



The role of data-driven policing in tackling high-risk criminal networks in the Netherlands

Wendy Schreurs, Jessica Cozzi, Jurjen Jansen

<https://doi.org/10.3013/m5f6q668>

Abstract

Communication is central to organised crime, and offenders increasingly rely on encrypted phones to exchange sensitive information while avoiding detection. Although encryption is crucial for safeguarding fundamental rights and the digital safety of citizens, governments, businesses and society, it also restricts the ability of law enforcement and judicial authorities to exercise their legal powers, as criminals exploit secure communication services for illicit purposes. In the context of high-risk criminal networks (HRCNs), however, encrypted communication can become a valuable data source once law enforcement gains lawful access. Decrypted datasets have enabled the Dutch police, in collaboration with international partners, to make arrests, seize substantial quantities of drugs and gain insight into criminal processes. As HRCNs continue to adapt their communication methods, the police must also anticipate this evolving digital landscape. One approach is to combine multiple data sources – such as automatic number plate recognition, open-source intelligence, video footage and confiscated digital devices – to create a more comprehensive operational picture. In response, the Dutch police launched the national programme ‘data-driven collaboration’ to strengthen their ability to collect, store, analyse and operationalise diverse forms of data. This paper discusses the future of data-driven policing in tackling HRCNs, based on interviews with strategic key players within the Dutch police.

Keywords: data-driven policing, encryption, technology, organisation, human aspects, criminal networks.

Introduction

In the digital age, rapid technological advancement has transformed various aspects of society, including organised crime. Criminal networks depend heavily on communication, and offenders increasingly rely on encrypted phones to exchange sensitive information while avoiding detection by law enforcement. Although encryption is vital for

protecting fundamental rights and digital safety, it simultaneously limits the ability of law enforcement agencies (LEAs) to exercise their legal powers, as criminals exploit secure communication services for illicit activities.

High-risk criminal networks (HRCNs) pose significant social and economic threats, and the ability to access and analyse large volumes of criminal communication has proven crucial for law enforcement (European Union Agency for Law Enforcement Cooperation, 2024a). Recent investigations into encrypted platforms such as EncroChat, Sky ECC and ANOM have enabled the Dutch police, in collaboration with international partners, to make arrests, seize large quantities of drugs and gain insight into criminal processes. Yet HRCNs are adaptive and continuously modify their communication strategies to evade detection, resulting in an ongoing cycle of innovation and countermeasures.

At the same time, the increasing digitalisation of society provides new opportunities for law enforcement, leading to the growing adoption of data-driven policing (DDP). Building on intelligence-led policing, DDP seeks to use all available and relevant data to enhance preventive, investigative and operational outcomes (Barros et al., 2024; Barros, 2022). Implementing DDP, however, introduces a range of technological, organisational, human and ethical challenges. The use of algorithms and artificial intelligence (AI) raises questions about transparency, accountability and the conditions under which data analysis may guide decision-making.

This study aims to address the following central research question: to what extent do technological, human, organisational and ethical aspects influence the effectiveness of DDP in tackling HRCNs within the Dutch National Police?

Theoretical background

The use of data in tackling high-risk criminal networks

The global rise of digitalisation has increased the use of data and encrypted communication tools. The prevalence of data and encryption across crimes has grown for two reasons. Encryption is widely embedded in both software and hardware, making it easily available to criminals. Second, it enables criminals to conceal crucial information and communications, which significantly aids criminal activity. As a result, LEAs are increasingly facing data and encryption challenges in their investigations. Research on the role of encryption in the Dutch criminal justice chain showed that encryption is common in all types of crime, but to a fairly large extent more so in high impact crime and plays a significant role in all types of organised crime (Jansen et al., 2023). This prevalence underlines the relevance of focusing on HRCNs in this study.

Encryption can both obstruct and enhance criminal investigations. It limits direct access to evidence, making it harder to identify relevant individuals or activities. However, even when the encrypted code cannot be cracked, alternative methods, such as the use of metadata, can still provide valuable evidence. Decrypting data, when successful, can significantly accelerate investigations and reveal crucial insights, such as *modus operandi* and criminal collaborations.

Despite its challenges, encryption also offers practical benefits for LEAs, such as providing reliable and unaltered evidence, which is often considered more trustworthy than witness statements. The study by Jansen et al. (2023) suggests that while encryption complicates criminal investigations, law enforcement continues to adapt and

develop new methods to overcome these obstacles. As technology evolves, ongoing investment in skills and knowledge related to encryption and digital tools is crucial. Although the impact of encryption is difficult to quantify, it shapes both the opportunities and challenges LEAs face in modern investigations.

When data are decrypted, LEAs gain access to a potential goldmine of information and intelligence. Within the Dutch National Police, crypto analysis teams (CATs) were established to analyse these large datasets. This development has been a catalyst for the adoption of DDP within the Dutch police.

Data-driven policing

DDP is part of a broader big data revolution across sectors such as healthcare, finance, transportation and criminal justice (Davis et al., 2022). While definitions vary, most describe DDP with a focus on its use, purpose and impact on law enforcement. Afzal and Panagiotopoulos (2024) explain that DDP uses tools such as data analysis, surveillance, predictive algorithms and public information to make police work more efficient and accurate. It combines different types of data, such as neighbourhood history, criminal profiles and crime records. Examples include the Real-Time Analysis Critical Response Division in Los Angeles and the Domain Awareness System in New York (Afzal and Pangiotopoulos, 2024). Jansen (2018, p. 2) employs a more preventive definition, illustrating how policing has transitioned from reacting to crimes after they happen, to preventing them proactively, thanks to data and new technology.

The emphasis of DDP is on using the insights, clues, connections and patterns obtained from data to guide police work in the form of detection, enforcement and emergency aid (den Hengst and Wijsman, 2023). Within the Dutch police, initiatives such as the operational information yield teams have developed tools to automatically process and analyse large datasets (i.e. big data) (Roest, 2023). Big data systems are characterised as follows: ‘they make use of vast quantities of data from a variety of data sources, and, using rapid computer processing and algorithms, identify correlations or patterns in the data, often patterns that humans would otherwise overlook, in order to classify new instances in the domain of interest’ (Davis et al., 2022).

