Policing: A Journal of Policy and Practice, 2023, **17**, 1–9
https://doi.org/10.1093/police/paad061
Advance access publication 23 September 2023
Original Article

Big data policing: The use of big data and algorithms by the Netherlands Police

Marc Schuilenburg[*] and Melvin Soudijn[**]

[*]Professor, Erasmus University Rotterdam, Rotterdam, Netherlands. E-mail: schuilenburg@law.eur.nl
[**]The Netherlands Police/NSCR, Amsterdam, Netherlands

ABSTRACT

In recent years, the rise of big data has revolutionized many domains, including policing. Research is lacking, however, on the various ways in which the police use big data applications. This study provides new insights into the ways the Netherlands Police currently use big data and algorithmic applications. Based on a novel data source—job vacancies in the IT domain for the Netherlands Police—we distinguish three areas in which big data is used: frontline policing, criminal investigations, and intelligence. Our research shows that the use of big data by the Netherlands Police mainly involves relatively simple applications and that—in contrast to police forces in the USA—big data applications with the objective of assessing risks are the least common. The research also shows that big data policing leads to greater discretionary powers for police functions such as software developers and network designers.

INTRODUCTION

Big data policing refers to the use of large volumes of data made accessible by means of algorithms and gathered with the objective of making society safer. Various causes have been identified for the emergence and rapid growth of big data policing (e.g. Brayne, 2017; Ferguson, 2017; Fussey and Sandhu, 2022). One is the sheer volume of digital data available, which increases constantly with the daily use of the internet, social media, mobile phones, and product innovations such as consumer databases (Ridgeway, 2018; Smith and O'Malley, 2017). Second, big data policing benefits from the increasing technological possibilities for gathering, processing, and analysing such large quantities of data, as well as the expanding options for using the results in police duties (e.g. Brayne, 2021; Ferguson, 2017; Smith *et al.*, 2018). The political and societal climate is equally important. This impacts a variety of aspects, ranging from the political will to tackle certain types of crime at an ever earlier stage (Zedner, 2007) to a strong belief in technology as *the* solution for societal problems such as safety issues (Morozov, 2013).

Despite the increase in the use of big data policing and the attention it has generated in the last few years in academic research, much is unclear about its applications and effects. Scientific attention to big data policing focuses mainly on the implementation of predictive policing by police organizations and a number of associated fundamental risks, including self-fulfilling prophecies, discrimination, bureaucratization, and overpolicing minority neighbourhoods (e.g. Benjamin, 2019; Ferguson, 2017; O'Neil, 2016; Peeters and Schuilenburg, 2018). In the case of predictive policing, rule-of-law concerns are also regularly expressed, relating to the use of dirty data, function creep in terms of reusing data for other purposes than for which it was originally recorded, and violation of the presumption of innocence (e.g. Kraft, 2018; Richardson *et al.*, 2019; Schuilenburg, 2021). The use of self-learning algorithms in predictive policing tools may even lead to loss of control: the so-called black box scenario (Pasquale, 2015). This refers to situations in which decision-making processes are not only inaccessible and, as a result, unverifiable for outsiders, but also cannot be understood or explained by the users themselves. An additional issue, often mentioned in the literature on predictive policing, is that data, expertise, and intellectual property rights are relinquished if the authorities are entirely dependent on private parties for the processing and analysis of their data (McDaniel and Pease, 2021).

However, as we argue in this article, the activity of big data policing includes more than just predictive policing by police organizations. Big data policing knows a very wide range of applications used by public and private parties, from facial recognition and crowd monitoring technologies in public spaces by tech companies to the implementation of digital devices by citizens to make private homes 'smarter' (e.g. Fussey and Murray, 2019; Hill *et al.*, 2022; Pali and Schuilenburg, 2020; Sadowski *et al.*, 2021). This means that a broader picture of the phenomenon of big data policing is needed than has been given in the literature thus far. In doing so, we focus on

the following two questions: (1) Which parties in the field of safety and security use big data applications? (2) What big data applications are actually being developed and used by the police organization?

In answering these questions, this article is structured as follows. The 'Big data policing: an overview' section furnishes general background information on the phenomenon of big data policing, in which we distinguish big data policing 'by', 'above', 'below', and 'beyond' the police organization. This answers the first research question. The 'Methodology' section focuses on the method (and limitations) used to answer the second research question. In answering this question, we turn in the 'Big data applications within the Netherlands Police' section to the policing practice of the Netherlands Police, a technologically advanced police organization that is very open about its methods and use of data tools. In the 'Conclusion and discussion' section, we reflect on the results and give directions to further research into big data policing.

BIG DATA POLICING: AN OVERVIEW

Our first question focuses on which parties in the field of safety and security use big data applications. This is important because it can be argued that policing 'cannot be understood without a sense of how the quest for "big data" approaches are becoming increasingly central' (Lyon, 2015, p. 68–69). In technological terms, big data is generally explained in terms of four characteristics: volume, velocity, variety, and digital. From this angle, big data involves an enormous volume of highly varied digital data, which is gathered at a huge speed (Ridgeway, 2018)[1] The social aspect of big data deals with how it is embedded and processed within organizations. Here, matters involving 'culture' and more specifically 'work methods' play an important role (e.g. Smircich, 1983; Reiner, 1985; Van der Sloot *et al.*, 2016; Sandt *et al.*, 2021).

However, the use of big data applications to keep society safe is not the exclusive preserve of the police and other specialized government authorities. Some parties have taken over safety and security duties from the police or execute such duties in consultation with the police. To gain more insight into what parties use big data policing, we will explore the following categories: big data policing 'by' the police, parties who operate 'above', 'below', and 'beyond' the police (cf. Loader, 2000).

