*, Lies, Damn Lies, and Arrest Statistics, Boulder, CO: Center for the Study and Prevention of Violence, 1995; *Chelsea Barabas,* Beyond Bias: Re-imagining the Terms of Ethical AI in Criminal Law, 2019, pp. 2-3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3377921.

Another fairness-related problem shown by *Kleinberg* et. al. occurs more statistically[31]: A risk score could either be equally predictive or equally wrong for all races or groups with different numbers of preconditions like criminal records or convictions – but not both. The reason was the difference in the frequency with which blacks and whites were charged with new crimes. "If you have two populations that have unequal base rates,'' *Kleinberg* said, "then you can't satisfy both definitions of fairness at the same time." The researchers constructed a mathematical proof that the two notions of fairness are incompatible. Especially in the criminal justice context, false findings can have far-reaching effects on the lives of people charged with crimes. Judges, prosecutors and parole boards use the scores to help decide whether defendants can be sent to rehab programs instead of prison or be given shorter sentences. Concerning future predictive measures, a self-fulfilling prophecy is nearly inevitable.[32] Trust is another important decision criterion maybe impossible to express as algorithmic function. To find a proper and individually just decision it must be considered if and how much the human being object of the decision can be trusted.

However, as *Cathy O´Neil* wrote, from a mathematical point of view, trust is hard to quantify.[33] Because trust can only be earned by personality and character. Those are just individual expectations not to be analyzed by typical Big Data. If so, usually the outcome would be to trust somebody more ore even less because he belongs to a certain group with a percentage XY failing to be compliant. Highly biased and kind of algorithm´s cognitive dissonance.[34] The problem exists in both areas, "Predictive Policing" and criminal investigation. Compared to criminal procedures there not that strong safeguards for civil rights for predicting crimes than for prosecuting them. So, the problem does not matter exactly in the same way. However, as the German debate on "Forensic DNA Phenotyping" showed, there is the risk that the whole political approach is biased even when it comes to preventive measures.[35]

8. Biased Learning Data

The data processed in "Predictive Policing" is drawn from police crime statistics, which can be tendentious. It registers reports, not actual crimes. If the police use this data to check people with a certain appearance or in socially deprived areas more frequently, more crime reports are also recorded there. These are used as case statistics in predicting crime and confirm the apparent assumption that crime is on the rise in these neighborhoods or by these groups of people. [36] This creates a variety of problems, in summary one could say only "conspicuous" people were cut in, such as people with hoodies, neglected clothing or dark skin color. The investigative journalist platform "propublica.org" also proved that people with dark skin color are indeed systematically disadvantaged by the (mostly unknown) algorithm.[37]

Similar stereotypes can also be observed in Germany.[38] In the German federal states, the state criminal investigation offices want to get close to the target group "travelling serial burglars". What is not said: In the international context, the term stands for "Mobile Organized Crime Groups", which usually refers to so-called "travelling criminals" from Romania and Bulgaria aka Sinti and Roma aka "Gypsies".[39] German and European "Predictive Policing" thus focuses on persons whose origin is suspected to be primarily in Southern and Eastern Europe. Again, the unintended effects increase the more the prognosis is narrowed down to individual persons.[40] This applies both in the area of "Predictive Policing" and in criminal prosecution. However, if the same data and analyses

---

31 *Jon Kleinberg, Sendhil Mullainathan, Manish Raghavan*, Inherent Trade-Offs in the Fair Determination of Risk Scores, Cornell University, 2016, https://arxiv.org/pdf/1609.05807.pdf.

32 *Julia Angwin and Jeff Larson,* Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say, ProPublica, Dec. 30, 2016, https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say.

33 *Cathy O´Neil*, Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, 2018, pp. 102-104.

34 *Carsten Momsen and Sarah Lisa Washington*, Wahrnehmungsverzerrungen im Strafprozess – die Beweisprüfung im Zwischenverfahren der StPO und US-amerikanische Alternativen (Perception Bias in Criminal Proceedings – the Examination of Evidence in Interim Proceedings in the German Code of Criminal Procedure and US-American Alternatives), in: Goeckenjan/Puschke/Singelnstein, Festschrift für Ulrich Eisenberg, Berlin 2019, S. 453 ff.