In 2023, the Dutch police launched a national programme called ‘data-driven collaboration’ (*Datagedreven Samen Werken*) aimed at facilitating data-driven operations across organisational levels. The police possess numerous internal and external data sources, such as automatic number plate recognition (ANPR), sound and motion sensors, video footage, and open-source intelligence (OSINT). It is anticipated that both the sources and the amount of data will continue to increase in the future (Dutch National Police, 2023).

Police (business) models in a digital police organisation

With the rise of intelligence-led policing, the intelligence cycle has been utilised by LEAs to systematically process intelligence analyses and criminal investigations.

Intelligence-led policing

The intelligence cycle (United States Department of Defense: Joint Chiefs of Staff, 2013) is an internationally accepted model used to describe intelligence work, which is also utilised by the Dutch police, as shown in Figure 12.1 (den Hengst and Wijsman, 2023). At the centre of the intelligence cycle is the joint operational mission. This outlines the

goal to which the intelligence should contribute, namely the decision-maker's intention. The model consists of six steps: (1) direction and planning, (2) collection, (3) data processing, (4) analysis, (5) dissemination and (6) continuous evaluation of both the process and the content. The impact that the decision-maker has by choosing an intervention based on intelligence is not reflected in this model. Additionally, the model lacks specific guidance for dealing with big data.

DDP is not seen as an entirely new approach, but rather as an enhancement of intelligence-led policing as data and their interpretation have become more widely accessible (Barros et al., 2024).



Figure 12.1. Intelligence cycle used by the Dutch police

The CSAE (collect, store, analyse, engage) model

To address the limitation of traditional intelligence cycles in a big data environment, particularly in the domain of cyber-facilitated crime, the CSAE model (Figure 12.2) was established (van de Sandt et al., 2021). This model provides a multilayered framework that integrates diverse investigative disciplines into a single coherent approach.



Figure 12.2. The stages of the CSAE model

The foundation of this model lies in the social and behavioural aspects of what we now refer to as traditional investigations, such as investigative interviews and physical surveillance. The second layer incorporates the technical perspective of digital investigations, which emerged in the 1980s. More recently, a numerical dimension incorporating advanced mathematical and statistical methods has been introduced into law enforcement practices. The synthesis of these three layers – social and behavioural, technical and numerical – constitutes data scientific investigations. This approach allows LEAs to identify complex patterns within HRCNs that would otherwise remain undetected by traditional methods alone (van de Sandt et al., 2021).

The primary objective of criminal investigations is to identify suspects and establish who did what to facilitate prosecution. LEAs hold a monopoly on this process of bringing suspects to justice. Before the digital age, all criminal investigations were what we now call traditional, offline investigations and forensics. These investigations primarily focused on the human aspects of crime, making them largely social and behavioural in nature. Investigators relied on techniques such as observations, investigative interviews and eavesdropping to uncover the truth, often supported by traditional forensic sciences like ballistics, DNA analysis, fingerprinting and pathology, which dealt with physical evidence from the offline world (van de Sandt et al., 2021).

As crimes became increasingly intertwined with and facilitated by information technologies, evidence began to shift to hardware and online environments, leading to the emergence of digital investigations. Digital forensics, involving computers, networks, mobile devices, etc., was developed to recover evidence from data storage devices. While digital investigations provided an additional layer to traditional investigative methods, their introduction marked a fundamental shift in the legal, organisational and technical dynamics of the justice system. The integration of traditional and digital investigations has been an ongoing process for many LEAs worldwide (van de Sandt et al., 2021). By integrating the CSAE model and the intelligence cycle, a new business model for data-driven policing was created (Figure 12.3) (den Hengst and Wijsman, 2023). In this model, the joint operational assignment is still central, but more attention is paid to the underlying business process and the need for multidisciplinary collaboration between, among others, AI experts, domain experts and intelligence analysts. Additionally, it includes the evaluation phase from the intelligence cycle. This business model acknowledges both the role of the decision-maker and the complexity of intelligence work when dealing with large amounts of data (den Hengst and Wijsman, 2023).

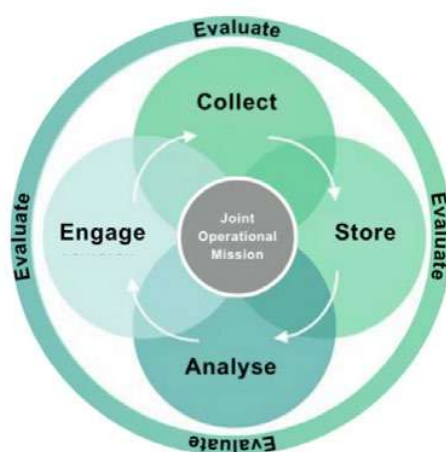


Figure 12.3. Business model for data-driven policing

In DDP, it is important to recognise that analysing big data with data science methods can reveal new patterns and trends that were previously invisible. However, it does not provide insight into the underlying reasons for these patterns (van der Zwet et al., 2022). In addition, the term 'big data' can give an unjustified sense of confidence in the completeness of the data (Dunietz, 2016). There are numerous examples where significant gaps in the data have been overlooked and/or the data are biased, for example, survey data and social media data (Bradley et al., 2021; Hargittai, 2020; Hargittai, 2015). The secrecy of criminal activities also results in a portion of crime remaining unseen and unregistered (i.e. dark number) (Barros et al., 2024).

Technology, human, organisational and ethical aspects

A well-known aspect of digital policing is its reliance on technology. However, technological, human, organisational and ethical aspects are equally important in the adoption of DDP. All four aspects are elaborated on in the next sections.

Technological aspects

DDP encompasses a broad range of technologies. Real-time identification technologies, for example, have transformed modern policing by making it possible to instantly identify people and objects. Tools such as ANPR, automated facial recognition and voice identification systems collect data in public areas without needing consent. Unlike traditional methods such as fingerprinting or DNA analysis, these systems allow live tracking and identification by comparing data with existing databases (Jansen et al., 2018).