Big data policing 'by' the police

Working with data and predictions is not a new phenomenon in police organizations. With its roots in the 19th century and the rise of statistical studies of crime and other forms of deviant and unwanted behaviour, the emergence of big data policing within the police organization is a prime example of *longue durée*. Improving police performance by using data and statistics started in the 19th century, when data were processed by means of statistical technologies to uncover underlying patterns and differences in time and place by researchers such as Quetelet and Guerry (Beirne, 1987). The final two decades of the 20th century saw the emergence of the phenomenon of 'actuarial justice', in which techniques derived from the insurance field are used in an attempt to predict the risk of criminal behaviours (Ericson and Haggerty, 1997; Feeley and Simon, 1994; Harcourt, 2007). Ericson and Haggerty (1997, p. 36) describe police employees as 'information managers' and show how 'policing is subject to intensive "informating" (translating events and objectives into visible information via formats) and "automating" or "fordization" (machine appropriation of human skills and labour)'.

Another step towards big data policing involved developments such as intelligence-led policing, in which crime trends in certain areas are visualized so the police are better equipped to anticipate crime and disorder (Ratcliffe, 2016). Manning (2008) points to the long history of 'crime mapping' and 'crime analysis', via the city diagrams of the Chicago School in the early 20th century, to the implementation of new instruments such as Compstat ('Computer Stats', a computer program used mainly by American police departments to compile periodical statistical crime reports) to increase the speed and accuracy of obtaining data on crime development in big city neighbourhoods. The most well-known example of big data policing is probably predictive policing, which is aimed at trying to predict the chances of crime occurring in specific areas during specific time periods and subsequently using these predictions to coordinate the deployment of police surveillance teams (Hardyns and Rummens, 2017; Perry *et al.*, 2013; Ratcliffe, 2014). In addition to US-based software systems to predict property crime such as PredPol and HunchLab, similar applications are used in other countries, including Precobs in Germany, KeyCrime in Italy, Maprevelation in France, and Crime Anticipation System (CAS) in the Netherlands. The evaluations of predictive policing show varying and even contradictory results. The deployment of predictive policing proved highly effective in several cities in the USA, whereas in other countries no clear positive effects were found (e.g. Mali *et al.*, 2017; Meijer and Wessels, 2019; Mohler *et al.*, 2015; Ratcliffe *et al.*, 2021).

Big data policing 'above' the police

In recent decades, various applications in the field of big data policing have been developed as part of diverse initiatives that operate above the national level. Big data policing is used by supranational organizations, such as Europol and Eurojust (Sheptycki, 2000)[2] Europol, for instance, set up the Europol Information System, which contains data from police organizations within the European Union. Big data policing is also developed through cooperation between national governments at the international level. A current example is the Prüm system, a pan-European network established for the automated exchange of fingerprints, DNA profiles, and motor vehicle information (Neiva *et al.*, 2022). Joh (2014) mentions shared DNA databases as one of the three big data applications used in the field of policing, in addition to crime prediction and mass surveillance. Another example is the Egmont

[1]During the years, additional 'V's were added, such as 'veracity' and 'value'.

[2]Europol is a law enforcement agency of the European Union. It serves as a central hub for coordinating criminal intelligence and promotes cooperation between law enforcement agencies of the EU member states. For more information, see https://www.europol.europa.eu/about-europol (accessed 7 July 2023). Eurojust is the European Union Agency for Criminal Justice Cooperation and facilitates Joint Investigations between EU member states. For more information, see https://www.eurojust.europa.eu/about-us/what-we-do (accessed 7 July 2023).

Group of Financial Intelligence Units (FIUs), an international initiative that facilitates cooperation and intelligence sharing between the various national FIUs. In a briefing, the Egmont Group indicates that it is engaged in 'incorporating different digital tools to assist their operational efforts. These tools range from automation to the use of large datasets, big data and advanced analytics such as artificial intelligence (AI) and machine learning'.[3] Big data and AI are also important focal points in the European Union's Security Strategy (2020–25). The European Union argues that 'artificial intelligence, space capabilities, Big Data and High Performance Computing are integrated into security policy in a way which is effective both in fighting crimes and in ensuring fundamental rights'.[4] This alludes to the risks posed by terrorism, organized crime, drugs trafficking, human trafficking, and cybercrime, among other things.

Big data policing 'below' the police

In practice, civilians also use big data applications to increase safety. Examples include apps on personal phones that, when combined with sensor data of devices such as smart cameras and noise sensors, can report suspicious movements within the neighbourhood. Globally, an increasing number of civilians are monitoring their neighbourhoods in neighbourhood crime prevention groups, assisted by apps specially designed for this purpose. These digital 'do-it-yourself surveillance' groups share their information with their followers on Facebook pages or WhatsApp messages (Van Steden and Mehlbaum, 2021; Westall, 2019). Another example of big data policing below the police is luxury surveillance such as the smart doorbell developed by Amazon's daughter company Ring (Gilliard and Golombia, 2021). With this doorbell, users can see who is on their doorstep and also record footage of these persons (West, 2019). Morris claims that 'people like them because they think that crime is rising and they say it helps them feel safer in their homes and in their neighborhood' (2021, p. 241). In the USA, Ring cooperates with over 2,000 police forces, allowing civilians to share the footage recorded by the smart doorbell with the police via the Neighbours app.[5]

Big data policing 'beyond' the police

Big data policing is not the exclusive preserve of the police or other specialized authorities operating in the field of public safety and security. The rapid growth and increasing popularity of big data policing is partly due to private companies developing an increasing number of digital activities to help make society safer. Many private parties, from Amazon and Google to Tesla, apply big data policing to increase public safety, and they are bound by fewer rules than governmental authorities. Often, their products are designed for classic surveillance purposes, such as compliance and crime prevention. However, private parties may also use big data policing for other purposes, ranging from verifying a person's identity to generating profits and obtaining strategic advantages (Marx, 2016, p. 65). Commercial suppliers add big data applications to 'smart home' automation devices (Sadowski *et al.*, 2021) and private cars (Cooke, 2021; Feldstein, 2019) to signal suspicious occurrences in and around these objects. A prime example of this is the Sentry safeguard mode in the electric cars manufactured by Tesla. This mode monitors and records both the driver's driving behaviour and the car's surroundings for suspicious movements, for instance, to record potential car thieves (Eski and Schuilenburg, 2022). An important development within big data policing 'beyond' the police is tech companies selling their smart surveillance devices and updates via their platforms, in this way monitoring the behaviour of their customers. This form of 'platform policing' has 'proved highly attractive to policing agencies, as they can potentially access a wide suite of new software applications and technologies through rental contracts and can additionally tailor these to the specific needs of their agency' (Wilson, 2021, p. 51).

