Ethical, legal and social challenges of Predictive Policing*

Oskar J. Gstrein**

University of Groningen, Campus Fryslân, Data Research Centre, Assistant Professor, Leeuwarden, The Netherlands

Anno Bunnik

University of Groningen, Campus Fryslân, Data Research Centre, PhD researcher, Leeuwarden, The Netherlands

Andrej J. Zwitter

University of Groningen, Dean of Campus Fryslân, Professor of Governance and Innovation, Leeuwarden, The Netherlands

---

SUMMARY

* Research for this article has been funded through the Cutting Crime Impact project (https://www.cuttingcrimeimpact.eu) sponsored by the European Union Horizon 2020 Framework (Grant Agreement number 720762).

** Corresponding author; o.j.gstrein@rug.nl.

1. Introduction

The police have always been 'information workers' (Stanier, 2016) and it comes as no surprise that law enforcement agencies (LEAs) are increasingly mobilising data for crime prevention. Historically, various systems and approaches have been developed such as the Police National Computer (Wilson, Ashton and Sharp, 2001, p. 73) in the United Kingdom (UK) in 1974. Recent developments related to digitalisation, the emergence of the Internet, mobile connectivity and advancements in computing power significantly increase the availability of information to LEAs (Bunnik *et al.*, 2016). In other words, the opportunities for 'data-driven-policing' are immense in the digital age. These capabilities are fundamentally tied to the use of 'Big Data' which can be characterised by huge volume, high velocity, diversity in variety, exhaustiveness in scope, fine-grained resolution, relational nature and flexibility (Kitchin, 2014, pp. 1, 2).

Starting in 2008 a new method of policing emerged in the United States (US) that seeks to capitalise on these opportunities. First piloted by the Los Angeles Police Department (LAPD) it soon became known as 'Predictive Policing' (PP). Originally, the idea of PP was to apply mathematical methods and insights from research on the occurrence of earthquakes to crime data in order to 'forecast crime' (Ferguson, 2017, p. 1126). Such forecasting is typically focused on places where (1) property crime (e.g., bicycle theft, domestic burglary) or (2) violent crime takes place. While PP tools typically focus on the location of future crime, there are also variants which focus on forecasting which (3) persons might be involved in criminal activity (Ferguson, 2017). The use of data analysis and statistical methods to predict the likelihood of crime quickly became popular among LEAs in the US (Querbach, 2019). Unsurprisingly, LEAs across Europe are interested in the application of this method as well. Particularly, the National Police of the Netherlands (NPN) and police forces in Germany (e.g., Lower Saxony, Baden-Württemberg, Bavaria) recently ran pilots and tested the inclusion of PP tools in their operations. It seems that most LEAs use finished solutions of corporations (e.g., PredPol, IBM, Palantir) or develop tools in cooperation with research institutes. However, some police forces also develop their own PP tools (Querbach, 2019, p. 18).

Whilst there has been lots of optimism about the potential and efficiency of PP, questions have been raised regarding its social, ethical and legal implications (Ferguson 2017; March 2019; Puente, 2019; Puente, 2019a). Many of those mirror general considerations about the ethical application of Big Data and automated individual decision-making. For example, the impact of PP on privacy and the development opportunities of individuals and groups still needs to be better understood. Additionally, propensity towards pre-existing assumptions might

be incapsulated in obscure algorithms (Zwitter, 2014). In this context, some researchers have claimed that there is a risk of public administration becoming a 'black box' (Pasquale, 2015).

This report provides an overview on key challenges as well as an empirical investigation into the use of PP in the Netherlands and Lower Saxony in Germany. We outline persistent concerns relating to the social, ethical and legal domain and call for the systematic integration of detailed substantive guidelines and effective institutional oversight processes. These measures could become part of a toolkit supporting the successful and sustainable inclusion of PP for law enforcement practices. We conclude that scholars, policymakers and practitioners ought to have clear objectives determining what PP should achieve for the work of LEAs and the safety of individuals. Developing such an advanced understanding is necessary to mitigate potential risks of the application of PP, enabling the evaluation of ongoing processes, and ultimately succeed through its use.

This submission is based on a general literature review plus the state-of-the-art report produced by the Cutting Crime Impact Project (CCI).[1] Consequently, it consists of a conceptual (section 3) and an empirical investigation (section 4). Subsequently, several salient points are identified in the ethical, legal and social domain with the intention to support the development of a holistic approach. Finally, conclusions and recommendations seek to improve the development of PP through the production of toolkits. As definition utilised here «[p]redictive policing is the collection and analysis of data about previous crimes for identification and statistical prediction of individuals or geospatial areas with an increased probability of criminal activity to help developing policing intervention and prevention strategies and tactics» (Meijer & Wessels, 2019, p. 3). Albeit with the annotation that some models have also included other types and sources of data – as the phrase 'data about previous crimes' suggests – these technologies rely exclusively on existing police data. However, the Dutch model specially includes a range of additional data sources, such as weather data or data provided by the national statistics office (Centraal Bureau Statistiek; Querbach, 2019).

2. Conceptual investigation

2.1. Why do ethics and human rights matter for Predictive Policing?

As outlined in the preamble of the Treaty on the European Union (TEU) member states are attached 'to the principles of liberty, democracy and respect for

1 https://www.cuttingcrimeimpact.eu – accessed 1 August 2019.

human rights and fundamental freedoms and of the rule of law.' Article 2 TEU sentence 1 states that the 'Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.' In addition, Article 10 TEU paragraph 1 points out that the 'functioning of the Union shall be founded on representative democracy.' Synthesizing the essence of these legal provisions in one statement, public administration (including law enforcement) in the EU and its member states is bound by the rule of law, has the objective to promote human dignity as detailed further through individual fundamental rights and freedoms, and is controlled by the people which are organised in a system of representative democracy.