Human aspects

A crucial aspect of DDP is the combination of both data-driven insights and human experience in decision-making. Officers often rely on their judgement and experience, sometimes overriding or modifying algorithmic suggestions to maintain their professional discretion. Officers heavily rely on their experience, which can sometimes clash with data-driven insights. For DDP to work well, officers need to combine their expertise with the data to recognise criminal patterns effectively (Buscariolli, 2023).

Challenges arise when tensions occur between data analysts and police officers, as officers tend to trust their own experience more than the data, which can hinder teamwork. For DDP to be effective, proper training and resources are needed, because officers and analysts sometimes lack the necessary skills or up-to-date knowledge (Afzal and Panagiotopoulos, 2024). Effective leadership is key to encouraging the use of data in policing. Leaders who inspire and involve others in their decisions can foster a culture of progress, while unclear objectives and poor management can hinder the successful adoption of data-driven strategies (Afzal and Panagiotopoulos, 2024).

Organisational aspects

On an organisational level, DDP changes the structure of how information and knowledge is exchanged (Marciniak, 2021). Policy and implementation do not always coincide. Data-driven policing has found its way into a network organisation, often alongside the traditional organisation (Dutch National Police, 2023). To what extent DDP is effectively implemented significantly depends on the resources and structure of police organisations. Having the right tools and properly trained staff is key to success. Smaller police departments often struggle with limited budgets, outdated technology and insufficient training. In contrast, larger organisations with more funding can

afford modern equipment, skilled data analysts and better training programmes. Furthermore, since HRCNs operate as network structures and quickly adapt to external factors (such as interventions by LEAs or other criminal networks), it is crucial for LEAs to also function as network organisations. They must be flexible in working with a diverse range of employees with various areas and levels of expertise (Schreurs and Martens, 2021).

Ethical aspects

The use of data-driven technologies in policing has made operations more efficient, improved decision-making and helped allocate resources better. However, these benefits come with ethical and privacy concerns, especially regarding the potential worsening of existing biases and harm to civil liberties. One major issue is the reliance on biased historical crime data, which often targets minority groups unfairly. For example, algorithms using factors like zip codes or minor offences can lead to over-policing in marginalised areas (Afzal and Panagiotopoulos, 2024). Predictive policing tools, despite being labelled as objective, risk creating cycles where biases are repeated and strengthened.

Real-time surveillance tools, like facial recognition and social media monitoring, add to privacy concerns. These technologies can undermine the presumption of innocence by flagging people based solely on their behaviour rather than solid, comprehensive evidence (Williams and Kind, 2019). Another challenge is the lack of transparency in machine learning systems, often called 'black box' algorithms. Policing tools created by private companies (like Palantir and PredPol), are protected by trade secrets, which make it hard for the public to hold them accountable (Afzal and Panagiotopoulos, 2024). These tools are also complicated, making it difficult for law enforcement officers to critically analyse their results. Hence, the ethical concerns of DDP go beyond technical problems and impact society.

Methodology

Study design

This study employed a mixed-methods qualitative design, combining desk research with empirical qualitative research to explore key perspectives within the Dutch police. In-depth interviews were conducted to gather rich, contextual data from key players involved in DDP. A semi-structured interview format was chosen to allow for flexibility while ensuring consistency across interviews. This approach was chosen to bridge the gap between theoretical frameworks and operational reality.

Participants

A total of 13 key players within the Dutch police organisation were selected by purposive sampling. These participants were identified based on their roles, expertise and involvement in DDP. As the Dutch police is a relatively small organisation, specific key players in the field of DDP-adoption are easily identifiable in a system search. In addition, interviewees were also asked for relevant key players within their networks and potential new interview subjects. The sample included a diverse range of individuals, such as project managers on DDP, legal advisors within the police organisation and employees of the national DDP programme, ensuring a comprehensive view of the organisation's structure regarding DDP.

To capture shared organisational insights, some sessions were conducted as group interviews; in total, nine interviews were held with the thirteen participants.

Data collection

The interviews took place between August and December 2024, either in person or virtually. Each interview lasted between 45 and 90 minutes. The interview focused on exploring the role of DDP in the Dutch National Police. The interview protocol was designed with a set of open-ended questions to explore the participants' views regarding the benefits, barriers and future developments of DDP across four primary dimensions: technological, human, organisational and ethical. The interview also addressed international collaboration, scientific research needs and any blind spots in current police practices related to DDP.

Interviews were audio-recorded with participants' consent and transcribed verbatim for subsequent analysis.

Data analysis

The transcribed interviews were analysed using thematic analysis to identify recurring patterns, themes and insights. To increase interrater reliability, the initial coding of one interview was performed independently by two researchers, after which the codes were compared and refined through an iterative process. Subsequently, the researchers each coded half of the remaining interviews. All data were anonymised to maintain participant confidentiality. The coding scheme can be found in Appendix 12.1. Quotes reported from the interviews were translated from Dutch to English, ensuring the preservation of the participants' original content.

Ethical considerations

The study adhered to standard ethical guidelines and all participants provided informed consent prior to their involvement. Participants were assured of their anonymity and the confidentiality of their responses, and they were given the option to withdraw from the study at any stage without any repercussions.

Results

This section presents a comprehensive analysis of the interviews, structured around the five key themes: defining DDP, and its technological, human, organisational and ethical dimensions, supplemented by additional relevant aspects.

Defining data-driven policing

Respondents offered diverse definitions of DDP but agreed that it is not a new concept. As one noted: 'We have always gathered information, from the moment we were a police force. And we register it all very carefully. However, nowadays we shove everything into specific bookcases and drawers, of which we have forgotten that they even exist.' Another respondent indicated that DDP is almost the same as intelligence-led policing, the only difference being the increased involvement of technology and big data, as it is difficult to ignore the impact of algorithms and AI in extracting valuable information from the data.

Despite the implication of the term 'data-driven', respondents emphasised that the data alone cannot lead decision-making in police practice. Current data systems cannot adequately account for contextual factors and risks, making

exclusive reliance on data undesirable. Some respondents differentiated between 'data-driven work', meaning the systematic analysis of existing data before an investigation, and 'working with data', which refers to combining data sources in the CSAE model. However, a consistent distinction did not clearly emerge. One respondent highlighted the importance of making critical choices about what data to specifically collect and how to use them. Others described data as 'the new weapon of the police'. The comparison being that as a baton or pepper spray are current weapons of the police, digital operations and interventions could be the weapons of the future, requiring similar levels of training, authorisation and evaluation before use.