METHODOLOGY

As shown in the overview section, big data policing is a broad and diverse topic. In order to focus on the second research question (what big data applications are actually being developed and used by the police organization), the present study focuses on the Netherlands Police. The reason is two-fold. First of all, the Netherlands Police is a technologically advanced police force. For instance, it pioneers the targeting of encrypted communication devices and used deepfake technology to solve crimes.[6] This makes it likely that big data and data science play an important role in policing in the Netherlands. Second, compared with other countries, the Netherlands Police is very open about its methods and data (Kleemans *et al.*, 2012). It therefore stands to reason that information regarding big data policing is publicly available.

However, at the start of our research, it turned out to be difficult to obtain a clear picture of what exactly goes on within the Netherlands Police with respect to big data. It turned out that there are no extensive overviews detailing big data applications. Although numerous documents regarding big data policing are freely accessible, these documents tend to only offer prospective views or rough outlines, making it difficult to determine which of the future plans described actually came to fruition.[7]

Interviewing key players or doing 'anthropological' on-site research is another route we decided not to take. Brayne (2021), for example, created an empirical account of how big data influences police surveillance practices by interviewing key players and doing on-site observations of the Los Angeles Police Department. Although these methods can be quite informative to understand how the police use big data, there are also several drawbacks. One problem is that it is a time-consuming and costly process. To go beyond formal answers, the interviewer

[3]https://egmontgroup.org/wp-content/uploads/2022/01/Digital-Transformation-executive-summary.pdf (accessed 29 March 2023).

[4]https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 (accessed 29 March 2023).

[5]https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras (accessed 13 July 2023).

[6]https://www.vice.com/en/article/wxnve9/dutch-police-read-messages-of-exclu; https://dataconomy.com/2022/05/27/dutch-police-deepfakes-solve-crime/

[7]For example, see an official overview of ICT innovations within police portfolios https://open.overheid.nl/documenten/ronl-9acea90a-ab27-48af-b13d-9b7a32e432e2/pdf. It describes numerous innovations in broad terms, most of which are 'under development' or 'pending'.

needs to establish a rapport, something that can only be done by building up trust over a longer period. Furthermore, there is still the problem of access, and finding knowledgeable respondents who are willing to share their thoughts and views.

Rather than exploring policies, public management reports, or going the route of interviews, we chose a different approach by focussing on the Netherlands Police's online job advertisements.[8] This is the official central recruitment site for every police job vacancy. The site has varied content-related job descriptions, it provides detailed information, it is thematically grouped, and has a keyword search function. We therefore used this site to carry out a qualitative content analysis between 1 March 2021 and 1 March 2023.

We first examined all job advertisements in those domains most likely to make use of big data, that is, IT, intelligence, and criminal investigations. We scanned all vacancies in those domains in order to find out what applicants were supposed to do and collected any vacancies that were in some way related to big data. For the purpose of this exercise, we defined big data as large volumes of digital data made accessible by means of algorithms (Gartner, 2011; Laney, 2001). We did not place a bottom limit on the exact amount of information because this was never mentioned in the advertisements.

Next, any text that touched upon big data was closely read, in order to form a comprehensive picture of the kind of data involved, the skills requested, the units which were working with big data, and the kind of police activities making use of or relying on big data applications. A typical example is a job vacancy for a 'data engineer'. It opens with the following question:

> Are you the expert on ontology, data models, structures and relationships in large data sets? And would you like to contribute to the further development of the data-driven tracking of the future?

Like every other job vacancy on the police site, it continues with four specific headings. First, a more in-depth description of the job activities is found in 'What are you going to do?'. Second, the heading 'Where are you going work?' specifies the candidate's placement in the police organization and physical place of work. Third, the heading 'Who are you?' describes what skillset is expected. Fourth, 'What we offer' gives information about internal training and salary.

The content of these headings enabled us to understand the work that was to be carried out, its scope, and the relative place of big data to the overall police organization. In turn, the reading of the full job descriptions also provided us with new, relevant keywords. For instance, we found that the term 'data warehouse'—a repository of electronically stored data extracted from operational systems—was used in one specific advertisement related to a position that involved the use of big data. Subsequently, we performed a separate search of the full career website for the term 'data warehouse' to obtain as complete a picture as possible. Other keywords we used were: 'artificial intelligence'/'business analytics'/'business intelligence'/'cloud'/'data analytics'/'data lake'/'data mining'/'data science'/'deep learning'/'machine learning'/'machine teaching'/'networked data'. For these terms too, a separate search was conducted for the full research period spanning over 2 years. Ultimately, 148 job advertisements proved relevant for this study. In all of them, one or more of the abovementioned keywords were used.

Because the focus of the second research question lies on which or what kind, instead of how many big data tools are developed and used within the police organization, we did not quantify keywords or job titles. In our analysis, the keyword with the highest ranking is not necessarily the most meaningful or important (see also: Byrne, 2022). That is because the keywords or job titles only functioned as gateways to find relevant material which could give impetus for reflexive thought about our topic (Braun and Clarke, 2013; Braun *et al.*, 2018; see also: Nairn and Roebuck, 2022). Likewise, no codebook was developed beforehand because we did not want to predefine certain themes in advance. Instead, we approached the data in a reflexive manner and reread the job vacancies multiple times to become familiar with the data (Braun and Clarke, 2019). This allowed us to develop a broad conceptual framework which is presented in the next section.