35 *Carsten Momsen* and *Thilo Weichert*, From DNA Tracing to DNA Phenotyping – Open Legal Issues and Risks in the new Bavarian Police Task Act (PAG) and beyond, Verfassungsblog, 2018, https://verfassungsblog.de/from-dna-tracing-to-dna-phenotyping-open-legal-issues-and-risks-in-the-new-bavarian-police-task-act-pag-and-beyond/.

36 *Matthias Monroy*, Soziale Kontrolle per Software: Zur Kritik an der vorhersagenden Polizeiarbeit, Cilip, Oktober, 2017, https://www.cilip.de/2017/10/11/soziale-kontrolle-per-software-zur-kritik-an-der-vorhersagenden-polizeiarbeit/; *Bernd Belina*: 'Predictive Policing' ist diskriminierend – und ein dubioses Geschäftsmodell (Predictive Policing' is Discriminatory - and a Dubious Business Model), www.rosalux.de/news/id/14431/schuldig-bei-verdacht.

37 *Julia Angwin and Jeff Larson*, ProPublica – Machine Bias – "Bias in Criminal Risk Scores Is Mathematically Inevitable, Researchers Say - ProPublica's analysis of bias against black defendants in criminal risk scores has prompted research showing that the disparity can be addressed – if the algorithms focus on the fairness of outcomes", Dec. 30, 2016, https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say.

38 *Carsten Momsen and Sarah Lisa Washington*, Wahrnehmungsverzerrungen im Strafprozess - die Beweisprüfung im Zwischenverfahren der StPO und US-amerikanische Alternativen (Perception Bias in Criminal Proceedings - the Examination of Evidence in Interim Proceedings in the German Code of Criminal Procedure and US-American Alternatives), in: Goeckenjan/Puschke/Singelnstein, Festschrift für Ulrich Eisenberg, Berlin 2019, S. 453 ff.

39 *Open Society, Institute*, Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory, 2009, https://www.justiceinitiative.org/uploads/8cef0d30-2833-40fd-b80b-9efb17c6de41/profiling_20090526.pdf.

40 *Melissa Hamilton*, The biased Algorithm: Evidence of Disparate Impact on Hispanics, in American Criminal Law Review, Vol. 56 (2018), pp. 1553 ff., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251763.

are used first in the security sector and then also in the identification of possible suspects, an additional biasing effect can occur, since the risk analysis can very easily only be confirmed without the specific legal guarantees of criminal proceedings being taken into account.

9. Confirmed Preconceptions

The creation of the data leads to further problems. As all police officers know crime data is the result of their own work, is forgotten by the algorithmizing and by the presentation of the results in the form of maps. The software's prediction appears as objective, as reliable, as a purely technical statement that has been made without human intervention and free from inaccuracies, influences and interests. If it is accepted that black, Muslim and poor people are much more likely to be controlled and reported by the police, then "Predictive Policing" has the potential to reinforce these racisms bigotries and classicisms. However, there will more data on some groups than on other. If certain groups are over-represented in the (learning) data, then the calculations will lead the police to exactly where those groups are present, and e.g. black, Muslim and poor people will be targeted again because the software suggests they are. The new technology thus may stand in the way of all attempts to reduce discriminatory police.[41]

10. Unknown Function and Limited Utility of Algorithms

There is no evidence that "Predictive Policing" leads to a reduction of crime in a certain area. There is a lack of robust research. This is also pointed out by the state-police in Lower Saxony, who commissioned the study mentioned above. So far, only perceived effects can be determined. Two studies should shed light on this: A "Study of New Technologies for Predicting Crime and its Consequences for Police Practice" is currently being prepared at the University of Hamburg. Meanwhile, the evaluation of a "Predictive Policing" project in Baden-Wurttemberg by the Max Planck Institute for Foreign and International Criminal Law in Freiburg has been completed.[42]

The roots of the problem might go deeper. It is very unlikely to assess a calculation or analysis properly as long the underlaying math function itself is not understood. The more complex and closer to kind of self-driven AI the analysis becomes the less likely it will become that even humans who created the tool (AI) are not staying in the dark about what the tool is going to learn or even process next.[43]

However, the selection and combination of the incoming information could have a discriminatory effect - even if no personal data are used. Moreover, the data could be taken out of context. The self-learning ability of modern software, commonly referred to as artificial intelligence, is likely to increase this risk. The presumption of innocence is then replaced by machine logic, as the Hamburg data protection commissioner aptly puts it.[44]

11. No Systematic Control – No Efficient Control

Obviously a profound and deliberate understanding of how data is processed and on what base answers haven been found and decisions have been made is crucial to control the tools and how they are used by human decision makers. Insofar a user or at least a regulating authority should be able to deconstruct the process and reconstruct the outcome. Otherwise no efficient disclosure of biased or erroneous data or processing criteria corrupting the outcome would be possible. It seems we do not have reached this level and may never will. Hence, public or parliamentary control of digital security regularly comes up against limits. Usually no statistics are kept on the use of software. Even data protection officers initially only check whether personal data is being processed and, if so, whether it is being used for the purpose for which it was processed.

It is also problematic that the – mostly private – producers do not disclose the source code of their software. Thus, it cannot be checked how the algorithms calculate and weight their forecasts. Those affected cannot defend themselves against a possibly falsifying classification. The German Federal and State Data Protection Commissioners are therefore right to point out that the constantly evolving technical evaluation options already show. "the potential for citizens to lose control of their data – to an extent and in a way that was unimaginable in the past". A political debate on "Predictive Policing" is therefore needed. Because once introduced, the calculation of burglaries or "endangerers" (probably dangerous individuals) can gradually be developed into an instrument of extensive social control. "By far the greatest danger of Artificial Intelligence is that people conclude too early that they understand it".[45]

12. The Presumption of Innocence – Consequences for Big Data /Algorithm-based Predictive Policing and Criminal Prosecution

The collection of data in general is problematic when the fundamental rights of (legally seen as) uninvolved parties are inevitably restricted. the name suggests – it is only through quantity that data quality is created. When collecting data, a balancing of interests is relevant to the presumption of innocence in so far as many innocent people - and suspects - suddenly find their fundamental rights curtailed, sometimes without knowing anything about it.

41 *Rosa-Luxemburg Stiftung (Bernd Belina)*, Schuldig bei Verdacht «Predictive Policing» ist diskriminierend – und ein dubioses Geschäftsmodell (Guilty on Suspicion "Predictive Policing" is Discriminatory - and a Dubious Business Model), February 2, 2017, https://www.rosalux.de/news/id/14431/schuldig-bei-verdacht.

42 www.wiso.uni-hamburg.de/fachbereich-sowi/professuren/hentschel/forschung/ predictive-policing.html; www.mpicc.de/de/forschung/forschungsarbeit/kriminologie/predictive_policing _p4.html.

43 *Flynn Coleman*, A Human Algorithm, 2019, p. XXXIII.

44 Mit der Methode Bayern gegen Wohnungseinbrecher", www.handelsblatt.com, v. 17.3.2017.

45 *Eliezer Yudkowsky*, cited by *Flynn Coleman*, A Human Algorithm, 2019, pp. XVII-XVIII.

The presumption of innocence dictates that action may only be taken if there is a concrete suspicion. In particular, the possibilities of technical surveillance involving large numbers of innocent people and surveillance without a specific objective should be criticized, although it should be proportionate to the presumption of innocence only in the case of serious offences. Otherwise the use of algorithms on big data would very likely create something like a general suspicion on everyone or even some parts of the community. This not just describes the road to discrimination according to prevalent factors but as well it tends to narrow the civic space in a specific way. As for example, it would become safe to behave in a way that does not match certain criteria the algorithm operates with. Or even better not to make extensive use of civil liberties.

Thus, the presumption of innocence will be conflicted twice - in a more specific procedural understanding but as well in a broader meaning of unsuspiciously using constitutional liberties even extensively without becoming a subject of policing and probable criminal investigation. Although these ideas are neither specifically tied to AI nor to human rights, we soon will see that the presumption of innocence is strongly connected to both. Thus, in particular when it comes to the question of legitimizing or delegitimizing the intrusion of individual rights by administrative and private entities.[46] The government must also exercise restraint in the sense of proportionality in order to protect the civil liberties of those concerned.

a) Constitutional Proportionality

Within the bigger picture, the presumption of innocence as well expresses the idea of constitutional proportionality as common in Germany, Canada and Ireland e.g.[47] Traditionally, prevention law has been based on the "concrete danger", which according to the German Federal Constitutional Court is not particularly defined in terms of its wording, but which has been sufficiently substantiated by case law over decades in a constitutional manner.