Type of crime

Respondents generally agreed that DDP is applicable across a wide range of offences, particularly highlighting HRCNs and serious crime, and is useful across all phases of investigation, including prevention, detection and strategic intelligence.

Crimes with a clear start and finish, like robbery or homicide, may require different data-driven analytical approaches than ongoing, open-ended crimes, like drug trafficking networks (e.g. crime scripting, social network analysis). Several respondents remarked that focused questions (e.g. 'Who did it?') tend to feel more concrete and satisfying than open-ended intelligence questions (e.g. 'Who else is involved in a criminal network?').

Technological aspects

Views on technological development varied. One respondent claimed that technological advancements are almost already at their peak, and that the speed of developments will likely slow down. However, others see a future of increasing and continuing technological developments. For the police, technology is primarily about accessing new data sources, connecting systems and supporting analysis. A technical barrier mentioned by a respondent is the outdated ICT infrastructure, which limits the ability to share seized data and accommodate growing computational needs.

With new tools such as dashboards and large language models (e.g. ChatGPT), data are becoming more easily accessible to a larger proportion of employees. However, this carries the risks that employees without proper training and education regarding the use and risks of data tools may trust the results of these tools and adopt them as facts more easily than others.

Data quality, or data hygiene, was cited as a significant risk. Police reports, registrations and existing databases form the base of DDP, but the quality of the output is determined by the quality of the data, reinforcing the 'garbage in, garbage out' principle, as some respondents mentioned. Every person working with data within the police force should have a basic understanding and level of awareness that even a small registrational error could have big effects. For example, multiple respondents noted that once people are registered in police systems, whether they are involved, suspected or convicted, they will be more prone to police scrutiny and thus keep 'reappearing' in police systems. In addition, other respondents mentioned the limited data storage capacity of the police, and how the police must be more critical of what data to gather, what data to keep, and more importantly, what data to permanently delete and when.

Another technological development is the rise of misinformation, which has become a constant cat-and-mouse game between those who create and spread it digitally and those developing technologies to detect and counter it. One respondent mentioned: 'That was, for example, the case with deep fakes, where people made deep fake detectors, but those [deep fake detectors] were then used to improve the deep fakes. This can also be very dangerous.' The risks are that these technological advancements also enhance the expertise of criminals. Another respondent feared how the police will be able to deal with data (e.g. pictures, images, videos) that are automatically generated by a citizen or suspect. Questions arise as to whether the police can detect them as fake, how these data will be interpreted and to what extent it is illegal to provide this 'false' information to the police.

Due to the ever-growing and overwhelming amount of information and data that are involved in police work nowadays, respondents agree that it has become impossible for humans to analyse them all by themselves. Additionally, respondents mentioned the current personnel and capacity shortage within the Dutch police organisation, stressing the critical need for efficient data management. Respondents speculated that, through AI, large amounts of data could be analysed to identify which data points should be further examined by humans. It is repeatedly emphasised that a human should still provide the interpretation of the data to avoid making incorrect decisions.

Human aspects

Mindset

In recent years, with the increase of the amount and the importance of data, the necessity for change has become unavoidable. According to one respondent's personal experience, organisational change only occurs when there is both a sense of urgency and necessity on a strategic level. For years, this respondent experienced that, at first, there was no perceived need to change or improve work processes: 'I think that the insights generated by the crypto communication data have led to the realization that we, as an organisation, need to take action and ... anticipate what is coming'. Additionally, respondents noted that pressure from the media and societal discourse were also seen as significant factors of organisational change.

Although the sampled respondents are enthusiastic about DDP and mentioned many different, local DDP initiatives, at the same time, the sense of success and satisfaction among colleagues differs. The traditional police mindset is described as being focused on 'catching kilos, cash and crooks' and less on effect-based interventions or the prevention of crime. The latter being less tangible. As an example, a respondent mentioned that a lot of information can be collected and endlessly analysed in a criminal investigation about a HRCN, but this is not perceived as a success by the detectives if no criminal has been arrested.

Respondents note that a part of the Dutch police culture revolves around people and data being compartmentalised, which hinders people from thinking beyond their own domain. This is improving according to the respondents, partly because colleagues are collaborating more and, as they work in different teams throughout their careers, they learn to understand each other's expertise better (with the CATs as a leading example). One respondent mentioned that, while the Dutch police want to work more flexibly as an organisation, employees quickly interpret that as the dissolution of existing teams. People like having stability and feeling connected to a team. A respondent described that, on an operational level, the organisation is currently not designed for flexibility. The example was

given that, when determining when an intervention should take place, intelligence is sometimes not the leading factor, but whether there is enough staff available at that moment.

An often-mentioned aspect of the DDP mindset is how police personnel should be very critical about the use of data in their investigations. As mentioned earlier, DDP-practitioners believe that, with so many data available, a shift in mindset is needed to focus on asking the right questions: what data and information do we really need for this investigation? What are we going to do with the data we collected? Some respondents used the example of smartphones to illustrate this. The average smartphone contains about 128 to 256 gigabytes of data. In a stalking case, would all the data on that phone be necessary? Or just the phone logs, messaging apps and recent photos? Respondents call for both a shift in mindset and proper internal checks and balances in this age of DDP.

Multiple respondents argue that other areas of police work, such as emergency services, are also valuable as information and data sensors. Respondents also commented on the mindset of street patrolling officers, who want to catch criminals, but do not see themselves as part of the 'intelligence organisation'. However, when these colleagues are motivated to gather information, and accurately register data in police systems, their input can be a valuable additional source and yield significant results.

Lastly, respondents noted how people like to remain critical as the 'human-in-the-loop'. At all levels – strategic, tactical and operational – people are perceived to be sceptical about sharing data: 'Should I share this?', 'Why would I share my data with you?'. The most reported value in operations is still: 'Then I'll lose my case!'. This leads to reluctance in sharing information.