Although analysing the job advertisements provided us with useful data, there are also some limitations to this method. First, we relied on publicly available data. Any job vacancy open only to internal candidates was therefore missed. Second, it is sometimes unclear if the job description matches the work the applicant will have to actually carry out. Third, our research only used one source, the police job vacancy site. Nevertheless, the advantages of analysing the job vacancy site are likely to outweigh the disadvantages. That is because we looked for a broad range of big data applications within the police organization, especially those not related to predictive policing. It was not our goal to provide a comprehensive, detailed overview of every police algorithm or big data setting, nor was it our intention to quantify data-driven activities within the Netherlands Police. Furthermore, it turns out that the job vacancies often describe work that is already carried out in different domains within the police organization which have been functioning for some time. The applicant's work is therefore likely to match the job description. Lastly, the job vacancy site is the official channel of the Netherlands Police for all vacancies. It is therefore unlikely we missed any outside recruitment efforts in complete contrast to the findings presented in the next paragraph.

BIG DATA APPLICATIONS WITHIN THE NETHERLANDS POLICE

In this paragraph, we describe on the basis of our analysis of police job vacancies what big data applications are used and in which domains (the second research question). Our findings show that in the Netherlands Police, big data is used in three domains of the organization: frontline policing, criminal investigations, and intelligence.

Frontline policing

The job vacancy site has some short explanations on different types of police work. The section about the IT domain includes a subsection on 'predictive policing'. The site explains that it is a

[8]See: www.kombijdepolitie.nl [jointhepolice].

method to try to predict the risk of crime occurring, or rules being broken, in a certain area during a certain period of time. This in turn leads to the deployment of police surveillance teams on these predictions. Predictive policing in the Netherlands makes use of a system known as the CAS. The system was developed by the Amsterdam Regional Police Unit in 2014 and, after a trial period, extended to 160 frontline teams across the Netherlands. The software draws a grid of 125 × 125 m on a city plan, and per section determines the risk of crime and disorderly behaviour occurring. This is done by making use of data from police systems, including official reports and crime figures, combined with information from Statistics Netherlands (an autonomous institution that gathers statistical information about the Netherlands) about the number of social benefits paid per area, the composition of households, etc. (Mali *et al.*, 2017; Schuilenburg, 2021).

However, during our research period, the job vacancy site is not recruiting for CAS-related activities. Furthermore, big data turns out to be used a great deal in ordinary, day-to-day policing. In these cases, it is often precisely *not* a matter of predictive models, but rather of practical applications made possible by digitalization. Consider recruitment for what are called 'DevOps [development and operations] teams' in connection with police-issued smartphones. These smartphones offer frontline police a dashboard to access various police systems. By using this platform, they can check on the spot whether a person has a history of gun violence, for instance, or can consult a permit database listing all firearms and ammunition registered for lawful use. One job advertisement gives the example of officers attending the scene of a robbery: they are able to access all emergency control room information on their phones at the push of a button, and then the location of the robbery is automatically entered into their vehicle's navigation system. Using the same phone, they scan licence plates, 'which the system directly translates into usable data'. Furthermore, they can lawfully look up information from other government authorities, for instance, to check whether a person is registered with the Netherlands FIU in connection with suspicious transactions, or whether they have unpaid fines at the Central Judicial Collection Agency.

The smartphone apps are developed and maintained by approximately 100 DevOps teams working from various locations throughout the Netherlands. In one job advertisement, a future 'Mid-level Test Specialist' for a DevOp Team is warned: 'Don't be surprised to find yourself working with big data or AI'. The successful candidate may work at any of the following departments: 'Business Operations, Business Intelligence, Connect, Law Enforcement, Criminal Investigations, Traffic and Remote Sensing, Aliens Cases, or Identity and Biometrics'. The apps run on approximately 6,000 servers. Some apps are used by a limited number of employees within the Netherlands Police, while others are available to all 50,000 police officers. An app was launched, for instance, that allows police officers to register shoplifting offences nearly entirely from their phone, and there are plans to add similar features for processing burglaries and bicycle theft. In addition to these operational policing apps, there are also business operations apps, which are of a different order. A digital police calendar, for instance, arranges operational capacity for large-scale police deployment for a planned event. All in all, a job vacancy claims that hundreds of criminal and forensic investigative apps and organizational apps have been developed. If, despite this, officers still have a need for a new app, an 'Enterprise Mobility Designer' can help them design it.

Police officers not only use search functions in apps, but also need to record their findings and activities. Again, big data is part of the solution. For this reason, the police seek to recruit a 'Junior Developer' who will assist with updating the current registration systems. The objective is to 'build a single system that combines various kinds of data, such as digital data relating to official reports, fines, sentences, and convictions'. There is also a need for a 'Backend Developer' to further develop an information system in which data can be recorded and looked up in a user-friendly way using mobile devices. This will be an 'application with a vast amount of data from a multitude of sources'. The application needs to be able to process anything from an official report on shoplifting to data from forensic investigations.

Moreover, it emerges that for some years now the Netherlands Police have been actively developing Automatic Speech Recognition software and related speech analysis tools. For this reason, the Netherlands Police is hiring a 'Senior Speech Technologist' to join the Pre-Development Department's Speech Technology Team. The job advertisement announces that conducting many tests, building prototypes, and carrying out pilot projects will make it possible in the near future to deploy speech technology—though the advertisement does not state for what exact purpose(s). Possibly what they have in mind is the emergency report system, where tools may be developed to automatically convert intake conversations to text.