This is not only relevant for the EU in the areas it has the competence to govern. Since these fundamental provisions are also a declaration of will of the parties forming the union, they can be understood as a summary of the constitutional traditions of European states where the EU does not have the competence to govern. The substantive essence of this finding is further solidified by international agreements that member states of the EU and across 'larger Europe' have signed in the same spirit, such as the European Convention of Human Rights (ECHR) or the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) of the Council of Europe (Gstrein, 2019, pp. 79-84).

While digitalisation and related technological developments create new opportunities for LEAs in preventative action through the mobilisation of vast amounts of data from a wide range of sources, the 2013 Edward Snowden revelations on global surveillance have highlighted the need for more public and political debate on the use of data in the context of law enforcement (Cannataci, 2017, pp. 17-21). As the United Nations have recognised in several resolutions on the right to privacy in the digital age, human rights apply online as much as they do offline (United Nations, 2018). However, what this means in practice remains rather unclear due to the abstract and general wording of human rights principles on the global and European level. In other words, while it is agreed that human rights are applicable to the digitalisation of law enforcement, it is unclear how they should be interpreted in detail. This is one of the main reasons why there is space for ethical deliberations to further inform the debate and actions of decision-makers. Particularly, when considering the application of innovative methods such as PP, which is based on novel technologies such as Big Data and automated decision-making, the need for a general and profound debate including ethical considerations is large.

Another important element relates to the understanding of public security and the task of LEAs in Europe. The objective of CCI is to develop toolkits for

LEAs which facilitate the fight against crime and ultimately assist in creating a safer society. Nevertheless, from an ethical, legal and social perspective and in light of what has been stated at the beginning of this section, this means that such understanding of security entails human dignity and individual freedom. Put differently, in principle a European concept of security is also an enabler of freedom, personal expression and privacy. This aspect might sometimes be overlooked and underemphasised in the day-to-day work of LEAs. It also differs from the understanding of security in other regions of the world. In countries such as the People's Republic of China the 'rule of trust' seems to replace the 'rule of law' with the digitalisation of law enforcement, manifested through the omnipresent installation of facial recognition, artificial intelligence (AI) and PP (Chen, Lin, Liu, 2018).

Furthermore, the use of data by law enforcement as well as the application of proprietary tools of third-parties frequently evokes cross-border scenarios where national regulation and territory-bound approaches face limitations. Hence, the importance of international frameworks including European and international human rights law is also stressed from this perspective. While actors such as the EU (proposal for an e-evidence package) or the US (Clarifying Lawful Overseas Use of Data Act; CLOUD) aim at addressing these gaps for investigatory purposes, most other LEA activities such as PP remain practically untouched (Cole, Quintel, 2018). In the absence of specified and detailed regulatory frameworks addressing this reality, human rights and ethics with their universal and non-territory-bound quality are put at the centre of the discourse.

Hence, it is not surprising that LEAs face increasing scrutiny about their practices in the digital domain (Bunnik, n.d.). Necessarily, PP has received significant attention from academics, media, activists and politicians in recent years. For the general public, the applicable norms governing the use of this new method seem to be a mixture of what corporations or data analysts embed in the code of the software on the one hand ('Code is Law'; Lessig, 2006), and administrative practice and expertise of LEAs on the other. Such an approach cannot satisfy the complex societal requirements and fails to build the necessary trust of a free society in the work of LEAs. Questions have been raised if PP results in the unfair targeting of minorities and ethnic or religious groups, amongst others (Ferguson 2017). Furthermore, PP invokes images of 'the Big Brother state' and Hollywood movies such as *Minority Report* from 2002 in which human behaviour is constantly monitored to prevent crime before it occurs (Bunnik, 2016; Richards, 2016).

In that sense, police intelligence moves further into the traditional domain of intelligence agencies and secret services. The wealth of data available to police the public sphere, thus, leads to a new power structure. However, differently as

one might expect, this shift not only favours the executive but also the private corporations that possess much of the used data (e.g., social media data) and produce the tools of analysis (Zwitter, 2015).

Perhaps most of all, PP is about bigger societal questions around power, governance and the relationship between the state and citizens. In the absence of detailed legal frameworks addressing these open questions, invoking ethics and human rights helps understand the (potentially) shifting power-relations between government, individuals and the communities that it seeks to protect.

2.2. Predictive Policing and the larger discussion on automated decision-making (AI, ML) in public administration

Ethical issues concerning PP are grounded in the wider context of digitalisation and related discussions on automated decision-making, surveillance and the impact of the use of such technologies on the developmental opportunities of individuals and groups. This particularly affects the right to information (transparency), freedom of expression and privacy (Cannataci, 2017a). PP does not emerge from a vacuum. Rather, it can be understood as a subsection of a global development where states and corporations mobilise Big Data to predict future human behaviour through systems based on AI and ML (Bunnik *et al.*, 2016; Gstrein, 2016; Veale, Brass, 2019). For companies like Amazon, Facebook or Google this concerns what user X or Y is likely to purchase or interested in (Zuboff, 2019). LEAs, meanwhile, are keen to predict where crime is most likely to occur (Mayer-Schönberger & Cukier, 2013). Whenever the automation of public administration occurs the main incentives are to increase the (1) quantity or (2) efficiency of one or a set of activities of a public service. This raises questions on the necessary and appropriate decisions on the macro (government strategy), meso (from policy objectives to practice) and micro level (implementing rights of a data subject, appropriate use of the system; Veale, Brass, 2019).