Skills and expertise

To operate in a data-driven manner, officers need to be skilled enough to handle large amounts of data and specific tooling. One respondent discussed that colleagues often know how to investigate 'the traditional way', through tapping phones, surveillance and other labour-intensive manners but, as mentioned before, investigators are less likely to think about what data are already available in the systems, and what data are still needed to solve a case. Hence, multiple respondents argue that analytical and critical thinking skills are increasingly important for detectives and intelligence analysts.

The respondents agree that a human is always needed as the 'man in the middle' between technology and operations, with the focus on human qualities like integrity and empathy. In addition, according to the respondents, more experts, such as data scientists, legal advisors and ethicists, are needed. As the data are still too unreliable, and technology and algorithms are not (yet) sufficiently reliable, the police organisation will need to maintain human control in the near future.

In conclusion, current employees will need to be trained to work effectively with both data and people, and expert skills will need to be brought in. As one respondent put it: 'it should soon become a basic rule that criminal investigators need to know a certain amount of tooling. They do not need to be an expert in everything, but DDP will become a standard way of working'.

Organisational aspects

Structure

As mentioned earlier, a topic that often came up in the interviews is that teams need to remain flexible for DDP to work. As one respondent described: 'As an organisation, we are still really at the foot of a high mountain, the organisation is sluggish and change is slow'. Multiple respondents argue that, to become a data-driven organisation, the organisation needs to be able to respond to rapid changes. To keep up with developments in society, and therefore also in crime, it is important to make effective choices regarding the organisational structure.

Most of the respondents mentioned the 'golden triangle', where intelligence departments, criminal investigation and 'specialist criminal investigation' – which entails specific expertise such as forensics or digital expertise – work together. As this has increased, for example in the CATs, the value of this multidisciplinary collaboration has proven itself and led to success stories. Currently, this collaboration does come with its hardships as, for example, intelligence analysts and investigators within the same team report to different supervisors who do not always share the same operational or strategic goals. A suggestion made by two respondents is to have thematic multidisciplinary teams at both the operational and strategic levels with a single supervisor, where, at the strategic level, disciplines can remain separate. These thematic teams can also assist in making the transition from the 'analyse' phase to the 'engage' phase (see Figure 12.3), as both employees work closely together in the same team.

As the Dutch police is a national police organisation with ten regional and two national units, the collaboration between these units is also discussed. Respondents argue that the regional units are structured similarly; however, in practice they still experience large differences between the units. One respondent mentions the increasing role of the two national units in the acquisition and distribution of knowledge and experience.

Human resources

When discussing the organisational needs for DDP, human resources issues were discussed on two levels: regional cases and organisation-wide cases. On a regional level, respondents repeated their views on strong, local leadership and the consequences for DDP implementation. Leaders with a clear vision and means to act on that vision are allowed to combine and even hire personnel to create multidisciplinary teams. These teams seem to thrive, but are threatened by overall personnel shortages and shifting priorities, and often are not sustainable. Respondents call for a flexible human resources policy that would allow leaders to create their own teams according to their needs, and to be able to keep these people on for as long as necessary, and for organisational flexibility, in the sense that the organisation can foster successful teams and change their structure, rather than ending them prematurely.

On a national scale, respondents foremostly mentioned the structural personnel shortage within the Dutch police, regardless of DDP implementation. Generally speaking, although there are regional differences, despite all the data that are available, there is a shortage of (data) analysts who can work with (big) data to generate actionable outcomes. In addition, even when such analysts are available and do generate results, there is a shortage of personnel who can act on those results.

In addition to the general personnel shortage, respondents describe how diversity in personnel and multidisciplinary teams are essential for DDP. Different backgrounds, specifically data sciences or OSINT skills, are mentioned as being important. However, respondents acknowledge that these often highly specialised people are scarce, and the Dutch police organisation must compete with corporate companies and other services. It is urged to challenge these highly sought individuals to work together with the police and build a resilient organisation.

Leadership

The role of management and leadership was brought up by the respondents in almost every interview. Several respondents reported that they noticed how individual team leaders determine the success of DDP integration. They agree that if a strong-willed leader has a clear vision of how DDP should be implemented, and he or she is given the space and means to express that vision in, for example, personnel changes and priority shifting, DDP is better adopted in the workplace. However, because this implementation is largely reliant on the efforts of individual leaders, respondents also noted that there are large differences between regional units.

As mentioned earlier, DDP activities, such as big data intelligence analysis, might not generate immediate tangible results. It was noted that police success is traditionally defined more by quantifiable results, like the amount of drugs or money seized, or the number arrests made. This apparent delay in traditional, tangible results might lead to feelings of dissatisfaction and frustration among personnel. It was noted that leaders should be able to defend their DDP vision and implementation to both their superiors and their team.

When asked about the role of strategic management and the national data-driven cooperation programme, respondents noted how the programme started off with a strong vocal presence and vision of what DDP should look like in the Dutch National Police. Several regional units were selected for pilots. Respondents observed that if their unit was not selected as one of the pilot units, their involvement in the national programme gradually diminished. Several respondents shared the thought that, to successfully implement DDP, strategic management should not only rely on the top-down flow of vision and practice but should also work together with (all) regional units to create a shared understanding of DDP implementation. Another respondent added that a new paradigm is needed, because thinking in terms of 'bottom-up' and 'top-down' traps you in a mindset of duality.

Education

Several respondents addressed the desire for more formal education regarding DDP. Regional units often organise local educational activities, ranging from a workshop day to their own educational courses. Respondents praise these initiatives but warn that knowledge gained and lessons learned in these courses should be more properly integrated into police education, as they seem to lack professional checks and guidance. Respondents agree that police educational institutions, like the Dutch Police Academy, should be involved in developing and providing such education.

Some respondents noted that new personnel seem to differ from 'regular' police personnel in terms of education and knowledge needs. For example, a data scientist might have sufficient knowledge of data and tooling but might lack domain-specific police knowledge. On the other hand, police personnel might be experts in their field or domain but could lack basic knowledge of data and data analyses to properly understand and interpret results. As mentioned under 'Skills and expertise', respondents call for a basic understanding of the uses and risks of data.

However, it is yet to be determined what this basic, general understanding of domain, data and tooling knowledge should consist of.