Criminal investigations

Access to large quantities of data and the combining of information from various sources are not limited to frontline policing. Especially in criminal investigations, the use of big data is an important part of the work process. In Criminal Investigations Training, students are taught that working with '(big) data' will be an important aspect of their daily work. With that in mind, the Infrastructure Division is looking for a 'Data Analyst' who will help the police organization to 'work more efficiently by using big data in criminal investigations'. A team involved in financial investigations is looking for a 'Data Tactics/Social Networks Specialist' who can handle the large quantities of data generated in combating financial-economic crimes.

The use of big data in criminal investigations has various levels of complexity, ranging from simple tools to the implementation of completely new digital infrastructures needed for complex digital criminal investigations. To support regular criminal investigative duties, the Netherlands Police advertises for a 'Technical Application Administrator'. Together with colleagues, this person will be responsible for maintaining investigative applications for the benefit of the Netherlands Police as well as the Fiscal Intelligence and Investigation Service and the Netherlands Food and Consumer Product Safety Authority. Examples of the applications include templates for door-to-door inquiries, a system to verify the personal details of suspects, and a tool to map criminal money flows.

Criminal Investigation Teams are also supported by the TROI Software Development Team, TROI being an abbreviation for Operational Information Efficiency Team. This team is looking for a 'UI-UX [User Interface & User Experience] Designer' who will support regional criminal investigations teams by 'extracting

the correct information from big data', among other activities. TROI is also looking for a 'Junior and a Senior Full-Stack Developer', as the team will 'play an important role in the data-driven policing of the future'.

Various job advertisements mention that, as a result of digitalization, nearly every criminal investigation nowadays includes a digital component, and that these components are becoming increasingly important. In both small and large cases, perpetrators tend to leave digital traces. In regular criminal investigations, digital investigators usually work on gathering, combining, and analysing information obtained from open sources, internet sources, interception, and seized devices such as smartphones. The career website states, under the heading 'Data Science', that the Netherlands Police now seize so many data carriers that it is impossible to process them all by hand. Consequently, the police have devised methods to help find (unexpected) connections, such as 'text mining', 'topic extraction', 'e-discovery', and 'deep learning'. This helps to solve crimes and prevent new crimes from being committed. The High-Tech Crime Team also employs a 'Senior Digital Specialist' to 'advise and supervise the Cybercrime Teams of Regional Police Units in matters concerning data and data science'. There is even a 'Data Innovation Specialist' who develops special tools to analyse data taps and crypto currency, and to search the dark web. Since cybercrime cases may have links to investigations abroad, developers at the Netherlands Police maintain close contacts with their counterparts at foreign police services.

In criminal investigations, even the Internet of Things and home automation, for example, robot vacuum cleaners and smart doorbells, have been found to hold digital traces. For this reason, there are advertisements for a 'Junior Digital Specialist Networks & IoT [Internet of Things]' and an 'Embedded Systems Digital Specialist' to extract data from vehicles, networks, servers, and other physical objects that connect and exchange data.

Intelligence

The policing activities of both frontline and criminal investigations teams generate new data, and such data is then recorded in various systems. Without Business Intelligence (BI), it would be a time-consuming task to make all these systems easily accessible. BI refers to the collection and analysis of all kinds of relevant data to convert it into intelligence products that can contribute to criminal investigations, law enforcement, and emergency services. The police use these big data applications, for example, to estimate whether a case has a high probability of successful investigation, or to assess the best way to approach a given case. BI is applied to a nationwide police data warehouse that houses the Central Shared Information Database (BVI), a system that facilitates single-search access to data from various source registers. It 'is a database in which all police information together with information from partners and external sources is collected and adequately processed to produce structured data'. This data can subsequently be used to perform social network analyses. Therefore, one of the police units is looking for a 'Business Intelligence Operations Senior' who has 'experience with data warehousing, reporting, analytics, text and datamining, and Scrum'. For this position, the type of crime does not matter: 'whether it's cybercrime, organized crime on the dark web, hooliganism, or terrorism, each theme has its own set of questions that can be answered using a data-driven approach'.

BVI itself is made accessible through Cognos, a BI tool developed by IBM, as we can read in the job advertisement for a 'Cognos Business Intelligence Developer'. The Netherlands Police's regional units and Business Intelligence Competence Centres also use Cognos to develop intelligence products for law enforcement and criminal investigations. Various development teams, including the Digital Investigations Team, create new features within the nationwide police data warehouse. Some advertisements even mention a so-called 'Warehouse Team' that continuously engages with this data. Furthermore, continuous efforts are made to explore 'whether new sources for the dataset may be of added value'. Thanks to this intermediary between the Digital Investigations Team and the General Criminal Investigations Teams, a more effective organization is created 'by making use of big data'.

In the intelligence branch of policing, big data is an ever-recurring theme. The Rotterdam Regional Police Unit, for instance, is looking for an analyst with experience with Palantir to 'help grow the (national) intelligence position with respect to various safety and security themes'. Palantir is an application developed by a US software company of the same name that is specialized in big data analysis.

The Netherlands Police itself is also involved in innovation. A 'Full-Stack Web Developer', for example, is expected to adapt existing software as well as design new software and applications. A 'Java Developer' is needed to further develop an application 'that provides access to systems with an enormous number of data sources, thus assisting the police in very complex cases and the fight against high-impact crime'. The job advertisement explains that more links between systems and more options to make data sources accessible will allow a Data Scientist to perform a so-called 'deep dive'. All this is arranged by Team Refinery, a police IT team that can 'very quickly make data accessible from open sources, seized phones, the Automatic Number Plate Recognition system, and similar sources'. Through automation, analyses can be provided to officers and investigations in near real-time. Additionally, an 'Intelligence Specialist' can make use of an application called 'Helios', a tool developed by the Netherlands Police to make large quantities of data from various police sources accessible for intelligence purposes through one application.