The new Bavarian state police law, for example, only requires an imminent (probable) danger. Thus, a development towards an abstract concept of hazardous situations can be seen, by which the suspicion as traditionally understood in criminal investigations is necessarily shifted forward. The interpretation is thus less clear and can potentially allow police security measures to be taken using Big Data without the police having to first search for facts that justify suspicion.

The most significant example where the police make use of Big Data to avert danger is “Predictive Policing”. An algorithm analyses the data of places or persons to find out which place or person is most likely to be affected by a crime or will commit it. It can be and is also used to solve past crimes.

In Germany, experience with “Predictive Policing” is still relatively new. In the states of Bavaria and Baden-Württemberg a system developed in the US and just slightly adjusted to local preconditions called “PRECOPS” is used to predict the location of domestic burglaries. In the state of North Rhine-Westphalia, there is a pilot project called “Skala”, which is also designed to predict other crime scenes and uses larger amounts of data. The states of Hessen and Hamburg have already passed laws that allow the use of programs from “Palantir”, some of which have already been commissioned to develop software.

In the USA, “Predictive Policing” is already an integral part of security policy. The police authorities there use much more data, such as social media data, weather data, socio-economic data, the places of residence of convicted criminals, etc., to obtain a more accurate location. In addition, dangerousness is now not only analyzed locally, but also on a personal level. For example, the Boston police department is experimenting with algorithms that monitor the social media appearances of suspects and then place or prioritize them on watch lists.

b) “Suspicion”, “Probable Cause” and “Defendant” – Blurred or Changed?

German law on policing and prevention imposes conditions on the concrete application of “Predictive Policing”: In calculating and preventing looming dangers, a computer-generated forecast is basically similar to a forecast made by a police officer. However, in security law, this requires a concrete factual situation which an algorithm cannot provide, since it only establishes an abstract risk assessment.

Similarly, in criminal law, concrete evidence is needed for someone to be considered a suspect. Forecasting decisions therefore always require a two-stage intervention by the police: the police must first look for a concrete danger, i.e. a suspicious fact, in the person or place identified by means of “Predictive Policing” before they can take action.
Conflicts with the presumption of innocence are mainly due to the measurement of the data in a statistical probability: Because under security law the police intervene before the crime is committed, a "false positive", a statistical exception that often occurs in “Predictive Policing”, is possible and currently still quite common. Thus, innocent people can become addressees of the advance police intervention without that person ever intending to commit a crime. This can lead to certain population groups being considered suspicious more often than others, particularly due to discriminatory tendencies reproduced and sometimes even intensified by Big Data.[48]

---

46 *Richard Berk*, Machine Learning Risk Assessments in Criminal Justice Settings, 2019, pp 116 ff., 128 ff.

47 *Richard Frase, Lisa Washington, Thomas O'Malley*, Proportionality of Punishment in Anglo-American and German Law, Core Issues in Criminal Law and Criminal Justice, Volume 1, ed. Kai Ambos et al., Cambridge University Press, 2020, pp. 213 ff.

48 Concerning DNA-analysis *Pfaffelhuber*, *Lipphardt* et. al just presented an empirical study on the influence of how sets of ancestry informative markers are chosen on the outcome of the algorithmic calculation.

c) Limitations due to the Binary Structure of Algorithms

Another looming problem according to *William Cullerne Bown* is that due to their binary structure adjusting algorithms on the presumption of innocence might be impossible.[49] Of course all criminal justice systems are dealing with these questions, the problem gets worse when the decision is to be made by a binary classification structure. Within a chain of binary decisions, the ultimate idea of a decision "in dubio pro reo" very much flaws. Because the yes-no structure does not allow a decision in dubio. The algorithm needs a point of decision related to a certain probability score. Binding the decision to any score obviously would miss the character of doubt. If, for example, one would take an extremely high hurdle and say beyond 90 percent the likelihood is high enough to convict, this would no decision in favor of doubt. It then becomes a simple yes-no decision. The idea of the presumption of innocence would completely fade away. Another problem with the binary structure is that the algorithm must be predicated on either guilt or innocence criteria. Either way the problem remains that the whole system would be adjusted to search for criteria and evidence to convict – or the opposite. Again, the idea of the presumption of innocence would have been failed.

However, currently the binary system is not working neither in criminal justice systems nor in "Predictive Policing" systems – as long as also the latter ones shall incorporate a presumption of innocence in a broader meaning. It may work if the basic assumption is that everybody (of the whole population or a designated group) is not just suspicious but subject of preventive investigation as long no evidence for innocence turns out. Particularly with regard to the use of Big Data tools, it would contribute to the transparency and fairness of decision-making processes if the binary structure were disclosed in as much detail as possible, thus making it clear where other types of decisions have to be taken, for example where the scope of the presumption of innocence begins. Because at this point the decision should no longer be directly justified by the results of the algorithm-driven analysis.[50]

Ignoring the presumption of innocence quite often expresses a lack of fairness against individuals or groups. According to *Russell*, the debates on fairness currently focus on the instruments. In legal contexts (harm caused by automated devices), for example, fairness determination has been based upon intent, which is nearly impossible to determine with an algorithm".[51]

V. Conclusion

In this sketch we have tried to show that the use of Big Data and algorithms in criminal proceedings, but above all in security precautions and "Predictive Policing" is an important factor that has become an integral part of reality and will become increasingly important. At the same time, the increasing use of probability prediction tools leads to overlaps in preventive and prosecutorial police work. Since criminal proceedings contain more far-reaching safeguards of individual freedom, they are in danger of changing their character more strongly if those instruments are used. If the same data pools and instruments are used in both areas, these effects will be even more significant.

More issues will be under scrutiny by coming up research. A further change is the increasing participation of private institutions following their own profit-oriented interests in security and criminal justice, rather than primarily for the common good. Therefore, legal protection is needed that is designed for this changed situation. Private stakeholders entering the playing field are the companies that design the tools and program the algorithms, but also those that (must) make available the data they collect for completely different purposes. These often have contractual relationships with the affected parties, as e. g. do social media providers. The citizen is thus no longer confronted only with the state but with a non-transparent mixture of state authority and private factual or contractual power. Due to the structure of the private stakeholders, but also due to the increasing exchange of data between national authorities, for example within the EU, many questions have an international component. If the technologies are to be used responsibly, it is therefore necessary to design a coordinated set of safeguards. Due to the international structure of this setting, human rights are the primary consideration here. These human rights, as they were formulated in the Universal Declaration of Human Rights in 1948 in the classical form, must be adapted to the living conditions in a digitalized environment. This includes addressing human rights also to private persons (companies) when they become an inseparable part of the government's power structure or act themselves as a public authority towards citizens who are in fact hierarchically subordinated.

---

49 *William Cullerne Bown*, The criminal justice system as a problem in binary classification, 2018, pp. 9,10 lexis nexis by Google Scholar Search.

50 *Richard Berk,* Machine Learning Risk Assessments in Criminal Justice Settings, 2019, p. 120: "In short, there can be a very instructive form of transparency if broad concerns are translated into precise questions that can be posed to a risk algorithm and the data on which the algorithm is trained. Trying to foster greater transparency by other means is far more difficult. At the same time, there may be important questions that cannot be answered empirically. Then one of the more difficult paths toward transparency would need to be taken. It will help enormously if stakeholders agree that the transparency provided by machine learning risk assessments only need be demonstrably better than the transparency of business as usual. Acceptable transparency simply can then be what stakeholders agree is acceptable transparency."

51 *Sam Corbett-Davies, Emma Pierson, Avi Feller, Sharad Goel, Aziz* Hug (2017) Algorithmic decision making and the cost of fairness, arXiv:1701.08230v4 {CS.CY] 10 June 2017; *Martha G. Russell and Rama Akkiraju*, Put AI in the Human Loop, 12 -2019, HICSS-Workshop-AI-and-Bias, p. 6-7.

In part, this leads to a reshaping of central rights such as privacy. In some cases, however, rights must be redesigned to ensure vital access to digital resources. In some cases, European legal systems are one step ahead of American legal practice in this respect, especially regarding to privacy and so-called IT fundamental rights. However, many human rights must also be completely rethought in order to ensure that the ideas originally associated with them continue to be valid in the digital environment.

In our opinion, newly shaped human rights are an essential element for the protection of individual freedoms and thus for the constitutional use of new technologies in security policy and criminal justice.