Ethical aspects

Only a few respondents mentioned the ethical aspects of DDP. Hence, the following results are mainly from one interview with an ethics expert. The respondent argues that organisations have generally transitioned from a functional structure to process optimisation, and eventually to a customer-centric approach. Now, the respondent argued, data are seen as the starting point. In DDP, the respondent described ethics as ‘the current biggest challenge’. The recently experienced ‘techno-optimism’ in organisations ensures that new technologies are used enthusiastically without thoroughly considering the consequences.

Respondents advocated for early ethical considerations via structured methods such as the guidance ethics approach. For the police, the tension between AI and ethics is even more relevant because of budget, time and workforce shortfalls, and the ongoing search for more efficient working methods. According to this respondent, even though police officers must make ethical decisions daily, there is a need for more awareness and professional governance. The expectation is that the impact of AI will only increase in the coming decades. Fundamental values will not change, but the rapid technological development requires continuous monitoring and adjustment to maintain a balance between people and technology. Aspects such as surveillance, privacy and democracy will become increasingly urgent. Data awareness requires analysis of processes, practices and possible biases. These considerations should be made at a strategic level, with input from both internal (police) and external experts. Although ethics and sustainability are considered important, concrete actions are often lacking.

Additional aspects

Several interviews touched upon additional aspects affecting DDP, for instance, societal involvement and legal developments. A few respondents noted how the Dutch society has yet to debate to what extent they value their fundamental rights of freedom and privacy over police authority and security. Both the Dutch and the European political climate, along with increasing societal polarisation, are expected to play a role in this debate and to shift the balance toward more freedom and less security in the near future.

Some respondents share the view that the current Dutch legal framework is not yet up to date with technological developments and their implications for police work. New technologies or data sources, such as civilian cameras (i.e. smart doorbell), could have a major impact on criminal investigations. However, the current legal framework (despite the approval of the EU AI Act) is not yet adapted to such technological advancements and is either ambiguous or reserved about the adoption of technological advancements in police work. According to the respondents, this leads to misunderstanding and frustration for both police personnel and civilians. Dutch criminal law is currently under major supervision, but respondents agree that the rate of legislation and jurisprudence development is too slow and already behind current technological developments.

Some respondents call for levels of authority or control of data and corresponding, proportional authorisation rights. Respondents believe the examining magistrate (*rechter-commissaris*) might play a role in this data authorisation in the future.

Discussion and conclusion

The rapid digitalisation of society has fundamentally altered the operating environment of LEAs. In particular, the widespread use of encrypted communication by criminals, especially within HRCNs, has generated unprecedented volumes of data, as criminals need communication to organise their business. This has led to the concept of DDP. This study combined desk research and interviews to gain better insight into the role and the current status of DDP in the Dutch police with regard to HRCNs. The use of data, algorithms and AI in policing raises technological, human, organisational and ethical challenges that must be addressed to develop an effective strategy against crime.

The current state of data-driven policing in the Netherlands

Recent research and respondents from the current study provide varied interpretations of what DDP entails, and there is no clear definition provided by the Dutch police. There is general agreement that DDP is not a new concept, but rather an evolution of intelligence-led policing, distinguished by the scale, complexity and speed of the data available through digitalisation and encryption. Within DDP, there is need for multidisciplinary collaboration between, among others, AI experts, domain experts and intelligence analysts. Therefore, we propose that a clear definition of what DDP entails should be introduced within the Dutch police organisation. In this way, the organisation can align expectations and create collaborative goals. It also enables them to work in a universal manner and systematically learn from it. By discussing learning points with different teams, the DDP approach can also be continuously improved throughout the whole organisation.

While encryption enables criminals to conceal their activities, it simultaneously produces highly structured datasets once law enforcement gains lawful access. Respondents emphasised that these datasets offer substantial investigative value but also introduce new risks. Data extracted from encrypted communication require interpretation, contextualisation and critical assessment, as automated systems cannot adequately account for investigative, legal and ethical nuances. This reinforces the central finding that DDP cannot be reduced to algorithmic decision-making: human judgement remains essential throughout the intelligence and investigative cycle, including with regard to prevention and detection. Operational practice should therefore formally embed 'human-in-the-loop' principles at all stages of data-driven investigations, ensuring that analytical outputs from encrypted data are validated, contextualised and authorised by trained personnel before operational action is taken.

The emergence of the CATs has been a catalyst for DDP within the Dutch police. The successes and barriers these teams have experienced increased their awareness of the potential, necessity and risks of the use of big data, algorithms and AI by the police. Additionally, since the start of the national programme of data-driven policing, it has become a key strategic issue in the police organisation. Change in the organisation has also been driven by the increasing volume of data and external pressures, partly from media and society. The realisation that action is necessary, spurred by insights from crypto communication data, has created an urgent need to adapt work processes. As technological advancements continue, new opportunities and threats will emerge (e.g. quantum computing (European Union Agency for Law Enforcement Cooperation, 2024b)), which LEAs will have to anticipate and prepare for.

Aspects and challenges

Technological advancements in policing are progressing at different rates, with some respondents noting slowdowns while others anticipate continued growth. The Dutch police face challenges such as outdated ICT systems and insufficient server capacity, hindering data accessibility and the full transition to DDP. New tools like dashboards and large language models (e.g. ChatGPT) have become widely available to many employees, but this could increase the risk of people unconsciously relying on unreliable data without having received proper training and with a lack of internal authorisation systems. Respondents call for a basic understanding of the uses and risks of data. The increased volume of data and the rise of misinformation, such as deepfakes, further complicates the situation, as these advancements also enhance criminal expertise.

The overwhelming amount of data available requires a shift in mindset, with a focus on asking the right questions about what additional data are necessary alongside the already comprehensive databases. The data quality and importance of correct registration in police systems ('garbage in, is garbage out') needs more attention. Ethical and legal considerations must guide data collection and their timely removal, but this awareness is not yet sufficiently present among employees working with data. There is a need to foster a mindset where information gathering is seen as a part of the broader police effort, not just the intelligence community. While technology and data sharing are crucial, there is reluctance among staff, which is often driven by the fear of losing control. A flexible authorisation model could be of assistance in structurally storing and sharing data, with a foreseen increased role for the examining magistrate.