Big data are also the responsibility of a 'Cloud Service Delivery Manager', whose job description includes 'providing services to the users of our big data private cloud platform'. As the job advertisement indicates, this is the best possible time to enter the organization, as the unit is in the midst of developing an 'innovative Kubernetes platform: the next step in the expansion of our big data platform', which is being added to the 'Tensorflow machine learning platform'. Kubernets is an open-source system for automating deployment, scaling, and management of containerized applications Tensorflow is an opensource software library for machine learning that is intended to result in a 'machine learning platform'.

CONCLUSION AND DISCUSSION

The emergence of big data and algorithms has significantly altered policing and, by extension, police operations. After all, big data and algorithms are ontogenetic and performative in

nature, in the sense that they bring about changes in work processes, which means that the technological possibilities offered by big data will also have an impact on the police organization and its employees. They cannot be considered a solely technological phenomenon, as their application also has social and cultural consequences for policing organizations. Just like any other tool, big data and algorithms can have both positive and negative effects depending on how they are used. Police organizations can use them in fighting crime and improving security. But they can also be used as tools to empower citizens and reduce the discriminatory effects on individuals, groups, and society as a whole (Future of Privacy Forum, 2015; Schuilenburg, 2024; Van Brakel, 2016).

It is striking, however, that the literature on the use of big data and algorithms to fight crime mainly seems to focus on forms of predictive policing, and the negative effects of these applications on citizens (e.g. Benjamin, 2019; Ferguson, 2017; Peeters and Schuilenburg, 2018; Schuilenburg, 2021). The danger of such a one-sided approach is that the concept of big data policing is narrowed down to the police as an institution and the pre-emptive logic of policing. In this way, the broader application of big data to policing is entirely overlooked. For these reasons, it is relevant to assess for which activities and processes big data applications are used and the effects they generate for the police organization. This assessment led to the following four findings.

First, we observed that big data applications in the field of safety and security were also used—in full or in part—by parties other than government authorities. Here, we distinguished parties 'above', 'below', and 'beyond' the police, though we showed that in practice the four categories may overlap. It is not only that in many cases we see joint efforts to combat urgent safety and security issues, but also that private companies may develop big data applications at the request of police organizations (or may process and analyse the data themselves), which entails potential risks such as vendor lock-in (Slobogin and Brayne, 2022; Zuboff, 2019).

Second, our study on the Netherlands Police shows that big data applications are used not only predictively, but also in real-time and retrospectively. What stands out is that big data applications with the objective of assessing risks are actually the *least* common. This finding stands in sharp contrast to Brayne's (2017) research into big data policing at the LAPD and her conclusion that 'data are used for predictive, rather than reactive or explanatory, purposes'. Furthermore, it can be concluded from our research that big data applications are widely used by the Netherlands Police. Classic frontline policing, criminal investigations, and intelligence all systematically use a large number of applications and possibilities from the field of big data. One possible explanation for the divergence between our findings and previous ones is that the situation in the Netherlands is very different from the UK or the USA. In the Netherlands, many big data applications are developed and maintained in-house by police employees, with the exception of applications like Palantir. In the USA, much is outsourced to third parties. These differences could lead to different results of big data policing in practice.

Our third conclusion relates to the nature of big data applications and the use of algorithms. The difference between rule-based and complex reasoning plays an important role in its effect on the police organization (D'Adderio, 2008). Glaser *et al.* (2021) argue that deep learning algorithms will have the largest effect on organizations, due to their lack of transparency ('black box') and their ability to generate their own objectives and rules. This is especially the case when a feedback loop emerges, so that new data generate different results or different police divisions respond differently. However, our research of big data applications used by the Netherlands Police based on openly available vacancies, shows that the fully autonomous solutions—that is, without any human intervention—are very rarely used within the organization. Our research shows that to date, the use of big data by the Netherlands Police mainly involves relatively simple applications, such as investigation apps with mainly relatively simple algorithms for frontline policing, or the connecting up of large data files to enhance access. In other words, what we see here are very weak forms of artificial intelligence.

Our fourth and final conclusion is that the deployment of big data applications leads to significant shifts in skills and positions within the police organization. Our research on the Netherlands Police shows that each police unit includes positions and development teams for programmers, coders, data scientists, cloud developers, test specialists, and backend developers. Working with big data and algorithms requires different skills and knowledge than were needed for the risk and actuarial systems used by the police in the past to analyse types of crime. In contrast to actuarial tools, the development and use of big data applications relies less on psychological and social scientific knowledge within the police organization (see also: Hannah-Moffat, 2019). It also indicates that this development leads to greater discretionary powers for certain police functions, as in the case of software developers and network designers for example. In that context, there is mention of a 'coding elite' (Burrell and Fourcade, 2021) that makes important choices in the design and development process of technology, from the datasets that serve as inputs to the algorithms that process the data. Not only is there a risk that the discretionary space of these IT experts eludes scrutiny and accountability, but also that they act without regard to their own privileged position and discriminatory practices when making decisions or performing actions based on algorithmic applications (Schuilenburg, 2024).

It is to be expected that in the future more complex and fully self-learning algorithms will be deployed for policing tasks. The literature has shown that potential risks such as algorithmic violence (e.g. discrimination and ethnic profiling) may then start to play a larger role than is the case with simple 'rule based' algorithms. After all, big data applications will become ever more complex as choices are no longer programmed completely freely, but are increasingly based on the data and experiences of the application itself. For that reason, ethical principles such as 'respect for human autonomy', 'prevention of harm', 'fairness', and 'explicability' will become increasingly important for the police organization in developing new big data applications (High-Level Expert Group on AI, 2019). For further research, it would therefore be of interest to determine whether and how police organizations around the world have succeeded in integrating such ethical values in designing new big data applications. Furthermore, future research should include the effectiveness of the big data tools used by public and private parties: to which results do they lead and at what costs?