Despite those largely open questions, the mass-adoption of such autonomous systems seems to occur with breath-taking speed and affects all sectors of public administration. An EU focused 2019 report of the German civil society organisation 'Algorithm Watch' and Bertelsmann Stiftung finds that autonomous systems in public administration are particularly in use in the security sector (e.g., border control, PP), workforce management (e.g., job applications, management of the unemployed) or to monitor social service schemes (e.g., fraud prevention; Spielkamp, 2019, pp. 17-144). However, the popularity of such systems with policy- and decision-makers is in stark contrast to the awareness of the general population on the use of them, or the perception of usefulness of the underlying

technologies. A representative survey carried out by Bertelsmann Stiftung at approximately the same time ('What Europe knows and thinks about algorithms') highlights that only 48 percent of Europeans claim to know what an algorithm is. Only 46 percent see more advantages of the use of algorithms, while 20 percent expect predominantly problems. A full 74 percent of the total participants demand more rigorous controls and regulation on their use. Additionally, the survey also highlights that national perceptions differ. For example, respondents in Poland seem rather optimistic on the use of algorithms, while participants in France were scared to a significant degree (Grzymek, Puntschuh, 2019).

An example from the US shows what can go wrong if autonomous systems are deployed in a rushed manner and without consideration of the broader ethical, legal, and social issues. On 23 May 2016 the non-profit organisation ProPublica published an article in which it was claimed that an analytical tool in use by judges in several US states was based on an algorithm that had an inherent bias against black people (Angwin *et al*., 2016). Through data analysis the tool called COMPAS offered judges a score which should help them predict the likelihood of recidivism of inmates. Although contested by the developer of the proprietary tool, empirical investigation of ProPublica found that the system produced worse outcomes for people with non-white genetic backgrounds. According to the investigation «[…] [t]he formula was particularly likely to falsely flag black defendants as future criminals, wrongly labelling them this way at almost twice the rate as white defendants. White defendants were mislabelled as low risk more often than black defendants. […] (Angwin *et al*., 2016).» Although the findings of COMPAS are only considered to be recommendations for the judge, their existence and potential harm have caused considerable public discussion and scepticism (Israni, 2017). As more research is carried out on the appropriate implementation of forecasting systems in the criminal justice sector, it becomes clear that they need not only to work reliably according to existing fundamental legal norms and values which enable them to meet the benchmarks of current practices. While they will never be perfect, they will only succeed if they can become part of decision-making processes that qualitatively exceed an 'entirely human' system (Berk, 2019). Yet, even if this complex task will be accomplished, the larger question of how to gain societal trust is only partially addressed.

Finally, in a court of law all evidence presented needs to be accessible and verifiable by the judge and the accused. Providing results of a black box that determines over guilt, innocence, likelihood of recidivism etc., without the ability of recourse, undermines fundamental legal principles such as the equality of arms and the access to evidence by all three instances, the judge, the public prosecutor and the accused. This reduces the justice system to an inquisition-like

process in which only the algorithm and possibly the IT expert will be able to understand the processes of decision making (Martini, 2019, pp. 27-112).

2.3. Useful concepts and theories

When considering technologies with the potential to have a wide and deep impact in society, 'value-sensitive design' (VSD) and 'moral overload' are both useful concepts to mitigate risks. VSD enables engineers, developers and others that engage in creating technical solutions to integrate ethics in the design process. It centres around engaging with questions such as: how are direct and indirect stakeholders affected by the technology? What human values are under stress? (Friedman, Kahn & Borning, 2008) VSD starts from the observation that technology is a force that (partially) constitutes the social context to which it is applied, including conventions, policies, regulations and institutions – but this social context in turn also impacts on the use and design of technology. Neither human experience nor technology take centre stage. Instead the interaction should be understood as an ongoing process during which the component values can be reviewed (Friedman, Kahn & Borning, 2008). As such, it does not focus solely on the design stage of new technologies, but also on its implementation and user experience in an organisational setting.

Closely linked to VSD is the concept of moral overload. Technologies are designed to make the world a better place, such as by increasing safety and security, while at the same time respecting fundamental human rights such as privacy, promoting a liberal society, as well as supporting human autonomy and dignity. Additionally, they need to be designed in a way that enables transparency and accountability. However, technologies that advance one value can come at the expense of others – privacy versus security is often invoked on law enforcement innovation through Big Data. This moral overload frequently causes a value trade-off where – in hindsight – hard decisions have to be made regarding what is more important (van den Hoven *et al*., 2012). Making the value component of new technologies, and its impact on society, more explicit in the design phase enables a frontloading of ethics (van den Hoven, 2007). By integrating ethics and human rights already in the design process, CCI strives to avoid the trade-off scenario and rather employs a holistic approach with a security concept that integrates freedom and privacy. This report contributes to this cause by informing some of the key stakeholders on persistent social, ethical and legal issues in the early stages of the design process. The following section explores these issues in more detail and explains why they should be approached in a holistic fashion.

3. Empirical investigation

3.1. The Netherlands

The Dutch Crime Anticipation System (CAS) developed in 2013 is implemented nationally. It is interesting for various reasons. First, it was developed in-house unlike most of the systems that are purchased in the Anglo-Saxon market where companies such as IBM and PredPol are important players. Secondly, compared to the German case, it relies on a wider variety of data sources. The Dutch clearly have less hesitation to aggregate data which could be explained by cultural factors, such as German recent history with the German Democratic Republic or the *Third Reich* in which surveillance was a dominant feature of the state. Additionally, a lot of data sources in the Netherlands are already aggregated to a high degree at institutions such as the central statistics office (Centraal Bureau voor de Statistiek; CBS). Hence, they are relatively easily accessible whereas in Germany institutions at different federal levels have different competences for the collection and use of data. Thirdly, the Dutch model does not solely predict future locations of crime but also delivers predictions on humans: «In some cases, the tools also seek to identify individuals at risk of victimisation. Referred to as 'risk taxation instruments', such instruments try to predict the probability of an individual (including young offenders) committing a crime or terrorist attack» (Querbach, 2019, p. 17). This is not only a lot more innovative than predicting hotpots, it is also an ethical minefield (Marsh, 2019). As terrorism luckily is a low-probability event, the chance of both false positives and false negatives becomes a major concern (Bunnik, 2016). A related problem could occur when these approaches start predicting possible victims of crime: should LEAs or partner agencies confront those persons with such devastating news, even if there is a chance of false positives?

Finally, the Dutch system is developed to support a multi-agency approach. This particular development is in line with previous findings in the UK. Interviews with senior law enforcement officers revealed that many are hopeful that digitalisation and Big Data will lead to better sharing of information and intelligence between agencies and public bodies, leading to a wider public sector approach to law enforcement (Bunnik, n.d.). This development taking place in both the UK and Netherlands raises ethical and legal questions on the sharing of data between agencies (Crockett *et al.*, 2013). Who gets access to what and for which purposes? It also raises a more existential question on the future of law enforcement, when public bodies and partners are increasingly collaborating as part of a shared, coherent governance approach.

3.2. Germany – Lower Saxony

Since 2014 six LEAs in Germany started to develop and use externally and internally developed PP tools. These efforts produced mixed results, including promising perspectives for some tools (Querbach, 2019, pp. 12, 13). Among the LEAs working with PP, the case of Lower Saxony is particularly interesting since it developed PP first in cooperation with IBM and the Karlsruhe Institute for Technology. However, due to concerns over the sharing of crime data with private corporations and the risk that LEAs would not be capable to explain decisions based on suggestions of an externally developed system, the 'PreMap' project started in 2016. The development of the tool was facilitated by the fact that the necessary expertise to develop PP was available within the LEA.

As all German PP tools, PreMap addresses domestic burglary, which was a particular concern in the last years. The basis for the prediction is historic crime data ranging from 2008 to 2013. PreMAP calculates a score that remains valid for 72 hours and includes the area within a radius of 400 m around an observed burglary. The tool can be accessed via an application for mobile phones which allows to access forecasts made using the 'near-repeat' theory (Querbach, 2019, p. 14). This approach is based on research showing that the 'repeat victimisation theory' is a useful basis to address crime such as burglary, domestic violence, and vehicle theft (Querbach, 2019, pp. 10, 11). The main organisational response to the predictions is the reconsideration of where LEA forces should be active to prevent or fight crime. Besides predictions on where burglary might take place, PreMap also offers a 'Crime Radar'. This radar displays all offences in public spaces in the last four weeks with the possibility for agents to access additional information on demand. An evaluation of the tool came to the conclusion that it does not violate civil rights. The LEA sees lots of positive potential to inform the work of agents. However, PreMap is primarily considered as one additional tool to facilitate crime prevention and there was more need to improve the accuracy of the predictions as well as the interpretation of results by officers (Querbach, 2019, p. 15).

4. Holistic approach: ethical, legal and social concerns

4.1. Ethical

PP evokes a wide range of ethical concerns. This section addresses several of these, such as the questions of data selection and machine bias, visualisation and interpretation of forecasts, transparency and accountability, time and

effectiveness as well as the problem of stigmatisation of individuals, environments and community areas. This list is not conclusive. It provides an overview of some salient aspects that should be addressed when designing PP toolkits.

Data selection and machine bias

PP is a tool to forecast the likelihood of crime based on statistical methods and gradually evolving interpretation mechanisms. Hence, the selection of data which is the basis of the forecast is essential. If there is not enough data, irrelevant data, inaccurate data, outdated data or data which is otherwise of poor quality the final predictions will likely reflect this. Furthermore, historic crime data plays an important role in the 'training' of many PP tools, which raises the question whether the resulting automated decisions only fortify potentially inherent bias and discrimination. The question how empirical facts in the form of historic data, which might include decisions based on overcome world views, affect the findings of PP systems still requires more research. A recent review of police practices in various US cities which used PP in different scenarios over a considerable amount of time revealed how 'dirty data' can lead to bad predictions with serious societal implications (Richardson, Schultz & Crawford, 2019). Such findings, which share many aspects of the COMPAS case described above, create serious tensions and a profound lack of trust (Jones, 2019). Senior officers in the UK are also worried about poor data quality in its forces (Bunnik, n.d.).

Hence, a sound data management culture is essential and gains increasing attention (Puente, 2019). While detailed legislative frameworks might help in establishing it, as we will expand below, the term culture is of utmost importance in this regard. As initial work in CCI with police forces from across Europe suggests that the selection and use of data are often also related to what is considered as a priority in policing itself. This mostly affects the choices made in relation to crimes addressed with PP as well as the choice of historic data relating to crime. While such data is typically at the heart of the PP prediction models, another question is which additional sources (e.g., statistical data on the population, data of police forces in other parts of a country, open data such as traffic maps or weather conditions) are used to augment predictions. In this respect, even the basic constitution of a state (e.g., more centralised like in the Netherlands, more federal like in Germany) might play an implicit role, since it is either relatively easy or very cumbersome to get access to those additional sources.

Visualisation and interpretation of forecasts

Once a prediction has been made it needs to be visualised. PP can be understood as a data-driven method to 'look at' the probability of crime. As Marshall McLuhan stated in his ground-breaking work on media theory, the process

of presenting content deserves particular attention since 'the medium is the message' (McLuhan, 1962). Many PP applications such as the Criminele Antipatie System (CAS) in the Netherlands create a 'heatmap' as result of the data analysis. In other words, a certain territory is mapped and divided in quarters of a particular size (e.g., 125 x 125 metres; Mali *et al*., 2017, p. 31). Where crime is more likely to occur, individual quarters are highlighted. Already during the design process decisions need to be made regarding under which circumstances certain quarters will be marked. If too many areas demand attention, if they are marked too quickly, or if they are marked on the wrong basis (e.g., bad quality data), the tool will rather confuse than support LEAs.

However, 'grid mapping' is not the only possibility to visualise data. Other approaches focus on the precise location of crime and not so much on the covered territory. Areas where crimes are most likely are covered by ellipses which can have various shapes. Another method focuses on crime density estimations ('Kernel Density Estimation'). Here, an area with peaks and valleys is displayed, the highest points indicating where crime is most likely to occur (Perry *et al*., 2013). All of these choices fundamentally influence how LEAs use PP and understand the results of a forecast. Furthermore, the visualisation problem also has a more fundamental dimension. The design of dashboards and visualisation tools is both a scientific as well as an artistic process. The manner in which data is represented directly impacts on the actions that will be undertaken. If for example colour coding is used, colour codes will determine the urgency that will be attributed by the law enforcement officer. Since the dashboard designer usually knows little about the decision-making parameters of law enforcement officers, it is paramount that both work together in the design phase in order to ensure that information is presented in a consistent and actionable way.

Transparency and accountability

One of the key issues concerns transparency and accountability. There is a danger that the predictions become the results of a process hidden in a 'black box'. As a result, they are difficult to understand for citizens, but perhaps even for police officers, policy-makers and politicians (Spielkamp, 2019). Can LEAs still explain why they send agents to monitor a specific location or target a potential victim or offender? This aspect is closely related to the accountability of police officers and is tied to the larger discussion of the ability to explain actions based on suggestions that AI/ML-driven systems produce (Wachter, Mittelstadt, Floridi, 2017). It is crucial that PP is understood as a data-driven tool with a limited role in fighting actual crime. In other words, PP is a means to an end and not an end in itself. Furthermore, transparency and accountability are not just an issue vis-à-vis the public but also internally within LEAs. What is the relationship

between the developers of algorithms, the managers of databases and police officers on the streets and in neighbourhoods? Who is accountable to whom in such a complex system of data, technology and human agency (Meijer & Wessels, 2019, p. 7)? Finally, if LEAs use PP tools that they buy from corporations, will any data or insights remain with the state or will such private parties gain the ability to create superior insights on safety and security by pooling the data from different LEAs?

Time and effectiveness

Ultimately, data-driven PP promises a lean and effective police force – a promise that in times of austerity hardly any police agency can resist. The potential disconnect between data which underlies a certain intervention and the action that has been a result thereof jeopardizes the success of PP. In current systems, the kind of response that is recommended is usually not specified. The effectiveness of the intervention is thus only implicitly featured in the newly collected data after it took place. This can lead to skewed assessments during evaluation and the unjustified preference of certain interventions over others.

Furthermore, not only LEAs will adapt their behaviour once PP is used. Potential criminals will react to the new method as well and adjust their behaviour. Remarkably, 2008 was not only the year in which the first PP systems were tested, but also the one in which the criminal organization Lashkar-e-Taiba used data analytics in orchestrating the Mumbai terror attacks (Zwitter, 2015, p. 377). This shows that criminals are also using data analytics to improve their operations. In police circles the discourse around reverse engineering of PP or counter-PP for criminal means is increasing.

Since PP is still a relatively new phenomenon it is hard to predict in which areas and to which magnitude such effects will materialize in practice. Obvious adoptions of behaviour include differently chosen targets, modified attacks on different locations at different times, and sensing new patterns in the behaviour of LEAs over time (e.g., when there is a rain forecast on Friday night for a certain part of a city, more officers will be patrolling).

Currently, it seems practically impossible to prove the effectiveness of the use of PP (Meijer & Wessels, 2019, pp. 7-8). If the only success factor is a reduced crime rate, the available evidence-based research cannot underpin the desirability of its use. While a pilot in the Netherlands claims that the predictions are 'good enough' (the Dutch CAS was apparently able to predict around 30 percent of burglaries in Amsterdam during a pilot which was published in 2017), another study of a system in Germany (Baden-Württemberg) concludes that there is a moderate effect at best (Mali *et al*., 2017, p. 31; Gerstner, 2018). Crime as a phenomenon still seems too complex and multi-faceted to be tackled and

prevented through the use and analysis of data only. Potentially, the biggest advantage of the use of PP is not the simple reduction of crime rates. Rather, it can be a useful and innovative tool in a larger toolbox LEAs use to better understand their own work and improve their own management practices internally, which might allow them to ultimately improve safety and security (Querbach, 2019, p. 21).

Stigmatisation of individuals, environments and community areas

Individual stigmatisation can occur when, for example, for the purpose of assessment of individual likelihood of recidivism (see COMPAS), individuals are assessed and subsequently subjected to different targeted approaches by law enforcement agencies, than they would have been without that knowledge. Furthermore, stigmatisation of individuals in risk communities can also occur when data analytics suggest police interventions in certain neighbourhoods. Particularly, the popular grid-mapping visualisation which emphasises the connection between crime and territory raises the concern if the use of PP results in stigmatisation of community areas. While LEAs and the general population might already be associating certain areas of a community with more crime, the use of data could reinforce such prejudice. This 'evidence-based stigma' negatively impacts the development perspectives of individuals and communities living in such areas. Additionally, practically no legal remedies and safeguards are in place to mitigate this risk (Gstrein & Ritsema van Eck, 2018). Hence, it is not only necessary to consider which data and process is used to create the forecasts, but also how the forecasts are stored, for which period they can be retrieved, with whom they are shared, and when they are ultimately erased/destroyed.

4.2. Legal

Many of the ethical issues outlined above can be mapped out in parallel in the legal landscape. More specifically, the introduction of PP raises concerns relating to the development of individuals and groups. These concerns of increased government-led monitoring and surveillance can be tied to the debate about privacy in the digital age. However, just as PP, privacy should not be considered as an end in itself. Rather and as already indicated earlier, it is an enabling right that is closely connected to other rights such as freedom of expression, or the right to information (Cannataci, 2017a).

The Charter of Fundamental Rights of the EU (CFEU) offers a unique way to protect this right (Hoofnagle, van der Sloot & Zuiderveen Borgesius, 2019 pp. 69-72). It is not only covered in Article 7 (Respect for private and family life), but also with a second provision covering 'the protection of personal data'

in Article 8 (González Fuster, 2014, pp. 202-5). The apparent coexistence and necessity of both of these rights raises the question how they differ. Other international legal instruments such as the 1950 European Convention on Human Rights (ECHR) with its rich and developing jurisprudence on privacy do not contain a specific provision relating to digital personal data (Kochenov, Gstrein & Veraldi, 2018, pp. 24-9). Also, the United Nations Framework just relates to privacy in Article 12 of the 1948 Universal Declaration of Human Rights and Article 17 of the 1966 International Covenant on Civil and Political Rights.

It might be argued that particularly an application based on Big Data and ML such as PP proves the necessity of the added provision focusing on personal data in the CFEU. Privacy is typically seen as an individual right, focusing on the implications of arbitrary, unnecessary and disproportionate state behaviour to limit the integrity of physical personal space and deliberation. However, more recently the discussion of legal scholars has shifted towards considering the protection for groups in the context of privacy and autonomy. If individuals are tied together in groups and willingly or unwillingly made subject to data analysis and data-driven decisions, they are largely left without effective legal safeguards and remedies (Taylor, van der Sloot & Floridi, 2017). PP might affect them negatively as part of groups while at the same time only allowing them to react based on individual rights with too narrow a scope.

This gets more concrete when considering EU GDPR and the corresponding EU directive 2016/680 for automated data processing in the LEA context. Both legal frameworks contain (in Article 17 GDPR and Article 11 of the directive) a right to human review of automated individual decisions as well as an obligation for states to adopt 'appropriate safeguards for the rights and freedoms of a data subject'. However, this provision does not address how an individual, that is considered as part of a group and only subject to data processing 'in bunch', could invoke the rights enshrined in this provision. Hence, it might be appropriate to develop a right for groups to check automated individual decisions and corresponding practices of LEAs. When specifically considering PP, communities subject to increased police scrutiny could have a right to review the PP tool and data-driven LEA practices. In the absence of such a provision, the only provision in place for individuals to protect them against negative consequences of PP remains the abstract Article 8 of the CFEU, which limits the collection of raw personal data that in turn become the basis for the use of PP.

A 2017 report on 'Big Data and security policies' published in the Netherlands – which could also inform the development of PP – summarizes the substantive legal and procedural challenges in three main points. First, the establishment of a duty of care when it comes to the selection of data is recommended. Secondly, more regulation covering the creation of profiles seems advisable. Thirdly, the

possibility for judicial review is crucial to stimulate the development of case law in this area (Broeders, Schijvers & Hirsch Ballin, 2017).

Ultimately, the mere fact that police action can be based on predictions of crime prevalence, specifically when it concerns analytics regarding potential crimes of individuals can shift the focus from short-term pre-emption to prevention. Legally speaking, such an approach might effectively transform the legal concept of 'innocent until proven guilty' into '(predicted) guilty until proven innocent'. At the same time, the existence of such a crime prediction forces LEAs to respond with at least surveillance and at worst interception, de facto hollowing out the assumption of innocence. Furthermore, after the occurrence of a major crime, in light of the new PP methods journalistic and political inspections tend to focus on whether the LEAs possessed the data to forecast the crime. This can have concrete consequences on whether and how LEAs adopt PP in their routines.

4.3. Social

Both the ethical and legal domain intersect with social challenges. Hence, this perspective is used in this report as an additional lens to highlight issues of PP with particular focus on the practical impact. As PP is introduced real-world implications for citizens materialize. First, PP raises questions on trust in government, the social contract between state and citizens, democracy and the rule of law. The previously mentioned case study on the use of PP in cities in the US including Chicago and New Orleans emphasises that bad data quality can lead to the unfair targeting of specific groups and communities (Richardson, Schultz & Crawford, 2019). If there is more and predominantly negative data on certain communities which are already stigmatised as being problematic, PP might repeatedly inspect target areas where those communities predominantly live. It will be difficult to escape from such a 'feedback loop'. In this context, it could also be problematic that PP uses ML as underlying technology. At this moment in time it remains unclear whether and how ML can integrate societal goals in the gradual development of an algorithm that produces individual automated-decisions.

Secondly, and related to the first point on trust, it is necessary to emphasize and scrutinize the culture around the collection, analysis, interpretation, sharing, storage and erasure of data which is crucial to use PP for good. For example, how could a cycle of interest for LEAs look like? For how long is historical crime data relevant and under which circumstances can it be left out for future predictions? Addressing this point might be an advantage for the EU as it traditionally has relatively developed ethical and legal frameworks in this area.

The third point relates to the possibility of transparency when using PP. LEAs will require confidentiality to be able to fight crime on the one hand, while wanting to keep a good relationship with citizens and communities on the other. To find the right means and venues of engagement is crucial in order to use the arrival of this new technology as an opportunity. If applied correctly, PP can also support the decisions of LEAs and make their actions more legitimate in the eyes of the public since they are data-driven and informed by empirical methods. It is certainly true that PP systems can become 'black boxes', but human decision-making processes can also be opaque and non-transparent.

In conclusion, if ethical and legal issues are not addressed in the design of these systems and technologies their implementation can and will lead to considerable societal disruptions. If certain groups or communities are unfairly targeted, or perceive as such, the danger exists of diminishing trust in policing, and perhaps even the state in general. This is somewhat similar to discussions on CCTV or stop and search, whereby discrimination is an ongoing issue of concern (Jones, 2019). Currently, it seems that several actors have recognised these dangers. As the decisions to ban the use of facial recognition in the law enforcement context in San Francisco (California), Somerville (Massachusetts), and Oakland (California) show, the speed of digitisation in law enforcement has intentionally slowed down and the culture around the use of data could be about to improve (Conger, Fausset & Kovaleski, 2019; Lecher, 2019).

5. Conclusion

While the spur to adopt a 'technology driven crime reduction spirit' is useful, the emergence and increasing importance of data-enabled interfaces to forecast and prevent crime comes with the risk that the means are being transformed into an end. However, by engaging with the many complex questions that digitalisation brings to policing, an opportunity also emerges to re-evaluate policing tasks and processes. We suggest that this is currently the biggest advantage of the use of PP. If the culture around the collection and use of data is solid and the decision-making processes as well as their interpretation are understood by LEAs, PP can become a tool to create a better internal understanding of processes as well as more public legitimacy and trust. If the focus on the benefits for the human individual and the good for society is maintained, PP has the potential to improve the work of LEAs.

PP is becoming an established practice in Europe and particularly in the Netherlands and Germany. Furthermore, the empirical review elucidated that PP is not a one-size-fits-all approach with differences between those countries,

particularly when it comes to the selection and combination of data sources. The German context provides for more hesitation to mobilise data for preventative governance practices than the Dutch. At the same time, the comparison invites speculation whether the digitisation of the work of LEAs will not only highlight differences in the traditional understanding of their work, but also foster a more unified understanding of their future tasks and methods.

Based on the literature and empirical review we have come to the conclusion that it is necessary to address several connected ethical, legal and social issues. These are centred around the topics of data selection and machine bias, visualisation and interpretation of forecasts, transparency and accountability, time and effectiveness as well as the problem of stigmatisation of individuals, environments and community areas. We hope that this review will inform the production of toolkits that will help LEAs to mitigate risks and improve their work. Furthermore, the focus on these issues will support decision-makers to create clear and meaningful success criteria for the deployment and use of PP. The formulation of such objectives is duly needed in order to develop PP further, ensuring that it will become an innovative and effective tool in the growing toolbox of LEAs that allows them to ensure safety and security in the digital age.

6. Bibliography

Angwin, J. *et al*., 2016, "Machine Bias", ProPublica, 23 May 2016, in https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (16.05.2019).

Bunnik, A., 2016, "Countering and Understanding Terrorism, Extremism, and Radicalisation in a Big Data Age", in A. Bunnik, A. Cawley, M. Mulqueen & A. Zwitter (eds), *Big Data Challenges: Society, Security, Innovation and Ethics*, Palgrave Macmillan, London, pp. 85-96.

Bunnik, A. *et al*., 2016, "Introduction to Big Data Challenges", in A. Bunnik, A. Cawley, M. Mulqueen & A. Zwitter (eds), *Big Data Challenges: Society, Security, Innovation and Ethics*, Palgrave Macmillan, London, pp. 1-7.

Bunnik, A., n.d., *Policing the Future? Assessing the implementation of Big Data by UK Law Enforcement*, PhD Dissertation, University of Groningen.

Cannataci, J., 2017, "Report of the UN Special Rapporteur on the right to privacy to the Human Rights Council", 24 February 2017, A/HRC/34/60.

Cannataci, J., 2017a, "Games people play – unvarnished insights about privacy at the global level", in G. Vermeulen, E. Lievens (eds), *Data Protection and Privacy under Pressure – Transatlantic tensions, EU surveillance, and big data*, Antwerp, Maklu, pp. 36-41.

Chen, Yu-Jie and Lin, Ching-Fu and Liu, Han-Wei, 2018, "'Rule of Trust': The Power and Perils of China's Social Credit Megaproject", *Columbia Journal of Asian Law*, vol. 32, number 1, pp. 1-36.

Cole, M. D. and Quintel T., 2018, "Transborder Access to e-Evidence by Law Enforcement Agencies", *University of Luxembourg Law Working*, Paper No. 2018-010. Available at SSRN: https://ssrn.com/abstract=3278780 or http://dx.doi.org/10.2139/ssrn.3278780

Conger, K., Fausset R. and Kovaleski S., 2019, "San Francisco Bans Facial Recognition Technology", New York Times 14 May 2019, in https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (21.05.2019).

Crockett, R. *et al*., 2013, "Assessing the early impact of Multi Agency Safeguarding Hubs (MASH) in London. Project Report", London Councils, London.

Ferguson, A., 2017, "Policing Predictive Policing", *Washington University Law Review*, vol. 94, number 5, pp. 1109-89

Gerstner, D., 2018, "Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany", *European Journal for Security Research*, vol. 3, number 2, pp. 115-38.

González Fuster, G., 2014, "The Emergence of Personal Data Protection as a Fundamental Right of the EU", Springer International Publishing, Switzerland.

Grzymek, V., Puntschuh, M., 2019, "What Europe knows and thinks about algorithms", 1st edition 2019, in https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WhatEuropeKnowsAndThinkAboutAlgorithm.pdf (13.02.2019)

Gstrein, O. J., 2016, "How to approach technology, human rights and personality in a digital age – A few thoughts". Blog, 24 October 2016, in https://www.privacyandpersonality.org/2016/10/how-to-approach-technology-human-rights-and-personality-in-the-digital-age-a-few-thoughts/ (21.05.2019)

Gstrein, O. J., Ritsema van Eck, G.J., 2018, "Mobile devices as stigmatizing security sensors: the GDPR and a future of crowdsourced 'broken windows", *International Data Privacy Law*, vol. 8, number 1, pp. 69-85.

Gstrein, O. J., 2019, "The Council of Europe as an Actor in the Digital Age: Past Achievements, Future Perspectives", in *Festschrift der Mitarbeiter*Innen und Doktorand*Innen zum 60. Geburtstag von Univ. – Prof. Dr. Thomas Giegerich*. Available at SSRN: https://ssrn.com/abstract=3359741 or http://dx.doi.org/10.2139/ssrn.3359741

Hoofnagle, C. J., van der Sloot, B. & Zuiderveen Borgesius, F., 2019, "The European Union general data protection regulation: what it is and what it means",

Information & Communications Technology Law, vol. 28, number 1, pp. 65--98.

Israni, I. T., 2017, "When an Algorithm helps send you to prison", New York Times, 26 October 2017, in https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html (21.05.2019)

Jones, C. C., 2019, "Fearing for his life", *The Verge*, 13 March 2019, in https://www.theverge.com/2019/3/13/18253848/eric-garner-footage-ramsey-orta-police-brutality-killing-safety (21.05.2019)

Kitchin, R., 2014, "Big Data, new epistemologies and paradigm shifts", *Big Data & Society*, April–June 2014, pp. 1-12.

Kochenov, D. Gstrein, O.J., Veraldi, J., 2019, "The Naturalisation–Privacy Interface: Publication of Personal Data of New Citizens vs European Privacy Standards", *Jean Monnet Working Paper* (NYU Law School) No. 08, 2018.

Lecher, C., 2019, "Oakland city council votes to ban government use of facial recognition". *The Verge*, 17 July 2019, in https://www.theverge.com/2019/7/17/20697821/oakland-facial-recogntiion-ban-vote-government-california (17.07.2019)

Mali, B. *et al.*, 2017, "Predictive policing: lessen voor de toekomst", Politieacademie Nederland, in https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/93263.PDF (21.05.2019)

Mayer-Schönberger, V. and Cukier, K., 2013, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, New York.

Marsh, S., 2019, "Ethics committee raises alarm over 'Predictive Policing' tool", *The Guardian*, 20 April 2019, in https://www.theguardian.com/uk-news/2019/apr/20/predictive-policing-tool-could-entrench-bias-ethics-committee-warns (21.04.2019)

Martini, M., 2019, *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz*, Springer, Berlin Heidelberg.

Meijer, A. and Wessels, M., 2019, "Predictive Policing: Review of Benefits and Drawbacks", *International Journal of Public Administration,* vol. 1, number 9, pp. 1031-39.

McLuhan, M., 1962, *The Gutenberg Galaxy: The Making of Typographic Man*, University of Toronto Press, Toronto.

Querbach, M., 2019, "Review of state of the art: PP", *Cutting Crime Impact*, 30 April 2019.

Pasquale, F., 2015, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, MA.

Perry, W. L. *et al*., 2013, "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations", *RAND Corporation Safety and Justice Program*, pp. 19-33.

Puente, M., 2019, "LAPD to scrap some crime data programs after criticism", *Los Angeles Times*, 5 April 2019, in https://www.latimes.com/local/lanow/la-me-lapd-predictive-policing-big-data-20190405-story.html (25.04.2019)

Puente, M., 2019a, "LAPD pioneered predicting crime with data. Many police don't think it works", *Los Angeles Times*, 3 July 2019, in https://www.latimes.com/local/lanow/la-me-lapd-precision-policing-data-20190703-story.html (03.07.2019)

Richards, J., 2016, "Needles in haystacks: Law, capability, ethics and proportionality in Big-Data intelligence gathering", in A. Bunnik, A. Cawley, M. Mulqueen & A. Zwitter (eds), *Big Data Challenges: Society, Security, Innovation and Ethics*, Palgrave Macmillan, London, pp. 73-84.

Richardson, R. and Schultz, J. & Crawford, K., 2019, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, PP Systems, and Justice", *New York University Law Review Online*, Forthcoming.

Spielkamp, 2019, "Automating Society: Taking Stock of Automated Decision Making in the EU", AlgorithmWatch/Bertelsmann Stiftung, January 2019, in https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf (12.02.2017)

Stanier, I., 2016, "Enhancing Intelligence-Led Policing: Law Enforcement's Big Data Revolution", in A. Bunnik, A. Cawley, M. Mulqueen & A. Zwitter (eds), *Big Data Challenges: Society, Security, Innovation and Ethics*, Palgrave Macmillan, London, pp. 97-113.

Taylor, L. van der Sloot, B. & Floridi, L., 2017, "Conclusion: What do we know about group privacy?", in L. Taylor *et al*. (eds), *Group Privacy, Philosophical Studies Series 126*, Springer.

United Nations, 2018, 'The right to privacy in the Digital Age', General Assembly Resolution 14 November 2018, A/C.3/73/L.49/Rev.1.

Veale, M. and Brass, I., 2019, "Administration by Algorithm? Public Management meets Public Sector Machine Learning", in Yeung, K, Lodge, M. (eds), *Algorithmic Regulation*, Oxford University Press.

Van den Hoven, J., 2007, "ICT and value sensitive design" in *The information society: Innovation, legitimacy, ethics and democracy in honor of Professor Jacques Berleur SJ*, Springer, Boston, MA., pp. 67-72.

Van den Hoven, J., Lokhorst, G. J., & Van de Poel, I., 2012, "Engineering and the problem of moral overload", *Science and Engineering Ethics*, vol. 18, number 1, pp. 143-55.

Wachter, S., Mittelstadt, B., Floridi, L., 2017, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, vol. 7, number 2, pp. 76-99.

Wilson, D., Ashton, J., & Sharp, D., 2001, *What everyone in Britain should know about the police.* Blackstone Press, London.

Zuboff, S., 2019, "Surveillance Capitalism and the Challenge of Collective Action", *New Labor Forum*, Vol. 28, number 1, pp. 10-29.

Zwitter, A., 2014, "Big Data Ethics", *Big Data and Society*, July-December 2014, pp.1-6.

Zwitter, A., 2015, "Big Data and International Relations", *Ethics & International Affairs*, vol. 29, number 4, pp. 377-89.