Trust in data tooling and the outcomes of algorithms still impedes efforts to fully integrate DDP on all levels. This barrier is two-sided: on the one hand, police staff need to be aware of the shortcomings of data, presence of biases and lack of transparency of algorithms. Although all these data seem to be a gold mine, we argue that a critical mindset is needed to assess whether we are dealing with actual gold or 'gilded gold'. As LEAs will have to deal with deepfakes, misinformation and manipulation and the challenges they pose to data integrity and decision-making, we recommend that LEAs introduce an additional, manual approach in tooling to assess how reliable systems and algorithms are. Discussions need to be held on an organisational – and societal – level as to what degree of system (un)reliability to accept. A 95 % or even a 99 % accurate system will still generate mistakes. On the other hand, staff need to trust the outcomes of data enough to be willing to make data-based decisions and reduce human workload. This delicate balance can be achieved through awareness, training and experience over time.

Results showed that the integration of DDP within the Dutch police requires significant attention to organisational structure, leadership, and human resources to effectively leverage data analytics in operational contexts. One key aspect emerging from the interviews is the need for organisational flexibility to adapt to the demands of a data-driven, highly valued multidisciplinary approach. Respondents emphasised that, to respond to rapid societal and criminal developments, the organisation must adjust its structure to ensure efficient use of capacity and expertise. Data-driven decision-making necessitates the breakdown of silos between different disciplines. However, challenges persist, like aligning leadership goals across teams, as individual supervisors often set different operational or strategic objectives for analysts and investigators. An organisational mindset shift is needed to create a more adaptable workforce that can respond to changing demands.

Leadership plays a critical role in the success of DDP integration, with respondents noting that individual leaders' visions for DDP significantly influence the implementation process. Clear leadership with the ability to allocate resources and manage personnel changes has been shown to foster more successful DDP adoption, although discrepancies between regional units remain. We argue that a national collaborative approach is essential for the success of data-driven initiatives, as regional units, particularly those not involved in pilot projects, reported feeling sidelined as the national programme progressed. In the future, it would be beneficial to keep all regional units in the loop of current experiments and developments.

On the human resources front, a structural shortage of personnel, particularly data analysts with the necessary skills to handle big data, was noted as a significant barrier to effective DDP implementation. Despite the availability of data, there is an insufficient number of analysts who can transform it into actionable intelligence, and even when such individuals are available, a lack of personnel to act on these insights further limits effectiveness. However, they acknowledged that attracting such highly specialised individuals is a challenge due to competition from the private sector and other governmental organisations. To address these shortages, it was suggested that the police organisation must adopt strategies to attract and retain these professionals, fostering a resilient workforce capable of navigating the complex demands of DDP.

The current Dutch legal framework is not yet up to date with technological developments. Modern technologies or data sources could have a beneficial impact on criminal investigations, but the legal framework needs to be adapted to such technological advancements. Dutch criminal law is currently under major supervision, but respondents agree that the rate of legislation and jurisprudence development is too slow and already behind on current technological developments. With new legislation, such as Dutch law and the EU AI Act, education on these changes is necessary.

The police face significant tension between AI and ethics due to limited resources, unclear legal guidelines and the ongoing search for more efficient methods. In the interviews, ethical topics did not come up very easily. Police officers must make ethical decisions daily, but there is a need for greater awareness and professional governance to ensure that these ethical standards also apply in DDP contexts. The growing impact of big data and AI require ongoing monitoring and adjustment. Issues like surveillance, privacy and democratic values will become more pressing, making data awareness essential among police officers at all levels. Hence, we argue for increasing ethical awareness, for example, by including an ethical advisor in a flexible team or by establishing a compliance officer or an ethical (data) committee.

Data-driven policing also sparks a societal debate about the extent to which the public values their fundamental rights of freedom and privacy over police authority and security. The Dutch, but also European, political climate and societal polarisation are expected to play a role in this debate, and the outcome of this delicate balance will likely affect police legitimacy in the future.

In conclusion, this study highlights both the potential and the challenges of DDP within the Dutch police, particularly in the context of HRCNs. While DDP offers promising opportunities for addressing HRCNs, significant obstacles remain. Its success depends on the integration of technology, human judgement, organisational design, ethical governance and legal clarity. Operationally, this requires a clear and consistent definition of DDP, and greater

organisational flexibility and leadership. There is an urgent need for better training, collaboration and ethical awareness to ensure that data-driven approaches are used responsibly and effectively. Moving forward, LEAs should foster an adaptable, well-resourced and ethically conscious workforce to navigate the complexities of modern policing in an increasingly digital world. Future research and policy development should focus on bridging gaps in data reliability, improving education on DDP, conducting empirical evaluations of its effectiveness, adapting legal frameworks and strengthening human resources development to optimise the potential of DDP in combating crime while safeguarding civil liberties.

Acknowledgments

We would like to thank Femke van 't Hoff for her assistance in the literature review.

Artificial intelligence statement

During the drafting process, AI tools such as Copilot were used only for language improvement. All intellectual contributions, analysis and literature synthesis were made by the authors. The final manuscript reflects the authors' academic interpretation and critical evaluation of the reviewed studies.

References

- Afzal, M. and Panagiotopoulos, P. (2024), 'Data in policing: An integrative review', *International Journal of Public Administration*, Vol. 28, Issue 7, pp. 411–430, <https://doi.org/10.1080/01900692.2024.2360586>.
- Barros, A. I. (2022), *De Kracht van Intelligence: Bezint eer ge moet bijsturen*, Politieacademie, Apeldoorn, <https://mediatheek.politieacademie.nl/pdf/102452.PDF>.
- Barros, A. I., Doleman, R. and Schreurs, W. (2024), 'Intelligence', in: Kop, N., Muller, E. R. and van der Torre, E. J. (eds), *Politie – Organisatie en functioneren van de politie in Nederland*, Wolters Kluwer, Deventer, pp. 395–416.
- Bradley, V. C., Kuriwaki, S., Isakov, M., Sejdinovic, D., Meng, X.-L. et al. (2021), 'Unrepresentative big surveys significantly overestimated US vaccine uptake', *Nature*, Vol. 600, pp. 695–700, <https://doi.org/10.1038/s41586-021-04198-4>.
- Buscariolli, A. (2023), 'Making crime visible in the digital age: The ethnomethods of data policing', *Critical Criminology*, Vol. 31, No 2, pp. 545–562, <https://doi.org/10.1007/s10612-023-09683-y>.
- Davis, J., Purves, D., Gilbert, J. and Sturm, S. (2022), 'Five ethical challenges facing data-driven policing', *AI and Ethics*, Vol. 2, pp. 185–198, <https://doi.org/10.1007/s43681-021-00105-9>.
- Den Hengst, M. and Wijsman, O. (2023), 'Datagedreven politiewerk – Een organisatorisch en juridisch perspectief', in: Snaphaan, T., Hardyns, W., Van Dijk, A., Spithoven, R. and van Brakel, R. (eds), *Big Data Policing*, Vol. 1, No 66, Gompel en Svacina, pp. 71–90, <https://nscr.nl/app/uploads/2023/02/2023-den-Hengst-Wijsman-Datagedreven-politie-accepted.pdf>.

Dunietz, J. (2016), 'How big data creates false confidence', *Nautilus*, 22 April, <https://nautilus.us/how-big-data-creates-false-confidence-235908>.

Dutch National Police (2023), *Landelijk programmaplan – Magazine Datagedreven Samen Werken*.

European Union Agency for Law Enforcement Cooperation (2024a), *Decoding the EU's Most Threatening Criminal Networks*, Publications Office of the European Union, Luxembourg, <https://data.europa.eu/doi/10.2813/811566>.

European Union Agency for Law Enforcement Cooperation (2024b), *The Second Quantum Revolution – The impact of quantum computing and quantum technologies on law enforcement*, Publications Office of the European Union, Luxembourg, <https://data.europa.eu/doi/10.2813/42230>.

Hargittai, E. (2015), 'Is bigger always better? Potential biases of big data derived from social network sites', *The ANNALS of the American Academy of Political and Social Science*, Vol. 659, Issue 1, pp. 63–76, <https://doi.org/10.1177/0002716215570866>.

Hargittai, E. (2020), 'Potential biases in big data: Omitted voices on social media', *Social Science Computer Review*, Vol. 38, Issue 1, pp. 10–24, <https://doi.org/10.1177/0894439318788322>.

Jansen, F. (2018), 'Data driven policing in the context of Europe', Data Justice Lab, 7 May, <https://datajusticeproject.net/wp-content/uploads/2019/05/Report-Data-Driven-Policing-EU.pdf>.

Jansen, J., Westers, S., Schreurs, W., Berkenpas, M., Alpár, G. et al. (2023), *De Rol van Encryptie in de Opsporing: Belemmeringen en mogelijkheden*, NHL Stenden Hogeschool: Cybersafety Research Group, <https://open.overheid.nl/documenten/ronl-d497ea5bebe949b3cde930209d87e131413e6b09/pdf>.

Marciniak, D. (2021), 'Data-driven policing: How digital technologies transform the practice and governance of policing', University of Essex: Department of Sociology, [https://repository.essex.ac.uk/30103/1/Data-driven%20policing%20-%20how%20digital%20technologies%20transform%20the%20practice%20and%20governance%20of%20policing%20\(Daniel%20Marciniak\).pdf](https://repository.essex.ac.uk/30103/1/Data-driven%20policing%20-%20how%20digital%20technologies%20transform%20the%20practice%20and%20governance%20of%20policing%20(Daniel%20Marciniak).pdf).

Ministry of Justice and Security (2019), *Datagedreven Werken – Wat is er voor nodig?*, <https://open.overheid.nl/documenten/ronl-7cdd61bf-c43c-4cf8-a054-86dfe1a49951/pdf>.

Roest, D. (2023), 'Big data en politiewerk, een onoverbrugbare kloof? Hoe TROI de brug slaat van big data naar politiewerk', in: Snaphaan, T., Hardyns, W., Van Dijk, A., Spithoven, R. and van Brakel, R. (eds), *Big Data Policing*, Vol. 1, No 66, Gompel en Svacina, pp. 91–106.

Schreurs, W. and Martens, P. (2021), 'De politie als anticiperende en adaptieve organisatie – De criminele context en politie-interventies beter begrijpen en beïnvloeden', in: Meershoek, G., Nap, J. and van Spijk, L. (eds), *In Naam der Wat? Reflecties op politie en politiewerk*, Boom, The Hague, <https://doi.org/10.13140/RG.2.2.15492.55681>.

United States Department of Defense: Joint Chiefs of Staff (2013), 'Joint intelligence', *Joint Publication 2-0*, 22 October, https://www.benning.army.mil/infantry/doctrinesupplement/atp3-21.8/PDFs/jp2_0.pdf.

Van de 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*, National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online, <https://www.rephrain.ac.uk/wp-content/uploads/White-Paper-Towards-Data-Scientific-Investigations.pdf>.

Van der Zwet, K., Barros, A. I., van Engers, T. M. and Sloot, P. (2022), 'Emergence of protests during the COVID-19 pandemic: quantitative models to explore the contributions of societal conditions', *Humanities and Social Sciences Communications*, Vol. 9, pp. 1–11, <https://doi.org/10.1057/s41599-022-01082-y>.

Williams, P. and Kind, E. (2019), *Data-driven Policing: The hardwiring of discriminatory policing practices across Europe*, European Network Against Racism, Brussels, <https://www.statewatch.org/media/documents/news/2019/nov/data-driven-profiling-web-final.pdf>.

Appendix 12.1.

Code	Sub-code
Affiliation	
DDP	Definition
	Work process
	Data sources
	Developments
Type of crime	Organised crime
	Drug-related crime (specific)
	Cybercrime
	Police patrol
	Sexual offences
	Crime prevention
	Other
Organisational	Structure
	Leadership
	Human resources
	Education
Technological	
Human factor	Skills and expertise
	Mindset
	Societal
Legal	
Ethical	
SWOT	Strength
	Weakness
	Opportunity
	Threat
	Developments
International	Collaboration
	Positioning
Research proposals	