REFERENCES

Beirne, P. (1987). 'Adolphe Quetelet and the Origins of Positivist Criminology'. American Journal of Sociology **92**(5): 1140–1169.

Benjamin, R. (2019). Race After Technology: Abolitionist Tools for the New Jim Code. Cambridge: Polity Press.

Braun, V. and Clarke, V. (2013). Successful Qualitative Research: A Practical Guide for Beginners. London: Sage.

Braun, V. and Clarke, V. (2019). 'Reflecting on Reflexive Thematic Analysis'. Qualitative Research in Sport, Exercise and Health **11**(4): 589–597.

Braun, V., Clarke, V., Terry, G., and Hayfield, N. (2018). 'Thematic Analysis'. In Liamputtong, P. (ed), Handbook of Research Methods in Health and Social Sciences, Singapore: Springer, pp. 843–860.

Brayne, S. (2017). 'Big Data Surveillance: "The Case of Policing"'. American Sociological Review **82**(5): 977–1008.

Brayne, S. (2021). Predict and Surveil. Data, Discretion, and the Future of Policing. Oxford: Oxford University Press.

Burrell, J. and Fourcade, M. (2021). 'The Society of Algorithms'. Annual Review of Sociology **47**(1): 213–237.

Byrne, D. (2022). 'A Worked Example of Braun and Clarke's Approach to Reflexive Thematic Analysis'. Quality & Quantity **56**(3): 1391–1412.

Cooke, P. (2021). 'Three Disruptive Models of New Spatial Planning: "Attention", "Surveillance" or "Sustainable" Capitalisms? Journal of Open Innovation: Technology, Market, and Complexity **7**(46): 46–20.

D'Adderio, L. (2008). 'The Performativity of Routines: Theorising the Influence of Artefacts and Distributed Agencies on Routines Dynamics'. Research Policy **37**(5): 769–789.

Ericson, R. V. and Haggerty, K. (1997). Policing the Risk Society. Toronto: University of Toronto Press.

Eski, Y. and Schuilenburg, M. (2022). 'On Tesla: Balancing Sustainable Car Connectivity, Silent Lethality and Luxury Surveillance'. Criminological Encounters **5**(1): 234–251.

Feeley, M. and Simon, J. (1994). 'Actuarial Justice. The Emerging New Criminal Law'. In Nelken, D. (ed), The Futures of Criminology. London: Sage, pp. 173–201.

Feldstein, S. (2019). The Global Expansion of AI Surveillance (vol. **17**). Washington, DC: Carnegie Endowment for International Peace.

Ferguson, A. G. (2017). The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement. New York: NUY-Press.

Fussey, P. and Murray, D. (2019). Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. Colchester: Human Rights Centre, University of Essex.

Fussey, P. and Sandhu, A. (2022). 'Surveillance Arbitration in the Era of Digital Policing'. Theoretical Criminology **26**(1): 3–22.

Future of Privacy Forum. (2015). *Big Data: A Tool for Fighting Discrimination and Empowering Groups*. https://fpf.org/wp-content/uploads/2014/09/Big-Data-A-Tool-for-Fighting-Discrimination-and-Empowering-Groups-FINAL1.pdf (accessed 4 August 2023).

Gartner. (2011). *Gartner Says Solving 'Big Data' Challenge Involves More than Just Managing Volumes of Data*. www.businesswire.com/news/home/20110627005655/en/Gartner-Says-Solving-Big-Data-Challenge-Involves-More-Than-Just-Managing-Volumes-of-Data (accessed 7 July 2023).

Gilliard, C. and Golombia, D. (6 July 2021). 'Luxury Surveillance: People Pay a Premium for Tracking Technologies that Get Imposed Unwillingly on Others'. Real Life Magazine.

Glaser, V. L., Pollock, N., and D'Adderio, L. (2021). 'The Biography of an Algorithm: Performing Algorithmic Technologies in Organizations'. Organization Theory **2**(2): 263178772110046. doi:10.1177/26317877211004609.

Hannah-Moffat, K. (2019). 'Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates'. Theoretical Criminology **23**(4): 453–470.

Harcourt, B. E. (2007). Against Prediction: Profiling, Policing and Punishing in an Actuarial Age. Chicago: Chicago University Press.

Hardyns, W. and Rummens, A. (2017). 'Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges'. European Journal on Criminal Policy and Research **24**(0): 201–218.

High-Level Expert Group on AI. (2019). Ethics Guidelines for Trustworthy AI. Brussels: European Commission.

Hill, D., O'Connor, C. D., and Slane, A. (2022). 'Police Use of Facial Recognition Technology: The Potential for Engaging the Public through Co-constructed Policy-Making'. International Journal of Police Science & Management **24**(3): 325–335.

Joh, E. (2014). 'Policing by Numbers: Big Data and the Fourth Amendment'. Washington Law Review **89**(1): 35–68.

Kleemans, E. R., Soudijn, M. R. J., and Weenink, A. W. (2012). 'Organized Crime, Situational Crime Prevention and Routine Activity Theory'. Trends in Organized Crime **15**(2–3): 87–92.

Kraft, O. (2018). Sharpening the Money-laundering Risk Picture: How Data Analytics Can Support Financial Intelligence, Supervision and Enforcement. London: Royal United Services Institute for Defence and Security Studies (RUSI).

Laney, D. (2001). '3D Data Management: Controlling Data Volume, Velocity and Variety'. META Group Research Note, 1, file 949.

Loader, I. (2000). 'Plural Policing and Democratic Governance'. Social and Legal Studies **9**(3): 323–345.

Lyon, D. (2015). Surveillance After Snowden. New York: Polity Press.

Mali, B., Bronkhorst-Giesen, C., and Den Hengst, M. (2017). Predictive Policing: Lessen voor de toekomst. Een evaluatie van de landelijke pilot. Apeldoorn: Politieacademie.

Manning, P. (2008). The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control. New York & London: NYU-Press.

Marx, G. (2016). Windows into the Soul, Surveillance and Society in an Age of High Technology. Chicago: University of Chicago Press.

McDaniel, J. and Pease, K. (2021). Predictive Policing and Artificial Intelligence. New York: Routledge.

Meijer, A. and Wessels, M. (2019). 'Predictive Policing; Review of Benefits and Drawbacks.' International Journal of Public Administration **42**(12): 1031–1039.

Mohler, G. O., Short, M. B., Malinowski, S. *et al.* (2015). 'Randomized Controlled Field Trials of Predictive Policing'. Journal of the American Statistical Association **110**(512): 1399–1411.

Morozov, E. (2013). To Save Everything, Click Here. New York: Public Affairs Books.

Morris, J. (2021). 'Surveillance by Amazon: The Warrant Requirement, Tech Exceptionalism, & Ring Security'. Boston University Journal of Science & Technology Law **27**(1): 237–269.

Nairn, A. and Roebuck, R. (2022). 'Promoting the police: A thematic analysis of the New Zealand Police recruitment campaigns and the construction of officers' identities.' Journal of Criminology **55**(2): 221–238.

Neiva, L., Rafaela, G., and Machado, H. (2022). 'Big Data Applied to Criminal Investigations: Expectations of Professionals of Police Cooperation in the European Union'. Policing and Society **32**(10): 1167–1179. doi:10.1080/10439463.2022.2029433.

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. London: Penguin Books.

Pali, B. and Schuilenburg, M. (2020). 'Fear and Fantasy in the Smart City'. Critical Criminology: An International Journal **4**(28): 775–788.

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms that Control Money and Information. Boston: Harvard University Press.

Peeters, R. and Schuilenburg, M. (2018). 'Machine Justice: Governing Security through the Bureaucracy of Algorithms'. Information Polity **23**(3): 267–280.

Perry, W. L., McInnis, B., Price, C. C. *et al.* (2013). Predictive Policing, the Role of Crime Forecasting in Law Enforcement Operations. Santa Monica: RAND Corporation.

Ratcliffe, J. (2014). 'What is the Future of… Predictive Policing?'. Translational Criminology **6**(0): 4–5.

Ratcliffe, J. (2016). Intelligence Led Policing. London: Routledge.

Ratcliffe, J. H., Taylor, R. B., Askey, A. P. *et al.* (2021). 'The Philadelphia Predictive Policing Experiment'. Journal of Experimental Criminology **17**(1): 15–41.
Reiner, R. (1985). The Politics of the Police, Brighton: Wheatsheaf Books.
Richardson, R., Schultz, J., and Crawford, K. (2019). 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice'. New York University Law Review Online **94**(192): 192–233.
Ridgeway, G. (2018). 'Policing in the Era of Big Data'. Annual Review of Criminology **1**(1): 401–419.
Sadowski, J., Strengers, Y., and Kennedy, J. (2021). 'More Work for Big Mother: Revaluing Care and Control in Smart Homes'. Economy and Space **0**(0): 1–16. doi:10.1177/0308518X211022366.
Sandt, E., Van Bunningen, A., Van Lenthe, J., and Fokker, J. (2021). 'Towards Data Scientific Investigations: A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest'. White Paper Presented at the Third INTERPOL-UNICRI Global Meeting on AI for Law Enforcement, REPHRAIN.
Schuilenburg, M. (2021). Hysteria: Crime, Media, and Politics. London/New York: Routledge.
Schuilenburg, M. (2024). Making Surveillance Public: Why You Should Be More Woke About AI and Algorithms, The Hague: Eleven.
Sheptycki, J. W. E. (ed) (2000). Issues in Transnational Policing. London & New York: Routledge.
Slobogin, C. and Brayne, S. (2022). 'Surveillance Technologies and Constitutional Law'. Annual Review of Criminology **6**(0): 1–22.
Smircich, L. (1983). 'Concepts of Culture and Organizational Analysis'. Administrative Science Quarterly **28**(3): 339–385.
Smith, G. J. D., Moses, L. B., and Chan, J. (2018). 'The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach'. The British Journal of Criminology **57**(2): 259–274.
Smith, G. J. D. and O'Malley, P. (2017). 'Driving Politics: Data-driven Governance and Resistance'. British Journal of Criminology **57**(2): 275–298.
Van Brakel, R. (2016). 'Pre-emptive Big Data Surveillance and Its (dis) Empowering Consequences: The Case of Predictive Policing'. In van der Sloot, B., Broeders, D., and Schrijvers, E. (eds), Exploring the Boundaries of Big Data, Amsterdam: AUP, pp. 117–141.
Van der Sloot, B., Broeders, D., and Schrijvers, E. (eds). (2016). Exploring the Boundaries of Big Data. Amsterdam: Amsterdam University Press.
Van Steden, R. and Mehlbaum, S. (2021). 'Do-it-Yourself Surveillance: The Practices and Effects of WhatsApp Neighbourhood Crime Prevention Groups'. Crime, Media, Culture **18**(4): 543–560. doi: 10.1177/17416590211041017.
West, E. (2019). 'Amazon: Surveillance as a Service'. Surveillance & Society **17**(1/2): 27–33.
Westall, J. (2019). *Volunteer Street Patrols: An Ethnographic Study of Three Manchester Volunteer Street Patrols and their Role in Community Safety and the Policing Family*. Ph.D. Thesis. Manchester: Manchester Metropolitan University.
Wilson, D. (2021). 'The New Platform Policing'. In Završnik, A. and Badalic, V. (eds), Automating Crime Prevention, Surveillance, and Military Operations. Cham: Springer, pp. 47–68.
Zedner, L. (2007). 'Pre-crime and Post-criminology?'. Theoretical Criminology **11**(2): 261–281.
Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs.