# AI AND ADMINISTRATION OF CRIMINAL JUSTICE. REPORT ON THE NETHERLANDS

By Maša GALIČ, Abhijit DAS and Marc SCHUILENBURG [*]

## I. PREDICTIVE POLICING

### 1 Introduction

There is great enthusiasm for the use of Artificial Intelligence (AI) in the criminal justice domain in the Netherlands.[1] This enthusiasm is connected to a strong belief – at least on the side of the government – that experimenting with new technologies can enhance security as well as improve government efficiency.[2] New digital systems are considered as leading to rational, scientific and value-neutral ways to generate knowledge and expertise within the criminal justice domain.

AI in this domain therefore holds a central position not only in policy documents,[3] but can also be seen in numerous examples in practice. The Dutch police stand at the forefront of predictive policing practices, at least in Europe, being the first to deploy an AI-based system for predictive policing nation-wide, and continue to set up an increasing number predictive policing projects.[4] Facial recognition technology is increasingly used in public space, both by the police and municipalities, often in

[*] Dr. Maša Galič (m.galic@vu.nl) is an Assistant Professor in Privacy and Criminal Procedure Law at the VU University Amsterdam; Abhijit Das is a PhD researcher at the VU University Amsterdam and Programme Director at The Democracy and Media Foundation (a.das@stdem.org); Prof. dr. Marc Schuilenburg (m.b.schuilenburg@vu.nl) is Professor of Digital Surveillance at the Erasmus University Rotterdam and Assistant Professor of Criminology at the VU University Amsterdam.

[1] See, for instance, the overview of the AI-based systems used by the government form 2021 in Marissa Hoekstra, Cass Chideock and Anne Fleur van Veenstra, 'Quick scan AI in de publieke dienstverlening II' (TNO 2021) <https://www.rijksoverheid.nl/documenten/rapporten/2021/05/20/quickscan-ai-in-publieke-dienstverlening-ii> accessed 13 January 2022.

[2] See e.g., H.J. van den Herik, 'Kunnen computers rechtspreken?' (Inaugural lecture, Gouda Quint, 1991); Corien Prins and Jurgen van der Rust, 'AI en de rechtspraak: meer dan alleen de 'robotrechter'' (2017) Nederlands Juristenblad 260.

[3] See e.g., 'Nederlandse Digitaliseringsstrategie 2021' (Ministerie van Justitie en Veiligheid 2021) <https://www.rijksoverheid.nl/documenten/kamerstukken/2021/04/26/nederlandse-digitaliseringsstrategie-2021>; 'Innovatie Met AI' (Overheid) <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/artificiele-intelligentie-ai/innovatie-met-ai/> accessed 13 January 2022.

[4] See e.g., Marc Schuilenburg and Melvin Soudijn 'Big data in het veiligheidsdomein: Onderzoek naar big data-toepassingen bij de Nederlandse politie en de positieve effecten hiervan voor de politieorganisatie' (2021), 20 Tijdschrift voor Veiligheid 4; 'We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands' (Amnesty International Netherlands, 2020) 11.

public-private partnerships constituted within smart city initiatives.[5] And AI-based systems, such as Hansken, are used for the purpose of finding evidence among huge amounts of data gathered in contemporary criminal investigations.[6]

It should be noted, however, that in the Dutch public sector the term AI is oftentimes used in a broad manner, including algorithmic systems of various complexity. The term AI is used not only for data-driven algorithms (where algorithms are trained on the basis of input data) or rule-based algorithms (where the steps, methodologies and outcomes can be traced to pre-programmed instructions implemented by a human), but also for older and much simpler types of statistical analysis (e.g., actuarial risk assessment tools, which are based on the correlation between certain factors and past statistics concerning recidivism). Because of this broad use of the term AI and a lack of publicly available information on the functioning of many technological systems used in practice, it is sometimes difficult to know, whether the system used in the criminal justice domain is strictly speaking AI-based or not. In any case, older methods for statistical analysis should be seen as a precursor of contemporary advanced AI techniques. The development of risk assessment technology, such as predictive policing and tools used for the assessment of the risk of recidivism, is namely taking place on a continuum, where several generations can be discerned.[7]

## 2 Definition of predictive policing

Definitions of predictive policing in the Netherlands, at least those stemming from 2015 onwards, generally share the following three elements: the use of (1) analytical techniques across (2) big datasets with the goal to (3) predict an increased chance of crime and disorder at a particular time and place.[8] The focus of the majority of

[5] See e.g., Tom van Arman, 'Smart Cameras for a Smart City' (Amsterdam Smart city, 4 March 2019) <https://amsterdamsmartcity.com/updates/news/smart-cameras-for-a-smart-city> accessed 13 January 2022.

[6] 'Hansken: The Open Digital Forensic Platform' <https://www.hansken.nl> accessed 13 January 2022.

[7] See e.g., Malcolm M Feeley and Jonathan Simon, 'The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications' (1992) 30 Criminology 449; Bernard E Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* (The University of Chicago Press 2006); Fernando Ávila, Kelly Hannah-Moffat and Paula Maurutto, 'The Seductiveness of Fairness: Is Machine Learning the Answer? – Algorithmic Fairness in Criminal Justice Systems' in Marc Schuilenburg and Rik Peeters (eds), *The Algorithmic Society* (Routledge 2020).

[8] See definitions in, for instance, Marc Schuilenburg, 'Predictive policing: De opkomst van een gedachtenpolitie?' (2016) Ars Aequi 931; Abhijit Das and Marc Schuilenburg, 'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht' (2018) Strafblad 19; Wim Hardyns and Anneleen Rummens, 'Predictive policing as a new tool for law enforcement? Recent developments and challenges' (2018) 24 European Journal on Criminal Policy and Research 201; Reinder Doeleman and others, '3 Misverstanden over predictive policing' (2019) 6/7 Het Tijdschrift voor de Politie 40.

definitions of predictive policing is, therefore, on 'crime mapping', rather than on predictive policing aimed at identifying risky individuals ('hot lists'). Based on different types of scores, the Dutch police take measures aimed at preventing or detecting predicted criminal activity by proactively directing police patrols towards particular locations. The Dutch understanding of the measure therefore aligns well with Ratcliffe's wide-used definition of predictive policing from 2014:

> "The use of historical data to create a spatiotemporal forecast of areas of criminality or crime hot spots that will be the basis for police resource allocation decisions with the expectation that having officers at the proposed place and time will deter or detect criminal activity."[9]

However, looking at the practice of predictive policing in the Netherlands, which we describe in the following section, we see that projects focus not only crime mapping, but also on the creation of 'heat lists'. There is thus a discrepancy between the definitions of predictive policing (stemming, perhaps, out of a particular perception of predictive policing practices, at least when these definitions are given by the police themselves) and the more diverse practice of predictive policing in the Netherlands.

## 3 The use and perception of predictive policing

### 3.1 Predictive policing projects

There are numerous applications of predictive policing currently deployed in the Netherlands. In this section, we introduce four well-known and publicly discussed examples of predictive policing, which are discussed in more detail in subsequent sections.

One of the more recent and well-known projects is the 'Sensing project', deployed by the Dutch police since 2019 in the city of Roermond in order to predict, whether the driver and passengers of a car are potential pickpockets or shoplifters of 'Eastern European' origin. The particular focus of this project is on 'mobile banditry', where small groups of persons drive to Roermond from another country (e.g., Germany), with the intent to shoplift in the nearby Outlet shopping centre and then immediately drive back abroad.[10] This project was developed by the police itself and described by the police as a 'living lab'. According to a report on the 'Sensing project' by Amnesty International the police have not clarified, which nationalities are understood as 'Eastern European': 'When speaking of "mobile banditry" in general,

[9] Jerry Ratcliffe, 'What Is the Future… of Predictive Policing?' (2014) Translational Criminology 3.

[10] Lonneke Stevens, Marianne Hirsch Ballin, Maša Galič and others, 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling: Een analyse aan de hand van de casus "Sensingproject Outlet Roermond"' (2021) 7 Tijdschrift voor Bijzonder Strafrecht & Handhaving 234.

the police refer to people from Poland, Bulgaria, Romania, and Lithuania. In the internal study, the police also refer to people with a nationality from Bosnia and Herzegovina or Serbia. (…) In addition to the emphasis on nationality, the police associate "mobile banditry" with the Roma ethnicity in the internal study on "mobile banditry" Roermond.'[11] In criminological literature on mobile banditry, this term generally refers to 'professional thieves', including: '(1) mobile bandits who are members of a large criminal organisation in their own country or who are recruited by these organisations for specific operations (such as the Augurkas in Lithuania); (2) mobile bandits who organise themselves into gangs while abroad and who remain abroad for longer periods in order to commit crimes; (3) Roma families who travel from country to country to engage in criminal activities before returning to Romania or Bulgaria to invest the proceeds of their crimes.'[12] In the Roermond' 'Sensing project', the police makes use of 'police records and data collected through new and existing sensors installed in public spaces, including Automated Number Plate Recognition (ANPR) cameras, as well as cameras that are able to detect a vehicle's brand, model, year of manufacture, and colour.'[13]

Since 2017, the National Police has been using the 'Criminality Anticipation System' (CAS; *Criminaliteits Anticipatie Systeem*) to predict crimes ('hot spots') at a national level. CAS was developed by the Dutch police (specifically, the Amsterdam unit) in 2014, and tested in a pilot project in four police districts. On a geographical map, CAS displays its predictions on grids the size of 125×125m, including the risk of criminal incidents within a specific timeframe. The risk locations are coded on a heat map with three colours: red for a high increase in the likelihood that a crime will occur, orange for a medium increase, and yellow for a low increase.[14] Each square is assigned a risk score for the following two weeks, indicating not only where but also when the risk of crime is high. This information is updated and analysed with the purpose of being incorporated in daily police operations. The two-week intervals are necessary because of displacement effects, which might occur due to increased surveillance in an area (for instance, in the case of burglaries).[15] CAS is the latest

[11] 'We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands' (n 4) 25–26.

[12] Dina Siegel, Mobile Banditry: East and Central European Itinerant Criminal Groups in the Netherlands (Eleven International Publishing 2014) 130.

[13] 'We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands' (n 4) 26.

[14] Arnout de Vries and Selmar Smit, 'Predictive policing: politiewerk aan de hand van voorspellingen' (2016) 42 Justitiële verkenningen 9; Albert Meijer, Lukas Lorenz and Martijn Wessels, 'Algorithmization of Bureaucratic Organizations: Using a Practice Lens to Study How Context Shapes Predictive Policing Systems' (2021) 81 Public Administration Review 837.

[15] Rosamunde van Brakel, 'Pre-Emptive Big Data Surveillance and Its (Dis)Empowering Consequences: The Case of Predictive Policing' in Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds), Exploring the Boundaries of Big Data (Amsterdam University Press 2016).

development in 'intelligence-led-policing', that can be called proactive policing, where intelligence is central to decision-making, and a more objective basis for deciding priorities and resource allocation is promised.[16]

Since 2015, the Amsterdam municipality has also been using the 'Top600' programme, which calculates the risk of committing a crime for young individuals under the age of 16. As such, this example of predictive policing no longer focuses on crime 'hot spots', but on 'heat lists' of risky individuals, thus going beyond the commonly used definition of predictive policing in the Netherlands. Individuals are selected on the basis of criteria developed by the police and the Public Prosecution Office.[17] 'Top 600' stands for 600 offenders of High Impact Crimes (e.g., assaults, street robbery, burglaries in stores, serious and public violence and murder) known to the local police. The Top 600 strategy is said to make use of an intensive, integral and target oriented approach aiming at changing behaviour of those on the list. The program objectives are surveillance, control, investigation, aftercare and personal contact with those involved in High Impact Crimes.[18] The Top 600 goals are accomplished in partnership with the local police, the public prosecutor and the involvement of social services, including mental health institutions, schools, childcare, rehabilitation and probation officers, and drug and alcohol addiction self-help groups.

Since 2011, National Police have also been using 'ProKid 12-SI System', an actuarial semi-automated risk assessment instrument to assess the risk of future property and violent offending by youths aged 12-18 years who have come in contact with the police as a suspect, victim, or witness. This system is thus another example of predictive policing focusing on the early identification of risky individuals in order to tackle juvenile crime at an early stage. The system identifies youths with an elevated risk for offending for the purpose of referring them to specialised youth care agencies for further assessment, as well as for the provision of feedback to the police by these youth care agencies. For this purpose, the instrument includes static and dynamic risk factors, and uses actuarial methods to gather information available in operational police systems, thus enabling an automated assessment procedure.[19]

[16] Jerry Ratcliffe, Intelligence-Led Policing (Routledge 2011).

[17] See 'Top 600 Aanpak' (Openbaar Ministerie) <https://www.om.nl/organisatie/arrondissementsparket-amsterdam/top-600> accessed 13 January 2022.

[18] Ruth Prins and Elke Devroe, 'Local Strategies for Glocal Challenges: Comparing Policing Agendas in Amsterdam and Rotterdam' in Elke Devrou, Adam Edwards and Paul Ponsaers (eds), Policing European Metropolises: The Politics of Security in City-Regions (Routledge 2017).

[19] Jacqueline Wientjes and others, 'Identifying Potential Offenders on the Basis of Police Records: Development and Validation of the ProKid Risk Assessment Tool' (2017) 3 Journal of Criminological Research, Policy and Practice 249.

The different variables were chosen based on the scientific literature on risk factors for the development of juvenile delinquency.[20]

Other predictive policing systems that were used in the past (and received a lot of attention in the Dutch media), include (1) SyRI (System Risk Indication), a policing tool used by municipalities to detect various forms of fraud, including social benefits, allowances, and taxes fraud; and (2) the Child Benefits System, used by the Dutch Tax Administration to detect abuse of child-care benefits. We take a closer look at these systems in sections 3.4, 3.5 and 4.4.2.

## 3.2 Predictive policing from a technological perspective

Considering the high amount of predictive policing projects that are taking place in the Netherlands, very little is publicly known about the way they function from a technological perspective. For this reason, we base our description below on one of the most well-known and discussed examples, for which some information on the matter is publicly available: the 'Criminality Anticipation System' (CAS).

As already mentioned, CAS is used by the Dutch police to predict crimes at a national level. The system synthesizes big data and geospatial technology by assigning risk criteria to areas of Dutch cities, the size of 125x125m. As such, CAS is a spatiotemporal prediction system which focuses on locations ('hot spots') in Dutch cities. CAS produces a line-graph which shows time and risk of a crime happening. The results are presented in a grid map (red coloured squares represent the areas with the highest risk for a certain crime to take place, orange squares represent a medium risk, and yellow squares a low risk).

[20] ibid. 251.

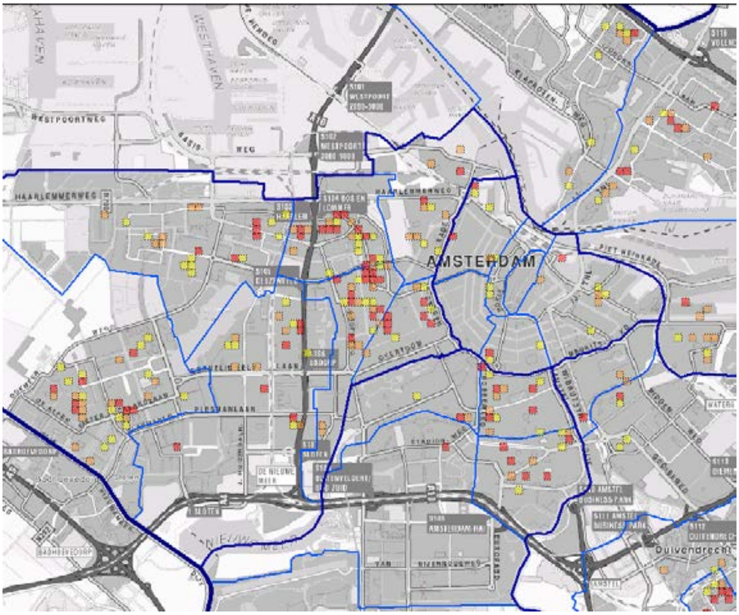


*Image 1: the CAS system showing risk areas in Amsterdam (source: Wikipedia,* <[https://nl.wikipedia.org/wiki/Criminaliteits_Anticipatie_Systeem#/media/Bestand:Criminaliteits_Anticipatie_Systeem.png](https://nl.wikipedia.org/wiki/Criminaliteits_Anticipatie_Systeem#/media/Bestand:Criminaliteits_Anticipatie_Systeem.png)> *accessed 13 January 2022)*

Originally, CAS was used to predict where and when the so-called 'High Impact Crimes' – crimes with a large impact on the victim, such as home burglary, street robbery and mugging – were likely to take place.[21] Later on, however, CAS has been extended to include several relatively minor crimes, such as pickpocketing, car burglaries, office burglaries, and bicycle theft, but also certain violent crimes.[22]

CAS uses a machine learning algorithm, which recognises and adapts to patterns in the gathered data. Risk-scores are attached to grids and are visualized by heat maps – using Gaussian filtering – to show the risk for crimes cartographically.[23] Predictions are made for each two-week period, based on historical data for a range of demographic, socio-economic and crime opportunity variables. These variables

[21] Dick Willems and Reinder Doeleman, 'Predictive Policing – Wens of Werkelijkheid?' (2014) 76 Het Tijdschrift voor de Politie 39.

[22] Hardyns and Rummens (n 8).

[23] Bas Mali, Carla Bronkhorst-Giesen and Mariëlle den Hengst, Predictive Policing: Lessen Voor de Toekomst: Een Evaluatie van de Landelijke Pilot (Politieacademie 2017); Paul Mutsaers and Tom van Nuenen, 'Predictively Policed: The Dutch CAS Case and Its Forerunners' in J Beek, T Bierschenk and A Kolloch (eds), Policing Differences: Perspectives from Europe (Manchester University Press forthcoming).)

are modelled using neural networks and the 3% of the highest risk locations on the map are flagged by the system.[24]

The data used by CAS are retrieved from a data-warehouse that combines input from the National Police Information System (*Basis Voorziening Informatie*; BVI), Statistics Netherlands (*Centraal Bureau voor de Statiestiek*) and GBA (Municipal Administration). BVI includes data that are collected by the Dutch police itself and provides CAS with addresses, locations and time/date of recent criminal incidents and known offenders ('suspects'). CBS, the main governmental agency responsible for collecting census data, provides socioeconomic and demographic data on the average income, social status, people's age, and family composition of inhabitants in postcode regions. Finally, geographical (location specific) data from GBA are used, such as information on the number of shops and the proximity of highways perceived as being 'escape routes' in the designated areas.

### 3.3 Predictive policing from a political and socio-organisational perspective

With the nation-wide deployment of CAS, the Netherlands is the first country in the world to predict on a national level where and when crime will be committed. In other countries, including the United States and Great Britain, this currently only happens on a local level.

In the Netherlands, the use of AI-based systems is being treated as part of a larger discussion on the digital transformation of society. Political and cultural developments play an important role in setting out how this digital transformation progresses in practice: from the political consensus to tackle criminality and disorder at an increasingly early stage (often spoken of in terms of war, such as 'war against crime'), to a strong belief in technology as the solution to social problems. As such, the political discourse in the Netherlands has been largely oriented towards avoiding all kind of risks and organised along the lines of security and insecurity, where security is defined in terms of the absence of risks. Risks that used to be regarded as self-evident have now become a question of poor governance.[25] Yet, the need for ever stronger pro-active control seems contradictory in a time when both recorded crime ('crime drop') and the number of people who sometimes feel insecure ('fear drop') continue to fall in the Netherlands. Not only are there fewer crimes and suspects, the number of criminal cases, sentences and prisoners is substantially lower than in the past as well. Figures from Statistics Netherlands

[24] Anneleen Rummens, Wim Hardyns and Lieven Pauwels, 'The Use of Predictive Analysis in Spatiotemporal Crime Forecasting: Building and Testing a Model in an Urban Context' (2017) 86 Applied Geography 255.

[25] Marc Schuilenburg, The Securitization of Society: Crime, Risk, and Social Order (New York University Press 2015) 93.

show that since 2002, crimes registered in the Netherlands have dropped by more than a quarter, and that the reduction applies to almost all crimes, from offences against property such as theft, burglary and muggings, to violent crimes, traffic offences and vandalism.[26] Nevertheless, from a socio-organisational perspective, AI-based systems are seen as the next step in technological developments that will substantially improve police work in the Netherlands, for instance, by revealing blind spots in tracking crimes, deploying the scarce resources of the Dutch police more efficiently to prevent crimes, and by determining adequate response strategies and adapting police patrols to these predictions. According to the Dutch police, 40% of burglaries and 60% of street robberies can be predicted this way.[27]

### 3.4 Public perception of predictive policing in the Netherlands

Prior to 2020, there was little (lay) public discussion on the use of AI-based systems for predictive policing purposes, which would aim to balance the benefits of technological innovation, while at the same time decreasing the potential negative effects of 'black-box' AI-systems on society.

The 2019 report of Amnesty International, 'We Sense Trouble', on mass surveillance in the Netherlands (with a particular focus on the mentioned 'Sensing project') is a notable exception. This report led to a public debate and questions from MP's to the Minister of Justice & Security.[28] The use of SyRI, a policing tool used by municipalities to detect various forms of fraud, including social benefits, allowances, and taxes fraud also generated public debate after the Hague District Court ruled in 2020 that the SyRI-tool did not comply with Article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life, home and correspondence.

The situation changed after the 2020 Child Benefits System scandal (*Toeslagenaffaire*), in which approximately 26,000 families were wrongly accused of social benefits fraud by Dutch tax authorities.[29] After this scandal was revealed and reported in the news, there has been a significant increase in critical public discussion in Dutch society on the dangers of using 'black-box' automated systems. A parliamentary report, 'Unprecedented Injustice', concluded that 'fundamental principles of the rule

[26] Marc Schuilenburg, Hysteria: Crime, Media and Politics (Routledge 2021) 75.

[27] Willems and Doeleman (n 21).

[28] 'We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands' (n 4).

[29] 'Dutch Childcare Benefit Scandal an Urgent Wake-up Call to Ban Racist Algorithms' (Amnesty International Netherlands, 25 October 2021) <https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/> accessed 14 January 2022.

of law had been violated'.[30] As a result, the Dutch government stepped down and resigned.

## 3.5 Reliability, impartiality and effectiveness of the predictive policing systems

The most interesting cases concerning the assessment of reliability of AI-based predictive policing systems relate to the (1) predictive tool SyRI and (2) the Child Benefits System scandal. The impartiality of such systems has not been specifically addressed.

In 2020, The Hague District Court delivered a judgment, concluding that the legislation regulating the use of SyRI (for the purpose of preventing and combating fraud in the interest of economic welfare) violated fundamental rights. The court decided that the legislation did not strike a fair balance, as required under the European Convention on Human Rights (particularly in relation to the right to respect for private life in Article 8), which requires adequate justification for violating private life. According to the Dutch court, 'the application of SyRI is insufficiently transparent and verifiable. As such, the SyRI legislation is unlawful, because it violates higher law and, as a result, has been declared as having no binding effect.'[31]

In 2020, The Childcare Allowance Parliamentary Inquiry Committee stated in their report 'Unprecedented Injustice' that, amongst others, basic principles of the rule of law were breached in the administration of childcare allowance. According to the Committee, 'the desire among politicians for the administration of benefits to be carried out efficiently and the wishes of politicians and society at large to prevent fraud resulted in the creation and implementation of legislation that permitted little scope, if any, for taking account of people's individual circumstances, such as administrative errors committed with no ill-intent.'[32] The Committee was particularly struck by the dismissal of the general principles of good governance that are supposed to act as a buffer and protective blanket for people in need.

In relation to effectiveness, the CAS system has been evaluated by the Dutch Police Academy in 2017. According to this study, the number of burglaries has reduced, but the researchers did not find a correlation between the drop and the predictions

[30] 'Dutch Childcare Benefit Scandal an Urgent Wake-up Call to Ban Racist Algorithms' (Amnesty International Netherlands, 25 October 2021) <https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/> accessed 14 January 2022.

[31] The Hague District Court, judgment of 5 February 2020, ECLI:NL:RBDHA:2020:1878 (case nr. C-09-550982-HA ZA 18-388).

[32] Van Dam and others (n 30) 7.

made by CAS.[33] Although the evaluation found no evidence that the system was effective (beyond the fact that the number of burglaries has indeed dropped), CAS was rolled out at a national level by the Dutch police in 2017.

## 4 The normative framework relating to predictive policing

### 4.1 The legal framework regulating the use of AI-based systems for predictive policing

The use of AI-based systems for law enforcement purposes is generally regulated by two main legal frameworks in the Netherlands: criminal procedure law and data protection law. Which of these two frameworks applies in a concrete case, depends on the phase of the use of the AI-based system: the collection or gathering of data is regulated by criminal procedure law, and the subsequent processing or use of the collected data is governed by data protection law for law enforcement (with a few exceptions, where data processing is included in criminal procedure law).[34] However, this distinction results in a set of issues for the regulation of digital investigation powers and has been criticised by several scholars.

#### *4.1.1 The gathering of data: the Code of Criminal Procedure and the Police Act*

The choice of a concrete provision (or a set of provisions) in the Code of Criminal Procedure (CCP), which would regulate the gathering of data, depends on the impact the method used to gather the data has on the rights of citizens, particularly the right to respect for private life (commonly referred to as the right to privacy). Currently, there are no provisions in the CCP that would regulate the gathering of data through AI-based systems (e.g., facial recognition systems). The upcoming modernisation of the CCP will introduce a specific provision concerning open-source intelligence (which commonly employs AI-based systems),[35] but no specific provision is envisioned for the use of facial recognition systems for the gathering of data, despite the fact that such systems are used in practice, especially in smart city-related projects.[36] As such, the description below relates solely to the regulation of methods through which data is gathered that may later on be processed by an AI-based system.

When the method used to gather data is considered to lead only to a minor intrusion into a person's rights, the method can be based on the general task description of the

[33] Mali, Bronkhorst-Giesen and den Hengst (n 23).

[34] Bart Schermer, 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens' (2017) 3 Tijdschrift voor Bijzonder Strafrecht & Handhaving.

[35] See Chapter 7, Article 2.8.8 of the draft Code of Criminal Procedure, 'Inhoud Nieuwe Wetboek van Strafvordering' <https://www.rijksoverheid.nl/onderwerpen/nieuwe-wetboek-van-strafvordering/inhoud-nieuwe-wetboek-van-strafvordering> accessed 13 January 2022.

[36] See Van Arman (n 5).

police (Article 3 Police Act or Article 141 CCP). This means that the use of such methods is not specifically regulated, as the task description does not contain any restrictive conditions (e.g., concerning the competent authority or the seriousness of the offence being investigated). According to Dutch case law, methods used for the gathering of location data of a specific person (e.g., through the use of 'silent SMS' or IMSI-catchers) leads to such a minor intrusion, on the condition that this practice does not take place for such a period of time, or with such a frequency or intensity, so that 'a more or less complete picture of certain aspects of a person's private life' is revealed.[37] This means that data, which may later be processed by an AI-based system, may be gathered through methods that are not specially regulated in criminal procedure law. However, the relevance for the gathering of data for AI-based systems through methods that are considered to make a minor infringement on fundamental rights seems limited. Generally, such methods are only suitable to gather relatively small amounts of data, as methods that would enable to gather larger amounts of data would in practice quickly amount to a bigger intrusion into the rights of citizens.

When the method used to gather data makes a 'more than minor' interference into fundamental rights (further distinguished into a 'far-reaching' and 'very far-reaching' intrusion), the legal rules and safeguards concerning the data gathering must be more detailed. The legal basis must contain restrictive conditions, such as the competent authority and the delimitation of the type of offences, for which the method may be used. An example particularly relevant in the context of AI-based systems, is the power to demand certain personal information regarding one or more persons (Article 126nc CCP). For instance, this power can be used to gather information on the visitors of a particular type of shop, such as a hardware store, where products are sold that can be used towards committing burglaries. The personal information gathered could be used in the prediction of the risk for committing certain criminal offences, particularly when combined with other information, enabling the creation of risk profiles. Because of the nature of this investigative method – it is coercive and intrudes into persons' privacy – the method is considered to make a 'more than minor' intrusion into the rights of citizens, therefore requiring a specific legal basis for the method.

In this way, Dutch criminal procedure regulates a relatively broad set of methods that can be used to gather data for AI-based systems, such as the network search (Article 125j CCP) and the hacking power (Article 126nba CCP). For some methods

[37] See e.g., Supreme Court of the Netherlands, judgment 1 July 2014, ECLI:NL:HR:2014:1563 (case nr. 13/04296); Supreme Court of the Netherlands, judgment of 1 July 2014, ECLI:NL:HR:2014:1562 (case nr. 12/01277), Supreme Court of the Netherlands, judgment of 1 July 2014, ECLI:NL:HR:2014:1569 (case nr. 13/04699).

that may interfere with the rights of citizens in a 'more than minor' way, but are not (yet) regulated in the current CCP, such as searching a smartphone incident to arrest, case law fills the void by building on more general provisions to formulate specific restrictive conditions.[38] However, as already mentioned, some powers, such as the use of facial recognition and predictive policing, which arguably also lead to a more than minor intrusion into a person's privacy (and other fundamental rights) are not specifically regulated either in the current or the draft CCP.

### *4.1.2 The processing of data: the Police Data Act (PDA)*

Considering the fact that no specific power using an AI-based system used for the gathering of data is regulated in the CCP (including in the draft CCP), the main legal framework regulating the use of AI-based systems in the Netherlands is data protection law for law enforcement. Data protection law for law enforcement regulates any processing of data for law enforcement purposes and it does not include any specific legal provision for the use of AI-based systems in criminal investigations. For policing activities, the most relevant Dutch data protection law is the Police Data Act (PDA), which is aligned with the EU Law Enforcement Directive.[39]

The applicable provision of the PDA depends on the purpose of the data processing: data can be processed for the daily police task (Article 8 PDA), for the purpose of upholding the legal order in a specific case (Article 9 PDA) and in the case of certain serious threats to the legal order (Article 10 PDA). The PDA also allows for the automated comparison and searching of data that has been processed in the context of the aforementioned provisions (Article 11 PDA).

However, AI-based systems used for predictive policing seem to fall in between the purposes for data processing regulated in the PDA. The data processing taking place in such systems is not meant for the daily police tasks, which consists of basic policing practices such as observation of activity on streets. Instead, AI-based systems are much more focused in their purpose, for instance, predicting in which

[38] For instance, Dutch criminal procedure does not contain a specific provision yet for the search and seizure of a smartphone during the arrest of a suspect, despite the fact that the search of a smartphone can indeed lead to a significant intrusion into a person's privacy. To provide an adequate protection to the right to privacy, case law has provided for restrictive conditions that apply to the investigation in the smartphone of a suspect. Dependent on the nature of the infringement, the Supreme court stipulates the authority that is authorised to carry out such an investigation (see e.g., Supreme Court of the Netherlands, judgment of 4 April 2017, ECLI:NL:HR:2017:584, case nr. 15/03882).

[39] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

area of the city a certain type of crime is likely to take place. However, the value of predictive policing systems also does not lie in the solving of a specific case or the focus on a specific threat, as Articles 9 and 10 PDA require.

Consequently, there seems to be a lack of legal rules for the processing of data by AI-based systems in the Netherlands.[40] As a temporary fix, the processing of data is in practice commonly based not only on the provisions in the PDA but also on the general task description of the police (Article 3 Police Act). However, as already mentioned, this legal provision allows only for minor interference with fundamental rights. Yet, it is highly debatable whether the data processing conducted by an AI-based system can be considered of such a minor character. We therefore argue that the legal framework applicable to the use of AI-based systems for law enforcement purposes in the Netherlands is not sufficiently regulated so as to provide for adequate protection against abuse of the powers, providing for few limitations and safeguards (these points are further discussed in 4.5.1 and 4.6.2).

## 4.2 Soft law instruments relating to the use of AI-based systems for predictive policing

The Dutch government has developed 'Guidelines for the use of algorithms by public authorities.'[41] The purpose of these guidelines is twofold: they are meant to help authorities develop AI-based systems as well as to inform the public on the use of such systems by government authorities. Through this twofold purpose, the government aims to enhance the quality and transparency of AI-based systems, and to provide for a better insight into (the use of) such systems. These guidelines have been drawn up by the government in consultation with experts from several public authorities and are partly based on the practices of these authorities. The guidelines contain a description of the different types of AI-based systems and the general safeguards for the quality of those systems. According to the guidelines, these general safeguards include:

- determine the purpose of data analysis (through the use of algorithms);
- determine the possible consequences of the data analysis for citizens;
- determine, whether machine learning is applied;
- identify the foundation in the law;
- determine the source of the data (which organisation do they come from) and their quality;
- determine who is responsible for the analysis;

[40] Cf. Stevens and others (n 10).

[41] 'Bijlage Bij Brief over Waarborgen Tegen Risico's van Data-Analyses Door de Overheid' (Ministerie van Justitie en Veiligheid, 2019) <https://www.rijksoverheid.nl/documenten/rapporten/2019/10/08/tk-bijlage-over-waarborgen-tegen-risico-s-van-data-analyses-door-de-overheid> accessed 13 January 2022.

- determine the role of third parties;
- identify the quality guarantees that are in place;
- determine how the human intervention between the analysis and the decision takes place;
- identify which normative frameworks apply and how the system is to be evaluated.

It should be noted, however, that this document is primarily meant as a tool for authorities when developing and using AI-based systems, rather than as a set of legal guarantees.

The police and the prosecution services have also drawn up the 'Quality framework Big Data',[42] which relates to the use of AI-based systems for law enforcement purposes, among others. The nature of this document is unclear, because of the informal character of the framework. The framework poses several questions that are relevant for the development of AI-based systems and stipulates the substantive interests that are to be protected (including privacy, non-discrimination and freedom of speech). However, the framework is explicitly not meant for assessing AI-based systems. As such, the framework is a development tool that can improve the quality of AI-based systems, but not much normative meaning can be attached to it.

Specifically in relation to the mentioned predictive policing project in Roermond, the police have composed a memo concerning the legality of the experiment.[43] This memo describes the concrete legal basis of the project: Article 3 Police Act in combination with Article 8 PDA (both relating to the daily police task). In itself, this memo is not of a regulative nature, but it does clarify the grounds on which the police presume they are acting in a legal and lawful manner.

### 4.3 International and regional normative instruments on the use of AI-based systems for predictive policing

In the development of its 'Guidelines for the use of algorithms by public authorities', the Dutch government regularly explicitly referred to – and drew inspiration from – international or regional normative instruments. This includes the EU Law Enforcement Directive and several documents drawn up by the European

[42] 'Kwaliteitskader Big Data' (Openbaar Ministerie en Politie, 2020) <https://www.rijksoverheid.nl/documenten/rapporten/2020/05/29/tk-bijlage-2-kwaliteitskader-big-data> accessed 13 January 2022.

[43] 'Nota Rechtmatigheid "Operationele Proeftuin Roermond" En "Generieke Proeftuinvoorziening"' (Politie, 2018) <https://www.politie.nl/binaries/content/assets/politie/wob/00-landelijk/programma-mobiel-banditisme-%E2%80%93-proeftuin-roermond/083---nota-rechtmatigheid-optr-en-gpv-v-1.3-2_def.pdf> accessed 13 January 2022.

Commission on the regulation of AI-based systems, such as the European strategy on Artificial Intelligence.[44] The most recent developments concerning AI-based systems, such as the draft EU Artificial Intelligence Act,[45] will probably also play an important role. The goal in the Guidelines is not so much the implementation of these supranational instruments, but using these instruments in order to (further) develop thoughts on how to design normative frameworks that would fit AI-based systems.

On a more general level, the EU Law Enforcement Directive and the jurisprudence of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) have played an important role in the design of legal instruments in the Netherlands. This is true both for the gathering and the processing of data. For instance, the restrictive conditions that apply to the methods used for gathering data partially stem from the requirement to provide for a detailed regulation in the law with sufficient safeguards that is in accordance with the jurisprudence of the ECtHR, especially concerning Article 8 ECHR.[46] In the judgments concerning the search of a smartphone incident to arrest, the Dutch Supreme Court explicitly referred to Article 8 ECHR when stipulating the condition that prior judicial approval is required in cases of searches that lead to a more than minor intrusion into a person's private life. Concerning the processing of personal data, the Police Data Act was amended in 2018 to implement the Law Enforcement Directive. However, this adjustment was relatively minor, since the Dutch PDA already strongly resembled the Directive.[47]

## 4.4 Case law

### *4.4.1 Decisions of the Dutch Data Protection Authority*

To the knowledge of the authors, the Dutch Data Protection Agency (*Autoriteit Persoonsgegevens*; DPA) has not yet taken any decisions concerning predictive policing. However, AI and algorithms are one of the focus areas of the DPA for the

[44] 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Artificial Intelligence for Europe' (European Commission, 25 April 2018) <https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)237&lang=en> accessed 14 January 2022.

[45] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 2021 [COM(2021) 206 final].

[46] E.g., ECtHR 4 December 2008, ECLI:CE:ECHR:2008:1204JUD003056204, appl. nos. 30562/04 and 30566/04 (S. and Marper v. the United Kingdom).

[47] Bart Custers and Lonneke Stevens, 'The Use of Data as Evidence in Dutch Criminal Courts' (2021) 29 European Journal of Crime, Criminal Law and Criminal Justice 25.

period 2020-2023.[48] The identified goals of the DPA concerning AI-based systems are: developing an effective system of supervision for the use of AI-based systems and promoting the explanation of the process, its key elements and the result of AI-based systems to citizens. Broad outlines of this system of supervision have been put down in a publicly accessible document.[49] Unfortunately, the document (of a mere 11 pages) is drafted in very general terms, stating that the system of supervision is based on three principles: lawfulness, fairness and transparency.[50] The document also does not discuss the use of AI-based systems in cases of predictive policing.

### *4.4.2 Jurisprudence concerning predictive policing*

Despite widespread use of predictive policing in the Netherlands, criminal courts have so far not yet ruled on a case concerning predictive policing. However, in the abovementioned SyRI-case (see 3.5), a civil court has decided on the lawfulness of a system for detecting benefit fraud.[51]

The Hague District Court ruled that the legislation underlying the system was in breach of Article 8 ECHR. According to Article 8, when states employ new digital technologies, they also need to strike a fair balance between the public interest (in this case, to fight benefit fraud) and the interest of individuals concerning their right to respect for private life.[52] According to the district court, the main problem with SyRI was that the system was not transparent enough, and consequently, not verifiable enough. As such, the system was considered not capable of striking a fair balance between the interest of combating fraud and the privacy violation caused by the investigative method.

However, currently a draft law introducing an AI-based system for detecting benefit fraud (*Wet gegevensverwerking door samenwerkingsverbanden*) – also called the 'super-SyRI' – is under debate in the upper chamber of the Dutch parliament, having already passed through the lower chamber.[53] Several parliamentary parties have protested the introduction of this new system, after which the upper chamber of the parliament sought additional advice from the Council of State. The Council of State

[48] 'Focus Autoriteit Persoonsgegevens 2020-2023' (Autoriteit Persoonsgegevens, 2020) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/focus_ap_202-2023_groot.pdf> accessed 13 January 2022.

[49] 'Toezicht Op AI & Algoritmes' (Autoriteit Persoonsgegevens) <https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezicht-op-algoritmes> accessed 13 January 2022.

[50] ibid 5–7.

[51] District Court of The Hague, judgment of 5 February 2020, ECLI:NL:RBDHA:2020:1878 (case nr. C-09-550982-HA ZA 18-388).

[52] See e.g., S. and Marper v. UK (n 46).

[53] 'Wet Gegevensverwerking Door Samenwerkingsverbanden' (Eerste kamer der Staten-Generaal, 2020) <https://www.eerstekamer.nl/wetsvoorstel/35447_wet_gegevensverwerking_door> accessed 13 January 2022.

issued an advice that was critical of the draft law, following which the upper chamber asked the relevant ministers for a reaction.[54]

## 4.5 Substantive guarantees: reliability, impartiality and effectiveness

### *4.5.1 Normative instruments guaranteeing the reliability, impartiality and effectiveness of AI-based systems*

As already discussed in section 4.1, the regulation of the use of AI-based systems for predictive policing in Dutch law is mainly found in the Police Data Act (PDA) and the Police Act. It is, however doubtful whether this legal framework can be considered sufficient from the perspective of Article 8 ECHR.

As we have seen in the example of the Roermond project, the police consider that a sufficient legal basis for such predictive policing projects can be found in Article 3 Police Act in combination with Article 8 PDA, which concern the daily police task. While Article 3 Police Act does not provide for any substantive guarantees whatsoever, the PDA does provide for some classic data-protection-types of guarantees concerning the reliability, impartiality and effectiveness of the AI-bases system. This includes a prohibition of fully automated decisions (without any human intervention; Article 7a). Furthermore, an important safeguard for the protection of the reliability, impartiality and effectiveness of AI-based systems is that the data used must be of a certain quality. Article 3 PDA prescribes that the data used must be accurate and legally obtained. However, it is up to the police themselves to guarantee that this is indeed the case. The PDA also provides individuals (data subjects) with the right to ask for information concerning any possible collection of their personal data (Article 25) and to have certain information rectified or removed (Article 28). However, in relation to both of these rights, there are exceptions to the rule for reasons of inter alia protection of investigative interests (Article 27). Individuals can also file a complaint with the Data Protection Authority (DPA; Article 31a) and can pursue compensation for damages in cases when an AI-based system is used in a criminal investigation, whether or not the system has been used legally (Article 31c). For the compensation of damages, the regular civil trajectory must be followed.[55]

[54] 'Voorlichting Met Betrekking Tot Het Wetsvoorstel Wet Gegevensverwerking Door Samenwerkingsverbanden' (Raad van state, 2021) <https://www.raadvanstate.nl/actueel/abonnementenservice/samenvattingen/samenvatting/@126518/w16-21-0223-ii-vo/#toonsamenvatting> accessed 13 January 2022.

[55] For a discussion on the lack of effectiveness of these safeguards to keep out so-called dirty data see Abhijit Das and Marc Schuilenburg, '"Garbage in, garbage out": Over predictive policing en vuile data' (2020) 47 Beleid en Maatschappij 254.

In the context of law enforcement, these safeguards have been criticised as being both inappropriate as well as ineffective.[56] First of all, by copying the approach of 'data subject rights' from general data protection law, these safeguards place a lot of responsibility on the individual subjected to investigative measures. However, these rights (for example, the right to receive information about the processing of personal data pertaining to the data subject and the right to get access to such data) may rather easily be limited or completely revoked, when such limitation is in the interest of prevention or investigation of crime. This lack of knowledge of the processing practices also impedes the effectiveness of the supervision of these policing practices conducted by the DPA. If the data subject does not know which of their personal data are processed and how, the individual is in no position to complain to the DPA that their personal data are not being processed in a fair and lawful manner. That means that the supervision of the processing practices of the police heavily depends on the proactive supervision of the DPA. As we have already mentioned, this does not seem to happen in practice, considering that the DPA has not issued a single decision concerning predictive policing. Moreover, the DPA also has very limited powers to remedy the violations pertaining to data processing (something which already stems from the EU Law Enforcement Directive).[57]

More generally, Dutch law also provides for general principles that must always be respected when a criminal investigation is taking place. Currently, these principles are unwritten and merely implicit in Dutch law, but they will be provided for explicitly in the modernised draft Code of Criminal Procedure.[58] These principles might play a role in guaranteeing the reliability, impartiality and effectiveness of predictive policing-systems in cases, assuming that predictive policing practices indeed fall within the scope of a criminal investigation (see discussion in 4.5.3). Of particular interest in the context of AI-based systems are: the principle of proportionality, the principle of subsidiarity and the principle that investigative methods are applied only when they are in the interest of a specific investigation.[59] According to these general principles, an AI-based system must contribute to the goal of a predefined criminal investigation, which needs to be – at least, to a certain degree – determined in objective terms. This places a certain burden of reliability

[56] See e.g., Schermer (n 34); Stevens and others (n 10).

[57] Paul De Hert and Juraj Sajfert, 'The Role of Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data' in C Brière and A Weyembergh (eds), *The needed balances in EU criminal law: past, present and future* (Hart 2018) 251–252.

[58] These principles are further described in Marianne Hirsch Ballin and Maša Galič, 'Digital Investigation Powers and Privacy: Recent ECtHR Case Law and Implications for the Modernisation of the Code of Criminal Procedure' (2021) 2 Boom Strafblad 148.

[59] See Book 2, Title 1.2 of the draft CCP; 'Inhoud Nieuwe Wetboek van Strafvordering' (n 36).

and impartiality on the use predictive policing-systems, since unreliable or biased systems cannot objectively contribute towards a criminal investigation.

However, the problem with such abstract principles is that the understanding of the principles can be so broad, that in concrete cases the regulatory meaning of principles is not much more than illusive. In fact, looking at past experience in the Netherlands, principles have failed to provide effective safeguards in practice.[60]

### *4.5.2 Prior assessment and monitoring of AI-based systems*

Before deploying any AI-based tools for predictive policing (or any other law enforcement purpose), a Data Protection Impact Assessment (DPIA) needs to be conducted (Article 4c PDA). According to the PDA (as well as the EU Law Enforcement Directive), such an assessment is always required when there is a risk for the rights of citizens.

The DPIA needs to include: a description of the data being processed and the goals of the processing; an assessment of the legality of the use of data (i.a., the legal basis, necessity, proportionality and the compatibility of the system with the designated goal); a description and assessment of the risks for the rights and freedoms of those concerned (including but not limited to the right to private life); and a description of the measures intended to mitigate these risks. These general substantive categories are described in more detail in a model DPIA that the central government has developed.[61] This assessment is carried out by the data controller within the police organisation. The results of the DPIA must be included in a register in which all of the activities of the data controller are recorded. After the DPIA has been conducted, the data controller is also responsible for the assessment, whether the authorities act in accordance with the DPIA. In case the result of the DPIA is that the risks cannot be sufficiently mitigated by certain measures, the Data Protection Authority (DPA) must be contacted and give specific permission for the use of the intended system.[62]

There is no obligation to continuously monitor and adjust the use of AI-based systems used for predictive policing. However, the DPA recommends that a DPIA

[60] AA Franken, 'Proportionaliteit en subsidiariteit in de opsporing' (2009) 8–13 Delikt en Delinkwent 7. For a similar critique of the principles in the modernised Code of Criminal Procedure see Abhijit Das, 'De codificatie van rechtsbeginselen in het gemoderniseerde Wetboek van Strafvordering' (2018) 1 Tijdschrift Modernisering Strafvordering.

[61] 'Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)' (Ministerie van Justitie en Veiligheid, 2017) <https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia> accessed 14 January 2022.

[62] 'Voorafgaande Raadpleging' (Autoriteit Persoonsgegevens, 2018) <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging> accessed 14 January 2022.

be repeated every three years.[63] The Dutch government also considers that a continuous validation of AI-based systems and audits of the results should be the norm.[64] These ex-post checks are meant to be complimentary to the ex-ante DPIA. Yet, there is no legal obligation for such a continuous process of monitoring. In certain cases, the necessity for an intermediate DPIA can arise, for instance if a new technology is to be used, or if the goals of the data processing have changed. This is so, because the new processing of data is no longer of the same nature as was the case when the initial DPIA was carried out.[65]

### *4.5.3 Guaranteeing transparency about the use of AI-based systems*

For the purpose of guaranteeing transparency, all relevant activities during criminal investigations need to be officially noted in a police report (Article 152 CCP). The police report first enables the public prosecutor in charge of the investigation to keep an eye on the proceedings. Furthermore, if the case is prosecuted, these reports form a part of the case file, which provides all involved parties, including the defence and the court, with insight into the phase of the criminal investigation. It is important to note in this regard that the definition of a criminal investigation in Dutch law (Article 132a CCP) is broad: the investigation does not need to be focussed on a specific crime that has been committed; it can focus on future, undefined, crimes as well. The only substantial requirement is that the purpose of the investigation is to contribute to solving criminality, such as burglaries in a particular municipality or thefts in a particular area.[66] As such, the general goal of predictive policing-systems to better identify risky geographical areas or individuals relevant to solving a certain type of crime – at least in principle – fits within this broad definition of a criminal investigation.

This means that when AI-based systems are used for the purpose of predictive policing, the police are required to guarantee the transparency of the investigative process, including the use of the AI-based system, by writing down all of the relevant activities in the police report. However, as scholars have pointed out, it is unclear what constitutes adequate reporting on the use of AI-based systems in

[63] 'Data Protection Impact Assessment (DPIA)' (Autoriteit Persoonsgegevens, 2019) <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia> accessed 14 January 2022.

[64] Bijlage 2 Bij Kamerbrief- Reactie Reguleringsopties Rapport Modernisering Procesrecht' (Ministerie van Justitie en Veiligheid, 2020) <https://www.rijksoverheid.nl/documenten/rapporten/2020/11/20/tk-bijlage-2-bij-kamerbrief-reactie-reguleringsopties-rapport-modernisering-procesrecht-in-het-licht-van-big-data> accessed 14 January 2022.

[65] 'Data Protection Impact Assessment (DPIA)' (n 63).

[66] See e.g., Supreme Court of the Netherlands, judgment of 30 June 2020, ECLI:NL:HR:2020:1155 (case nr. 18/03043).

practice.[67] The complexity of AI-based systems means that it is much more difficult to report on the use of such a system, than reporting, for instance, on physical observation of a person. Despite this issue being raised, there is still a lack of any more concrete instructions concerning the implementation of Article 152 CCP when it comes to the use of AI-based systems. Yet, this seems to be crucial if transparency is to be achieved in practice.

In general, the Dutch government and investigative authorities (police and public prosecution services) emphasise the importance of transparency in the context of AI-based systems. As already mentioned (see 4.2), both have drawn up frameworks to enhance the quality and transparency of the AI-systems they use. However, the two frameworks do not provide for legal guarantees, they merely serve as soft guidelines that the authorities should strive towards. Nevertheless, the government has at least made clear the categories of information that are important in order to guarantee transparency (e.g., the purpose of data analysis, the source and quality of data, whether machine learning is used, the foundation in the law, the data controller). This can help the legislator and the judiciary to identify those aspects of predictive policing, which need to be made transparent by the investigative authorities. As such, this framework (as well as the 'Quality framework Big Data' of the police and prosecution services) might be used to substantiate the meaning of the guarantee to document all relevant activities in a police report, which could be done either by the legislator or through case law.

Another safeguard guaranteeing a level of transparency can be found in Article 24a and subsequent articles in the PDA. According to these provisions, individuals who suspect that their personal data are used within AI-based systems for law enforcement purposes have the right to be informed about the use of their personal data in the process. This right to information may also include the right to be informed about the logic underlying the automated decision-making (Art. 24b(2)e PDA). However, as already discussed (see 2.5.1), the safeguards found in the PDA are ineffective in practice: this is generally due to the fact that citizens are not informed of government practices concerning predictive policing (and other uses of AI-based systems for law enforcement purposes), leading to very little use of the procedural mechanisms offered by the PDA.[68]

### *4.5.4 Accountability for the actions taken on the basis of AI-based systems*

Currently, the mere prediction of an AI-based system does not suffice to establish reasonable suspicion and, as such, cannot lead to the arrest of a suspect. This is not

[67] Das and Schuilenburg (n 8); Das and Schuilenburg (n 54).

[68] Bart Custers and Mark Leiser, 'Persoonsgegevens in het strafrecht: weeffouten in EU-Richtlijn 2016/680 leiden tot praktische problemen' (2019) 34 Nederlands Juristenblad 8.

likely to change in the nearby future.[69] At most, predictions of AI-based systems may lead to further investigative activities, such as the surveillance of specific areas, people or a specific vehicle.[70] Only these subsequent investigative activities can lead to reasonable suspicion and thus result in the arrest of a suspect.

This has important consequences concerning the accountability for the actions taken on the basis of AI-based systems. In those (arguably predominant) cases, where the prediction of an AI-based system does not lead to a subsequent investigation, arrest and prosecution, there is simply no judicial oversight of the use of the AI-system. However, as recent academic research has shown, there is no effective alternative to judicial oversight either, for instance through civil judicial proceedings or an independent oversight committee.[71] This results in a general lack of effective oversight concerning the use of AI-based systems, let alone holding authorities accountable.

Another issue arises in cases, in which the prediction of an AI-based system does lead to prosecution, thus, triggering judicial oversight. This issue relates to the lack of concrete legal rules for the assessment, whether the prediction is sufficiently accurate. As discussed in sections 4.5.1 and 4.5.2, the regulation of AI-based systems currently depends on very general principles. The quality of data used by authorities in the phase before investigative methods that actually lead to an arrest are used is completely neglected in case law. As such, there is no threshold according to which authorities can be held accountable for the predictions used in a criminal investigation.[72] The question concerning accountability therefore largely remains unaddressed and unanswered. Instead, public discussion focuses on issues resulting from the prediction, which can actually be observed, such as discrimination and ethnic profiling (discussed in 4.6.1).

From the perspective of accountability, it is also relevant to note that even when unlawfulness relating to the use of an AI-based system is established by the trial court, holding the authorities accountable for their actions is not considered the primary focus of the criminal judicial process. The Dutch Supreme Court is, namely, of the opinion that holding authorities accountable and the lawfulness of criminal proceedings, as such, are not the primary tasks of the criminal judge.[73] According to

[69] RA Hoving, 'Verdacht door een algoritme. Kan predictive policing leiden tot een redelijke verdenking?' (2019) 41 Delikt en delinkwent 530.

[70] Das and Schuilenburg (n 8).

[71] Mojan Samadi, *Normering en toezicht in de opsporing: Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen* (Boom Juridisch 2020).

[72] Das and Schuilenburg (n 8).

[73] Supreme Court of the Netherlands, judgment of 1 December 2020, ECLI:NL:HR:2020:1889 (case nr. 18/03503).

the Supreme Court, the focus of the criminal judge is on guaranteeing a fair trial, rather than on protecting other rights of citizens, such as the right to non-discrimination or privacy.[74] Consequently, even when AI-based calculations contain a problematic element in this regard, authorities are generally not held accountable in practice. Only in the most severe cases of unlawfulness, Dutch courts actually opt for the exclusion of evidence. And even in those cases, this generally goes unnoticed by relevant authorities, meaning that accountability remains distant and formal.[75]

## 4.6 General principles of law

### *4.6.1 The right to non-discrimination*

The public discussion in the Netherlands on the risk of discrimination stemming from the use of AI-based systems for predictive policing was primarily triggered by the already mentioned report by Amnesty International Netherlands (Amnesty International) on the risk of ethnic profiling through AI-based methods.[76] According to both Amnesty International as well as some Dutch legal scholars, methods used for predictive policing (including AI-based systems) pose a risk to the right to non-discrimination, because such methods can lead to ethnic profiling.[77]

Amnesty International defines ethnic profiling as 'the use, without objective and reasonable justification, of personal characteristics such as colour, religion, nationality and/or ethnic origin in police control, surveillance or investigation activities.'[78] It may occur not only when one of these characteristics is used directly as a profiling factor, but also in less visible ways, when seemingly neutral factors (e.g., a postcode) disproportionally affect certain groups in practice. In its report, Amnesty International used the Roermond project as an example of ethnic profiling. The risk model used in the project attached a higher 'score' to license plates from certain ('Eastern European') countries, operating as a proxy for the ethnicity of the driver (e.g., Roma); as such, vehicles with such license plates were at a greater risk of being selected for additional investigative actions, such as stops and searches. Consequently, such profiling led to discrimination.

[74] ibid.

[75] Elke Devroe and others, 'Toezicht Op Strafvorderlijk Overheidsoptreden' (WODC 2017), available at <https://repository.wodc.nl/handle/20.500.12832/2258> accessed 6 January 2023.

[76] 'Nederland, Maak Een Einde Aan Gevaarlijke Politie-Experimenten Met Massasurveillance' (Amnesty International Netherlands, 29 September 2020) <https://www.amnesty.nl/actueel/nederland-maak-een-einde-aan-gevaarlijke-politie-experimenten-met-massasurveillance> accessed 14 January 2022.

[77] Das and Schuilenburg (n 8).

[78] 'We Sense Trouble: Automated Discrimination and Mass Surveillance in Predictive Policing in the Netherlands' (n 4) 22.

According to Amnesty International and legal scholars, Dutch law lacks specific norms that look to prevent discrimination in criminal investigations.[79] Concrete legal safeguards to prevent discrimination through AI-based systems and, especially, the follow up actions based on its predictions (such as traffic stops or surveillance) are hard to find. Of course, international law provides certain safeguards against discrimination, but within the Dutch legal order these have not been materialised into any clear-cut legal standards applicable in criminal cases. This has been pointed out as a cause for concern. Brinkoff considers that the right to non-discrimination should at least be recognised by the legislator as a general principle of criminal procedure (see 4.5.1 on general principles in Dutch criminal procedure).[80]

According to Das and Schuilenburg, the void concerning the right to non-discrimination left by Dutch legislation has also been insufficiently addressed in case law.[81] The Dutch Supreme Court considers that profiling (whether or not automated) of certain (groups of) people is generally unproblematic as long as the profile is not solely or decisively based on potentially discriminatory factors, such as ethnicity.[82] These decisions have come under heavy criticism from legal scholars. According to Bouwman, this criterion is effectively useless in practice, as it is hardly possible to determine the exact role of a certain factor, such as ethnicity, in creating a profile when several factors are involved.[83] As such, it can lead to the whitewashing of discrimination: through the inclusion of additional factors, types of data, questions, etc. in the process of creating a profile, the role of a potentially discriminating factor can easily be ignored in practice.[84] Furthermore, the interpretation of the Supreme Court, which allows for profiling in criminal cases, might also be incompatible with international law.[85]

### *4.6.2 The right to privacy*

[79] Sven Brinkhoff, 'The Dutch paradox: over discriminatoir handelen in de Nederlandse strafrechtspleging en concrete handvatten om dit tegen te gaan' (2021) Nederlands Juristenblad 7; Vera E Prins, 'Sensoren, Risicoscores En Mensenrechten: Een Onderzoek Naar de Mensenrechtenimplicaties van Het Predictive-Policingproject Sensing Mobiel Banditisme in Roermond' (Master's Thesis, Utrecht University 2020).

[80] Brinkhoff (n 79).

[81] Das and Schuilenburg (n 54).

[82] See e.g., Supreme Court of the Netherlands, judgment of 1 November 2016, ECLI:NL:HR:2016:2454 (case nr. 16/00207); Supreme Court of the Netherlands, judgment of 9 October 2018, ECLI:NL:HR:2018:1872 (case nr. 16/00166).

[83] A Bouwman, 'Etnisch profileren bij proactief politieoptreden, mag dat van de strafrechter?' [2021] Delikt en delinkwent 62.

[84] ibid.

[85] 'Debat over etnisch profileren vraagt om meer juridische duidelijkheid' (College voor de rechten van de mens 2021) <https://publicaties.mensenrechten.nl/file/a261a614-6d6e-4d1d-be8c-0c88fd43b954.pdf> accessed 14 January 2022.

The right to respect for private life in Article 8 ECHR is a common tool to discuss and problematise AI-based systems used for predictive policing. Examining the Roermond predictive policing project from an Art. 8 ECHR perspective, Stevens, Hirsch Ballin, Galič et al. conclude that the very general legal basis relating to the daily police task as found in Art. 3 Police Act and Art. 8 PDA, which is without any meaningful safeguards (e.g., a limitation on the scope and duration of the measure, the grounds for ordering it and the authorities to authorise it), does not offer adequate protection against arbitrary interference with the right to respect for private life.[86] This conclusion is based on longstanding ECtHR case law on surveillance and (digital) surveillance technologies,[87] according to which the legal basis for privacy intrusive powers needs to be of a certain quality, offering sufficient safeguards and limitations. The ECtHR, of course, distinguishes between more or less privacy intrusive powers. For instance, non-systematic GPS surveillance is not considered as intrusive as the interception of communications or searching data on a computer.[88] Consequently, the safeguards found in the legal basis need not be as strict and detailed as in regard to more intrusive powers. However, in the 2018 Ben Faiza v. France case, the ECtHR considered that even in the case of non-systematic GPS surveillance (a relatively minor privacy intrusion), a very general legal basis (as is usually found in relation to the daily police task), did not indicate with sufficient clarity to what extent and how the designated authority (in this case the investigatory judge) was entitled to use this discretionary power, thus finding a violation of Art. 8 ECHR.[89]

As already mentioned, the Dutch approach to the right to privacy (stemming from case law) distinguishes between three types of privacy intrusions: a minor, more than minor and far-reaching intrusion into privacy. Only those interferences with privacy, which are considered minor may have a very general basis in the law, such as the one for the daily police task, essentially offering no limitations and safeguards. According to Dutch case law, using an infrared camera for thermal imaging of houses (for the detection of growing cannabis), IMSI-catchers and silent SMS are all considered leading to such a minor privacy intrusion, requiring no specific legal

[86] Stevens and others (n 10); see also Hans Lammerans and Paul De Hert, in Bart Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the boundaries of big data* (Amsterdam University Press / WRR 2016).

[87] For an overview of relevant ECtHR case law see Maša Galič, 'Surveillance and Privacy in Smart Cities and Living Labs: Conceptualising Privacy for Public Space' (Doctoral dissertation, Tilburg University 2019) 267–322.

[88] ECtHR 2 September 2010, ECLI:CE:ECHR:2010:0902JUD003562305, appl. no. 35623/05, para. 61 (Uzun v. Germany); ECtHR 8 February 2018, ECLI:CE:ECHR:2018:0208JUD003144612, appl. no. 31446/12 (Ben Faiza v. France).

[89] The French provision at the time (Art. 81 Code Pénal) referred merely to a very general power, allowing the police to conduct all 'acts of information deemed useful to establishing the truth' (Ben Faiza v. France, paras. 58-60).

basis.[90] The police and public prosecution thus seem to consider that predictive policing, even when conducted with AI-based systems, leads to a minor intrusion into privacy. This is connected to the fact that Dutch courts generally do not consider the whole process of data processing, which includes the collection, aggregation, processing and, finally, use(s) of data; instead, they only consider the level of privacy intrusion at the very first step: when the data are collected.[91] Thus, if a particular power allows a one-time gathering of data that are not particularly privacy sensitive – which is usually the case in IMSI-catchers, silent SMS but also predictive policing – courts (and investigatory judges) will rather quickly consider that the privacy intrusion is minor. This takes place despite the fact that the creation of various types of databases and the aggregation of data, which are then further processed by increasingly complex technologies – thus leading to a potentially very far-reaching privacy intrusion – is an increasingly common practice in the Netherlands, and certainly a goal for the future.

Stevens, Hirsch Ballin, Galič et al. offer another possible reason, why the police, public prosecution and Dutch courts might consider that predictive policing does not lead to more than a minor privacy intrusion. They point to the fact that within the hot spot-type of predictive policing, no individual is targeted, since the focus lies on a specific profile (e.g., people that might be considered mobile bandits). Moreover, the data that are collected and processed also do not (directly) relate to an individual (e.g., crime statistics relating to a particular area and the types of data relating to vehicles, such as colour and the route taken, as collected in the Roermond project). Nevertheless, as the debate in field of data protection law shows, through data aggregation and analysis, individuals may later on still be indirectly identifiable and affected by the measure (as was indeed the case in the social benefits scandal mentioned earlier).[92] In this regard, Stevens, Hirsch Ballin, Galič et al. point to research concerning the notion of 'group privacy',[93] according to which the privacy intrusion takes place before an individual is actually identified and affected by the surveillance measure, at the stage when persons become a part of a profile.

[90] See judgments of the Dutch Supreme court mentioned in reference (n 37).

[91] Cf. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, 'Regulering van Opsporingsbevoegdheden in Een Digitale Omgeving' (2018) 24–26 <https://kennisopenbaarbestuur.nl/documenten/rapport-commissie-koops-regulering-van-opsporingsbevoegdheden-in-een-digitale-omgeving/> accessed 14 January 2022. See also judgments of the Supreme Court mentioned in reference (n 37).

[92] See e.g., Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40; Maša Galič and Raphaël Gellert, 'Data Protection Law beyond Identifiability? Atmospheric Profiles, Nudging and the Stratumseind Living Lab' (2021) 40 Computer Law & Security Review 1.

[93] See e.g., Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer 2017).

This discussion therefore underscores the importance of looking at the whole process when it comes to assessing the level of privacy interference of digital investigation powers.

### *4.6.3 The principle of proportionality*

Proportionality is one of the general principles of criminal procedure law, which also regulates the use of AI-based systems for predictive policing. Stevens, Hirsch Ballin, Galič et al. have drawn on the principle of proportionality to question the nature of the relationship between AI-based systems performing large scale data analysis for predictive policing and the combating of minor offences, such as shoplifting.[94] Amnesty International has gone further, stating that predictive policing projects inevitably rely on mass surveillance and can therefore never be proportionate.[95] In this context, Prins has called for an ex ante definition and delimitation of the scope of the use of AI-based systems for predictive policing, for instance by limiting the use of such systems to investigations regarding serious offences.[96]

Dutch legal scholars seem to agree that there is a lack of concrete safeguards concerning the proportionality of AI-based systems.[97] This is connected to two points of critique already discussed: (1) the questionable regulatory value of general principles such as proportionality in Dutch law; and (2) a lack of a clear legal framework with restrictive conditions concerning the use of AI-based systems in Dutch law.

### *4.6.4 Suspicion and procedural legality*

As mentioned in section 4.5.3 of the report, a criminal investigation may be initiated for the purpose of preventing crime, even when there is no reasonable suspicion that a crime has or will be committed. The use of AI-based systems for predictive policing therefore does not require the existence of reasonable suspicion. While every investigative method used in a criminal investigation must contribute – to a certain degree in objective terms – to the goal of investigation (see 4.5.1), this broad and abstract safeguard has not led to any concrete level of protection in practice.

The lack of an objective justification for the use of predictive policing has led to some scholarly discussion, particularly in relation to the risk of unequal treatment (including ethnic profiling) and legal certainty.[98] According to Amnesty International, the absence of a requirement for reasonable suspicion for the

[94] Stevens and others (n 10).

[95] 'Nederland, Maak Een Einde Aan Gevaarlijke Politie-Experimenten Met Massasurveillance' (n 76).

[96] Prins (n 79).

[97] See e.g., Stevens and others (n 10); Prins (n 79).

[98] ibid.

justification of the use of an AI-based system, is one of the reasons why such systems are seen as indiscriminate mass surveillance instruments.[99] Das and Schuilenburg posit that this legal regime results in a situation in which every citizen is a potential suspect for AI-based predictive policing systems, regardless of the existence of any specific factual circumstances that would justify placing a person under an investigation.[100] In a similar vein, Stevens, Hirsch Ballin, Galič et al. point out how the lack of the requirement of reasonable suspicion could be problematic in relation to the presumption of innocence.[101] The prediction resulting from AI-based systems used without objective grounds, which leads to the use of further investigative methods, namely entails an implicit judgement of guilt on the part of the person who has to undergo repressive state actions. This risk would be mitigated by requiring that the grounds for any investigative activity are to a certain extent based on objective factors.

## 5 Conclusion

Based on our examination of predictive policing practices employing AI-based techniques, it is clear that the Netherlands stands at the forefront of using such technologies, at least in Europe. For instance, CAS, a predictive policing tool, which employs machine learning, is already being deployed nation-wide. The question that emerges is, whether these practices are properly regulated in the law, offering adequate protection of the fundamental rights of persons. Put differently by paraphrasing the ECtHR: a country that wishes to stand at the forefront of the development and deployment of new investigatory technologies, also needs to stand at the forefront of human rights protection.[102] Unfortunately, the regulation of predictive policing is lagging behind in the Netherlands. No specific legal basis exists for its use, including in cases, when AI-based tools are used. Instead, the police rely on a very general legal basis relating to the daily police task, as found in the Police Act and the Police Data Act (a law that has implemented the EU Law Enforcement Directive on data protection). This legal basis essentially offers no safeguards and limitations on the use of predictive policing techniques, even when these employ complex AI-based systems. Fundamental rights and general principles of law also remain largely ineffective, offering few protections in practice. Consequently, (AI-based) predictive policing projects take place in general obscurity and with little accountability.

[99] 'Nederland, Maak Een Einde Aan Gevaarlijke Politie-Experimenten Met Massasurveillance' (n 76).

[100] Das and Schuilenburg (n 8).

[101] Stevens and others (n 10).

[102] See S. and Marper v. UK, para. 112 (n 46).

## II. PREDICTIVE JUSTICE: THE EXAMPLE OF OXREC

### 1. Introduction

While there is no all-encompassing definition of predictive justice in the Netherlands, most definitions share the following elements: the use of (1) analytical techniques across (2) datasets with the goal to (3) inform decision-making processes at different stages of the criminal justice system, including sentencing, release, parole, and probation.

To the best knowledge of the authors, AI-based systems are as yet not used for predictive justice purposes in the Netherlands, nor do any such plans exist for the future. There is also no public debate in the Netherlands on the use of such systems for predictive justice. However, actuarial risk assessment tools, which function on the basis of statistics, are being used in the predictive justice domain, especially by the Dutch Probation Services. Since actuarial risk assessment tools are a predecessor of AI-based systems, an examination of the use of such a system can tell us something about the standards and requirements for legal decision-making aided by technology in the criminal justice domain. This might offer some indications as to why AI-based systems are not being employed at the moment, and the types of requirements, if they were to be deployed in the future. For this reason, we briefly explore in this section the example of OxRec, an actuarial risk assessment tool for reoffending used by the Dutch Probation Service.

### 2. The use and perception of OxRec in the Netherlands

Since 2019, the Oxford Risk of Recidivism Tool (OxRec) has been used by the Dutch Probation Services to provide a probability score for reoffending (according to prespecified low [< 30%], medium [30%-50%] and high categories [≥50%]) and violent reoffending (according to prespecified low [< 10%], medium [10%-30%] and high categories [≥30%]). OxRec is part of the 'Risk Assesments Scales'-instrument (RISc), a diagnostic tool of the Probation Services, which assesses the offender's likelihood of reconviction, provides the criminogenic needs of offenders, and allows probation officers to formulate supervision plans.[103] OxRec integrates static variables with dynamic criminogenic risk factors that allow for mutable risk scores. It treats each case (i.e., offender) alike by using the same set of variables that are statistically correlated with (violent) reoffending, whether static or dynamic. As

[103] RISC: Gestructureerde Basis Voor Reclasseringsadviezen' (Reclassering Nederland) <https://www.reclassering.nl/over-de-reclassering/wat-wij-doen/risc> accessed 14 January 2022; LM van der Knaap and DL Alberda, 'De predictieve validiteit van de Recidive Inschattingsschalen (RISc)' (WODC 2009).

such, OxRec is a traditional risk assessment tool, rather than a machine learning AI-based system.

OxRec is used as an addition to professional judgement, thus keeping humans 'in the loop'.[104] In practice, the probation officer makes an individual estimate of the risk of recidivism in a specific case in addition to OxRec, because individual factors and circumstances might need to be considered. The probability score reached through OxRec is then used to inform (in the form of an advice) the decisions of judges and public prosecutors in individual cases. Judges are, however, free to take decisions that differ from the advice.

OxRec was developed by University of Oxford, and externally validated in Sweden[105]106 and the Netherlands.[107] The Dutch tool is based on research, which consists of an analysis of 9072 released convicts and 6329 persons on probation in the period 2011-2012. The sample was almost exclusively male, with the median age of 30 in the prison sample and 34 in the sample of persons on probation.[108]

### a. OxRec from a technological perspective

OxRec was developed using a prespecified protocol, which outlined how the different predictor variables would be tested and categorised before any statistical analyses were conducted.[109] A prediction using OxRec can be completed in 5-10 minutes by using the collected predictors and inserting them in an online calculator that can be used freely by criminal justice professionals.[110] The weight of particular predictors and the way in which they are combined to create a probability score has

[104] Marjolein Maas, Ellen Legters and Seena Fazel, 'Professional en risicotaxatie- instrument hand in hand' (2020) 95 Nederlands Juristenblad 2055; Van den Berg, C., Bruggeman, M., Houston, R., Joosten, A., & Harte, JM. (2021). Validatiestudie risico- en beschermende factoren van de RISC: Een evaluatieonderzoek naar de leefgebieden van het risicotaxatie en adviesinstrument van de 3RO <https://www.researchgate.net/publication/355965668_Validatiestudie_risico-_en_beschermende_factoren_van_de_RISC_Een_evaluatiestudie_naar_de_leefgebieden_van_het_risicotaxatie_en_adviesinstrument_van_de_3RO> accessed 15 January 2022.

[105] Zheng Chang and others, 'Psychiatric Disorders and Violent Reoffending: A National Cohort Study of Convicted Prisoners in Sweden' (2015) 2 The Lancet Psychiatry 891; Seena Fazel and others, 'OxRec Model for Assessing Risk of Recidivism: Ethics – Authors' Reply' (2016) 3 The Lancet Psychiatry 809.

[106] Zheng Chang and others, 'Psychiatric Disorders and Violent Reoffending: A National Cohort Study of Convicted Prisoners in Sweden' (2015) 2 The Lancet Psychiatry 891; Seena Fazel and others, 'OxRec Model for Assessing Risk of Recidivism: Ethics – Authors' Reply' (2016) 3 The Lancet Psychiatry 809.

[107] Seena Fazel and others, 'Prediction of Violent Reoffending in Prisoners and Individuals on Probation: A Dutch Validation Study (OxRec)' (2019) 9 Scientific Reports 841.

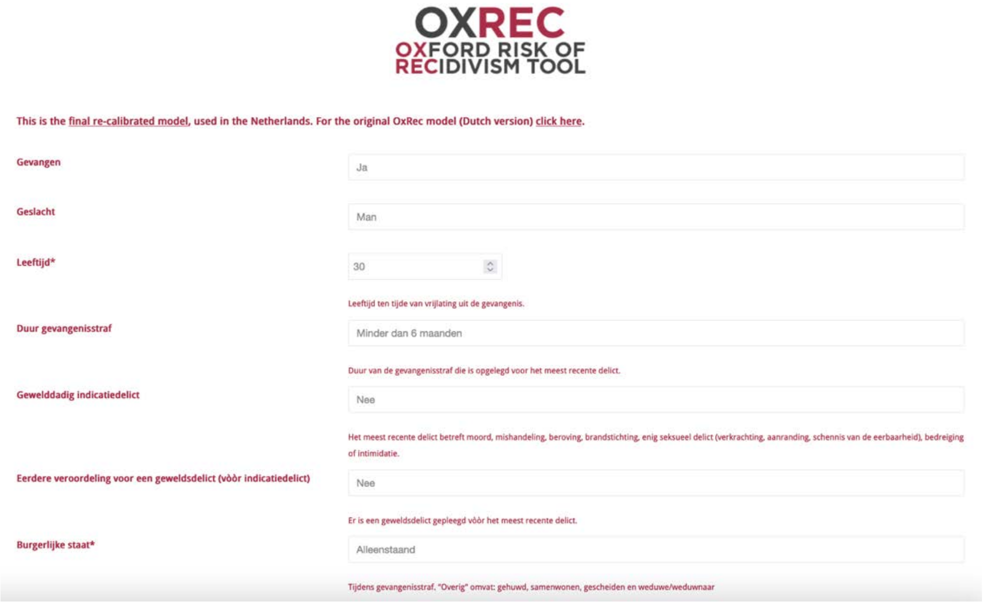
[108] ibid.

[109] ibid.

[110] See 'OxRisk: Oxford Risk of Recidivism Tool' <https://oxrisk.com/oxrec-nl-2-backup/> accessed 14 January 2022.

been published, and can be accessed publicly, making OxRec a fully transparent risk prediction model.

OxRec uses a range of variables, including sex, age, length of incarceration, civil status, education, employment, alcohol or drug use, violent offence, deprivation, and mental illness. Violent offences include homicide, assault, robbery, arson, sexual offences (rape, sexual coercion, child molestation, indecent exposure or sexual harassment), illegal threats or intimidation.[111] Socio-economic deprivation is defined via a standardised, normalised score, including rates of welfare recipiency, unemployment, poor education, crime rates and the median income in an individual's residential area.[112]



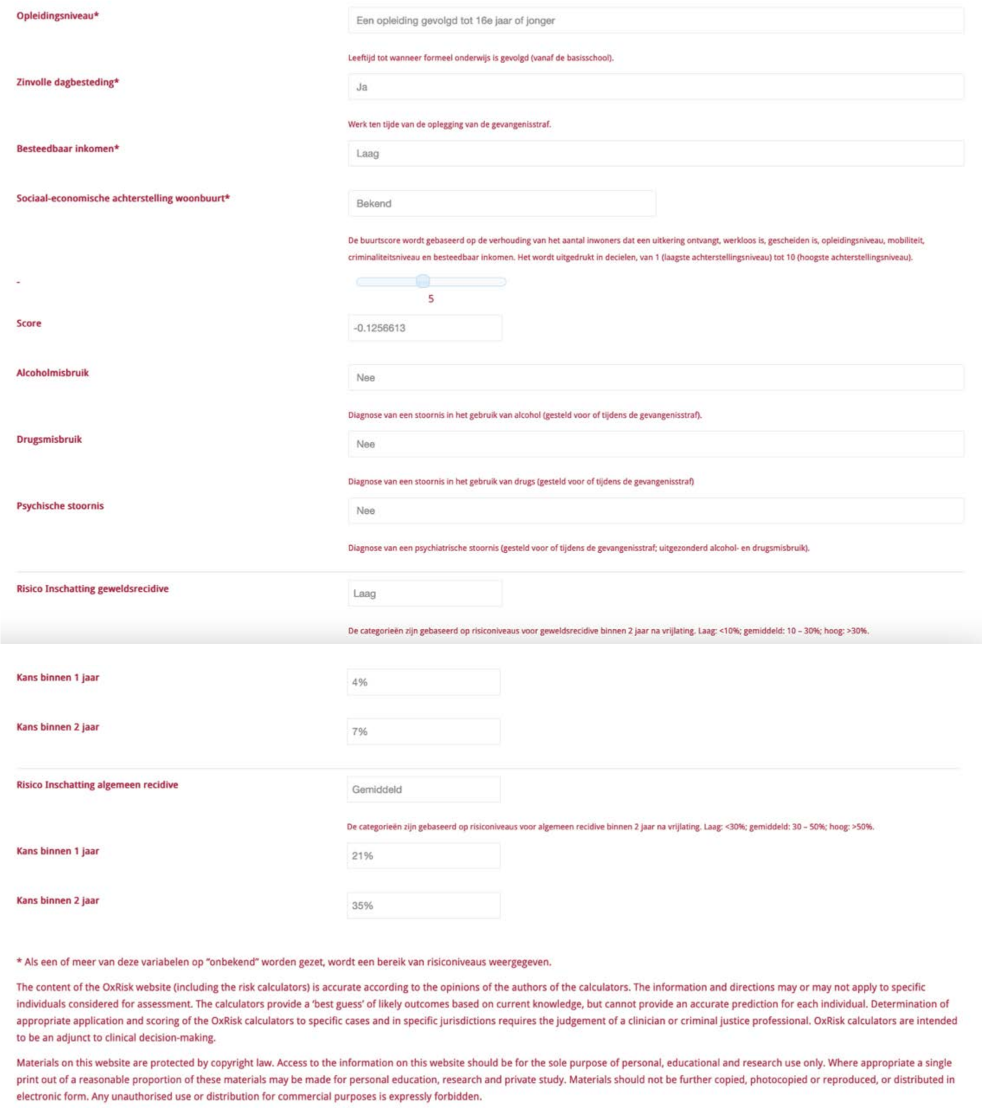
OXREC
OXFORD RISK OF
RECIDIVISM TOOL

This is the final re-calibrated model, used in the Netherlands. For the original OxRec model (Dutch version) click here.

| | |
|---|---|
| Gevangen | Ja |
| Geslacht | Man |
| Leeftijd* | 30<br>Leeftijd ten tijde van vrijlating uit de gevangenis. |
| Duur gevangenisstraf | Minder dan 6 maanden<br>Duur van de gevangenisstraf die is opgelegd voor het meest recente delict. |
| Gewelddadig indicatiedelict | Nee<br>Het meest recente delict betreft moord, mishandeling, beroving, brandstichting, enig seksueel delict (verkrachting, aanranding, schennis van de eerbaarheid), bedreiging of intimidatie. |
| Eerdere veroordeling voor een geweldsdelict (vòòr indicatiedelict) | Nee<br>Er is een geweldsdelict gepleegd vòòr het meest recente delict. |
| Burgerlijke staat* | Alleenstaand<br>Tijdens gevangenisstraf. "Overig" omvat: gehuwd, samenwonen, gescheiden en weduwe/weduwnaar |

[111] ibid.

[112] Seena Fazel and others, 'Factsheet: Oxford Risk of Recidivism Tool (OxRec)' (Risk Management Authority, 2019) <https://www.rma.scot/wp-content/uploads/2019/08/RATED_OxRec_July-2019_Hyperlink-Version.pdf> accessed 14 January 2022; Chang and others (n 4).



| | |
|---|---|
| Opleidingsniveau* | Een opleiding gevolgd tot 16e jaar of jonger |
| | Leeftijd tot wanneer formeel onderwijs is gevolgd (vanaf de basisschool). |
| Zinvolle dagbesteding* | Ja |
| | Werk ten tijde van de oplegging van de gevangenisstraf. |
| Besteedbaar inkomen* | Laag |
| Sociaal-economische achterstelling woonbuurt* | Bekend |
| | De buurtscore wordt gebaseerd op de verhouding van het aantal inwoners dat een uitkering ontvangt, werkloos is, gescheiden is, opleidingsniveau, mobiliteit, criminaliteitsniveau en besteedbaar inkomen. Het wordt uitgedrukt in decielen, van 1 (laagste achterstellingsniveau) tot 10 (hoogste achterstellingsniveau). |
| - | 5 |
| Score | -0.1256613 |
| Alcoholmisbruik | Nee |
| | Diagnose van een stoornis in het gebruik van alcohol (gesteld voor of tijdens de gevangenisstraf). |
| Drugsmisbruik | Nee |
| | Diagnose van een stoornis in het gebruik van drugs (gesteld voor of tijdens de gevangenisstraf) |
| Psychische stoornis | Nee |
| | Diagnose van een psychiatrische stoornis (gesteld voor of tijdens de gevangenisstraf; uitgezonderd alcohol- en drugsmisbruik). |
| Risico Inschatting geweldsrecidive | Laag |
| | De categorieën zijn gebaseerd op risiconiveaus voor geweldsrecidive binnen 2 jaar na vrijlating. Laag: <10%; gemiddeld: 10 – 30%; hoog: >30%. |
| Kans binnen 1 jaar | 4% |
| Kans binnen 2 jaar | 7% |
| Risico Inschatting algemeen recidive | Gemiddeld |
| | De categorieën zijn gebaseerd op risiconiveaus voor algemeen recidive binnen 2 jaar na vrijlating. Laag: <30%; gemiddeld: 30 – 50%; hoog: >50%. |
| Kans binnen 1 jaar | 21% |
| Kans binnen 2 jaar | 35% |

* Als een of meer van deze variabelen op "onbekend" worden gezet, wordt een bereik van risiconiveaus weergegeven.

The content of the OxRisk website (including the risk calculators) is accurate according to the opinions of the authors of the calculators. The information and directions may or may not apply to specific individuals considered for assessment. The calculators provide a 'best guess' of likely outcomes based on current knowledge, but cannot provide an accurate prediction for each individual. Determination of appropriate application and scoring of the OxRisk calculators to specific cases and in specific jurisdictions requires the judgement of a clinician or criminal justice professional. OxRisk calculators are intended to be an adjunct to clinical decision-making.

Materials on this website are protected by copyright law. Access to the information on this website should be for the sole purpose of personal, educational and research use only. Where appropriate a single print out of a reasonable proportion of these materials may be made for personal education, research and private study. Materials should not be further copied, photocopied or reproduced, or distributed in electronic form. Any unauthorised use or distribution for commercial purposes is expressly forbidden.

*Image 1: A screenshot of the Dutch version of the online OxRec tool (source: <https://oxrisk.com/oxrec-nl-2-backup/> accessed 13 January 2022)*

### b. The political and socio-economic incentives for using OxRec

There is a strong belief in the Netherlands that experimenting with new technologies can improve government efficiency. This includes the idea that crime would be further reduced, if offenders who are more likely to violate the law in the future are given a fitting punishment, including effective probation conditions, is important to prevent reoffending. There is also a strong belief that new digital systems lead to rational, scientific and value-neutral ways to generate knowledge and expertise within the criminal justice domain. They are seen as making sentencing more accountable by protecting it against human bias and curbing discriminatory and racist sentencing practices.[113]

Within this broader context, the Dutch Probation Services see OxRec as a way of improving their task of informing the decisions of judges and public prosecutors in individual cases. According to the Probation Services, research shows that statistical prediction methods are more accurate than clinical procedures. Moreover, professionals' biases can be reduced if they receive feedback on their decisions and can learn whether their estimate was correct (based on follow-up assessment of recidivism data) or not.[114]

### c. Reliability, impartiality and equality of OxRec

The evaluation of OxRec for the Netherlands was done in 2019 by Oxford University. A total national sample of all offenders in the Netherlands from 2011–2012 (9072 people in prison and 6329 individuals on probation) was followed up for violent and other reoffending over two years. The study concluded that a calibrated model for OxRec can be used in the Netherlands both for individuals released from prison and individuals on probation to stratify their risk of future violent and other types of reoffending. According to the external validation in Sweden and the Netherlands, the probability score of OxRec is relatively precise.[115]

Nevertheless, Dutch scholars have expressed concern with the inclusion of various socio-economic variables, such as income, education, employment and neighbourhood, for the prediction of recidivism through OxRec. These variables are namely correlated with bias in terms of race, class, or other forms of social disadvantage.[116] As such, socio-economic variables are seen as an indicator of

[113] See Sharad Goel, Justin M Rao and Ravi Shroff, 'Personalized Risk Assessments in the Criminal Justice System' (2016) 106 American Economic Review: Papers & Proceedings 119; Rik Peeters and Marc Schuilenburg, 'Machine Justice: Governing Security through the Bureaucracy of Algorithms' (2018) 23 Information Polity 267; Rik Peeters and Marc Schuilenburg, 'The Algorithmic Society: An Introduction' in Marc Schuilenburg and Rik Peeters (eds), The Algorithmic Society (Routledge 2021).

[114] Maas, Legters and Fazel (n 2).

[115] ibid.

[116] See e.g., Bernard E Harcourt, Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age (The University of Chicago Press 2006); Derek W Braverman and others, 'OxRec Model for Assessing Risk of Recidivism: Ethics' (2016) 3 The Lancet Psychiatry 808; Kelly Hannah-Moffat, 'A Conceptual Kaleidoscope: Contemplating "Dynamic Structural Risk" and an Uncoupling of Risk from Need' (2016) 22 Psychology, crime and law 33; Michael Tonry, 'Predictions of Dangerousness in Sentencing: Déjà Vu All Over Again' (2019) 48 Crime and Justice 439; Gwen van Eijk, 'Inclusion and Exclusion Through Risk-

individual criminogenic risk, decontextualising the offender's risk of recidivism from broader social, political, economic and historical disadvantages that are often correlated with such variables. Consequently, they can reproduce and magnify bias. Furthermore, several authors have pointed out that this is particularly problematic given the fact that 'socially marginalized individuals are overrepresented in Western criminal justice systems, even in relatively equal societies such as the Netherlands.'[117]

This criticism on the use of socio-economic variables in OxRec has led to a response from the authors of the OxRec evaluation for the Netherlands in combination with the Dutch Probation Services,[118] and the Minister of Justice.[119] They argue in a similar vein that OxRec has key advantages over many other instruments, including a transparent methodology, prespecified protocol and a large representative sample to develop the tool. Furthermore, they have stated that the socio-economic variables amount to a relatively weak risk factor and that the effect of changing individual risk factors can clearly be seen by using the system. In fact, the exclusion of socio-economic variables would render 'the tool weaker (and possibly inadequate) in terms of prediction, but it would be discriminatory because it would, in the case of sex for example, predict that women have higher risk than they really have, and by underestimating risk in men, lead to higher false-negative rates.'[120]

## 3. The normative framework for predictive justice

### a. The legal framework concerning the use of OxRec

Considering the fact that AI-based systems are currently not used for purposes of predictive justice, it is not surprising that legal rules specifically governing the use of such systems are also lacking. However, even when it comes to the use of statistical algorithmic systems like OxRec, which are being used, legal rules are scarce.

Based Justice: Analysing Combinations of Risk Assessment from Pretrial Detention to Release' (2020) 60 The British Journal of Criminology 1080; Gijs van Dijck, 'Algoritmische risicotaxatie van recidive: over de Oxford Risk of Recidivism tool (OXREC), ongelijke behandeling en discriminatie in strafzaken' (2020) 95 Nederlands Juristenblad 1784.

[117] Gwen van Eijk, 'Algorithmic Reasoning: The Production of Subjectivity through Data' in Marc Schuilenburg and Rik Peeters (eds), The Algorithmic Society (Routledge 2020) 123.

[118] Fazel and others, 'OxRec Model for Assessing Risk of Recidivism' (n 3); Maas, Legters and Fazel (n 2).

[119] 'Antwoorden Kamervragen over Twijfels Gebruik Risicotaxatie-Instrument Vanwege Gevaar Voor Etnisch Profileren' (Ministerie van Justitie en Veiligheid, 2020) <https://www.rijksoverheid.nl/documenten/kamerstukken/2020/08/18/antwoorden-kamervragen-over-twijfels-gebruik-van-een-bepaald-risicotaxatie-instrument-bij-de-reclassering-vanwege-het-gevaar-op-etnisch-profileren> accessed 14 January 2022.

[120] Fazel and others, 'OxRec Model for Assessing Risk of Recidivism' (n 3) 810.

One of the reasons for this is that OxRec operates in the sphere of sentencing. The Dutch legal system is characterised by a very large discretion left to the judge to decide on the appropriate sentence in a particular case, something which is not regulated in the law at all (aside from rules on the maximum sentence prescribed in the law for particular crimes). This means that it is completely up to judges to choose, whether they will rely on the prediction made by OxRec and, if so, in which way they will make use of it.[121] Research shows that judges generally do not blindly follow the OxRec probability score, but tend to use it alongside their own assessment of the recidivism risk to decide, whether a sentence will be conditional or unconditional, and which (if any) conditions are appropriate during the probation period.[122] It has been suggested that this is why judges are not particularly concerned about the reliability of such systems.[123]

The use of OxRec by the Dutch Probation Services is also not regulated by any specific rules. In that regard Dutch law does not ensure the accurate use of such systems or minimizing the risks of its use; instead, a responsible and reliable use of such systems within the rule of law is sought by ensuring the quality of the technological system as such.[124]

### b. Case law

While OxRec is commonly used in the reports by Probation Services, informing the decision-making of criminal judges, there are no legal decisions on the use of the system as such. However, there are a few civil law judgments concerning the use of an automated decision-making system by a government body. One particular case by the Dutch Supreme Court is worth mentioning in the context of predictive justice.

In this case, a government body had valued the price of land for the purpose of collecting a particular tax using an automated decision process.[125] The litigant contested the correctness of the result of this automated process. The Supreme Court formulated a general rule in this case, noting that stakeholders need to be able to verify the correctness of the decision made in the automated process as well as the correctness of the data and the assumptions underlying the process.[126] This rule puts a burden on the governing body to provide for a sufficient level of transparency when it comes to automated decision-making processes. Without this transparency,

[121] Sigrid van Wingerden, Martin Moerings and Johan van Wilsem, Recidiverisico En Straftoemeting (Sdu Uitgevers 2011).

[122] ibid 116.

[123] ibid.

[124] Maas, Legters and Fazel (n 2).

[125] Supreme Court of the Netherlands, judgment of 17 August 2018, ECLI:NL:HR:2018:1316 (case nr. 17/01448).

[126] ibid., para. 2.3.3.

the litigant would namely be confronted with a 'black box' and the relationship between parties would be fundamentally unequal.

### c. Substantive guarantees: transparency and accountability

As already mentioned, the use of OxRec in criminal cases functions in a transparent way. The use of the system is described in the report of the Probation Services and the report itself is accompanied by a text elaborating on the way to interpret the result. On the basis of provisions in the Dutch Code of Criminal Procedure (Articles 33 and 51b), the parties of the proceedings, including the defendant, also have access to the information about the results of OxRec.

There is no specific legal regime for accountability in this context. The only resort would be to file a complaint in a civil court.

### d. General principles of law[127]

#### *i. The right to non-discrimination*

There is some discussion in Dutch academic literature on bias and the risk of discrimination in relation to the criminal justice domain stemming from the use of AI-based systems. Some scholars have suggested that these risks might be countered by measures, such as equating the percentage between false-positives within different groups.[128] However, others have pointed out that this can lead to the prevention of discrimination, but can also mean a loss of effectiveness of the instrument.[129] In the popular media the issue of discrimination has been brought up as well.[130] This led to questions for the Minister of Justice by Members of the Parliament.[131] However, the answer provided by the Minister and the Dutch Probation Service merely stated that ethnicity is not a relevant factor in the OxRec system. Indirect discrimination through for instance the use of socio-economic variable, such as postcodes (discussed in 2.3), was not seen as a problem by the Minister.

[127] We have no findings on the presumption of innocence in the context of predictive justice.

[128] Bart Custers, 'Artificiële intelligentie in het strafrecht: een overzicht van actuele ontwikkelingen' (2021) Computerrecht 330; Johannes Bijlsma, Floris Bex and Gerben Meynen, 'Artificiële intelligentie en risicotaxatie: drie kernvragen voor strafrechtjuristen' [2019] Nederlands Juristenblad 3313.

[129] Mireille Hildebrandt, 'Algometrisch strafrecht: spiegel of echoput. Kunstmatige intelligentie in het strafrecht' (2021) 51 Delikt en Delinkwent 651.

[130] See Kristel van Teeffelen, 'Algoritmes Gebruikt Door Reclassering Zorgen Voor Etnisch Profileren' [2020] Trouw <https://www.trouw.nl/binnenland/algoritmes-gebruikt-door-reclassering-zorgen-voor-etnisch-profileren~b8918776/> accessed 14 January 2022.

[131] 'Antwoorden Kamervragen over Twijfels Gebruik Risicotaxatie-Instrument Vanwege Gevaar Voor Etnisch Profileren' (n 17).

### *ii. The independence of judges and access to a human judge*

A discussion concerning the independence of judges is taking place in relation to the notion of a 'robot judge', an idea that is not yet reality, but that might be relevant in the future.[132] Despite its name, a 'robot judge' is not seen as an automated decision-making system, but rather as an AI-based system used for the purpose of assisting decision-making. This might include the prediction, whether the ECtHR would judge the situation to be in violation of Article 6 or 8 ECHR.[133] In general, the idea of a judge being assisted by an AI-based system is not viewed necessarily as problematic. However, when a judge is steered (that is, when the system's suggestions impair the autonomy of the judicial decision, what is more commonly known as 'automation bias') or even replaced by such a system, this clearly creates an issue regarding the independence of the judge. While this discussion is still in its infancy, the differentiation between assistance and steering of decision-making is a useful starting point.

### *iii. Access to a human judge and the right to appeal*

Concerning the access to a (human) judge, there is scarcely any discussion in the Netherlands concerning. Hildebrandt points out that there are two general paths that can be followed in regard to the right to appeal, which also affects the question of access to a human judge.[134] On the one hand, a broad scope for appeal can be left to a human judge following a decision made by an AI-based system. The other option is to limit the scope to overturn decisions made by an AI-based system, thus also limiting access to a human judge. According to Hildebrandt, the second option has the strong appeal of efficiency as well as protecting the additional value of the AI-based system, such as accuracy. However, limiting the possibility of appeal might also diminish the normative meaning of a judicial decision in criminal cases: the decision is not so much a personal reprimand towards a person, but an automated, impersonal decision.[135] For instance, this might change the character of a criminal sentence: the societal, normative disapproval becomes less visible and the sentence comes to be viewed more like a cost, such as a tax.

Aside from this theoretical discussion by Hildebrandt, the right to access to a court within the scope of Article 6 ECHR might limit or even prohibit the possibility to replace a human judge by an automated decision-making system. If so, even if a

[132] See e.g., Corien Prins and Jurgen van der Rust, 'AI en de rechtspraak: meer dan alleen de 'robotrechter'' (2017) Nederlands Juristenblad 260; Ybo Buruma, 'De toekomst van de strafrechtspraak' (2021) 46 Delikt en Delinkwent 571; Hildebrandt (n 27).

[133] Hildebrandt (n 27).

[134] ibid.

[135] ibid.

decision would be taken by an AI-based system, access to a human judge would still need be guaranteed. Consequently, automated decision-making might not be as effective in practice as is often imagined, leading instead merely to an extra layer of bureaucracy in the decision-making process.[136]

## 4. Conclusion

Based on the information that is publicly available, AI-based systems are as yet not used in the Netherlands for purposes of predictive justice, that is, to provide assistance in the application of the law. However, the Dutch Probation Services do use a traditional actuarial risk assessment tool for the purpose of predicting recidivism, OxRec, which functions on the basis of relatively simple statistical analysis. Despite the fact that the predictions offered by OxRec are understood (or understandable) by humans, this advice comes with an explanation on how the system has reached the prediction and is used as a mere advice to the judge. Moreover, the system is publicly available online and was developed and validated in a transparent manner by scholars in the United Kingdom, Sweden and the Netherlands. There is thus a notable difference between the situation concerning predictive policing and predictive justice. Since we have not conducted any specific research concerning the reasons for this stark difference, we cannot offer any substantiated answers concerning the issue. What we can say on the basis of this report is that decision-making in the domain of criminal justice, which affects the interpretation and application of the law during a trial, requires high standards of transparency, accuracy and fairness, thus posing a significant limit to any future use of ‘black box’ AI-based systems.

[136] ibid.

# III. EVIDENCE LAW

## 1. Introduction

Following the structure of the questionnaire, this part of the report is based on the distinction between evidence *gathered* and evidence *produced* by AI-based systems. However, we argue that such a distinction is misplaced. Contemporary AI-based systems, such as Hansken (described below) that are used to gather evidence in a case also produce data. Criminal investigations nowadays lead to huge data sets composed of multimodal data (i.e., unstructured data of different types, including text, photo, video, audio data). Consequently, traditional tools, developed for searching structured textual data, no longer suffice to find what one is looking for. For this reason, new and more complex AI-based systems needed to be developed. These new tools first need to interpret the data by themselves (e.g., a tool searching for images of drugs needs to be able to determine that a particular photo indeed represents drugs). Second, they need to be able to find relevant correlations (or links) between the numerous data points in the data set (e.g., resulting in a convincing time-line and scenario). This means that we are not dealing with simple gathering of data, but with complex production of data by such systems.

## 2. Gathering evidence through AI-based systems

### a. The example of Hansken

The Netherlands Forensic Institute (NFI) has developed a digital forensic tool called 'Hansken' that can process large volumes of (seized) digital material in order to find relevant data points and the connections between them.[137] Hansken is used by several investigative bodies in the Netherlands, including the Dutch National Police for the purpose of criminal investigation and the Dutch Fiscal Information and Investigation Service for the purpose of fraud detection in tax investigations.[138]

Hansken is used to extract and process data from all types of digital devices, such as laptops, smartphones, hard-disks and even whole servers (e.g., in the case of the seized Ennetcom server).[139] At the moment the tool is said to have the capacity to process three terabytes of data per hour.[140] Hansken includes a wide variety of tools

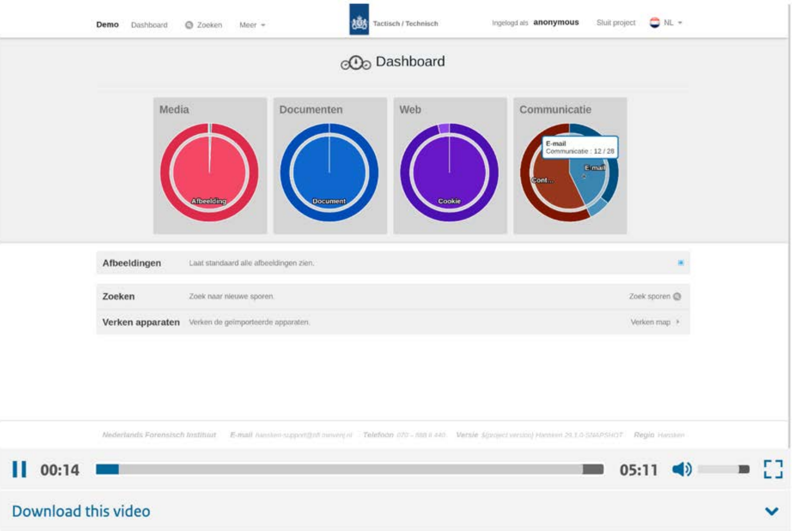
[137] Merve Bas Seyyar and Zeno Geradts, 'Privacy Impact Assessment in Large-Scale Digital Forensic Investigations' (2020) 33 Forensic Science International: Digital Investigation 1, 4.

[138] Other national bodies that use them are: the Netherlands Food and Consumer Product Safety Authority and Human Environment and Transport Inspectorate.

[139] See e.g., 'Dutch Police Seize Encrypted Communication Network with 19,000 Users' (*Reuters*, 22 April 2016) <https://www.reuters.com/article/us-netherlands-cyber-idUSKCN0XJ2HQ> accessed 14 January 2022.

[140] Bas Seyyar and Geradts (n 1) 2.

(software),[141] which can be used to analyse diverse file systems, extract files, carve unallocated space and create full text indexes, parse chat logs, browse history and e-mail databases.[142] These tools can be used to examine various types of structured and unstructured data that may be relevant for the investigation, including text (e.g., names, keywords, phone numbers, chat-messages, e-mails), photos, videos, various types of metadata, and location data.[143]



Afbeeldingen Laat standaard alle afbeeldingen zien.

Zoeken Zoek naar nieuwe sporen.

Verken apparaten Verken de geïmporteerde apparaten.

*Image 1: A screenshot of the Hansken dashboard from the publicly available demo video (source: <https://www.hansken.nl/an-introduction-to-hansken/hansken-demo> accessed 14 January 2022)*

## b. The normative framework for the use of AI-based systems for gathering evidence

### i. *The legal framework*

In the current legal framework, there are no provisions that specifically deal with Hansken or similar AI-based technologies used for the purpose of gathering evidence in criminal investigations. Instead, existing provisions that were developed for the 'analogue' world are used.[144] However, these provisions are few and mainly

[141] Examples of software include: UFED, EnCase, FTK, EXIF, HDFS, Map Reduce, Cassandra, HBase, Elastic Search and Kafka; see Harm van Beek and others, 'Digital Forensics as a Service: Game On' (2015) 15 Digital Investigation 20.

[142] ibid 21.

[143] Bas Seyyar and Geradts (n 1) 4.

[144] Bart Custers and Lonneke Stevens, 'The Use of Data as Evidence in Dutch Criminal Courts' (2021) 29 European Journal of Crime, Criminal Law and Criminal Justice 25, 40.

concern types of evidence admissible in court and very general requirements concerning the lawfulness and reliability of evidence.

Based on the broad wording of Article 339 of the Dutch Code of Criminal Procedure (CCP), almost any type of evidence is admissible in Dutch courts.[145] Nevertheless, when digital data are used as evidence, they are usually submitted in the form of written police statements that report the results of an investigation.[146] Concerning the lawfulness of evidence, Article 359a CCP provides for the possibility to attach consequences to the unlawful gathering of evidence. Depending on the circumstances, the judge can decide to decrease the severity of the punishment, to exclude the evidence or to declare the public prosecutor inadmissible in the prosecution. However, in practice evidence is hardly ever excluded and cases are not negatively affected by unlawfully obtained evidence.[147] As to reliability, Article 359(2) CCP states that when the prosecution or the defence argues that evidence submitted by the other party is unreliable, the judge needs to motivate their rejection of a 'plea against the use of unreliable evidence'.

While the CCP does not contain any concrete provisions concerning the assessment of expert evidence, the Dutch Supreme Court has developed criteria for assessing expert evidence. According to these criteria, if the reliability of expert evidence is disputed, the judge needs to examine whether the expert has the required expertise and, if so, which method(s) the expert used, why the expert considers that these methods are reliable, and the extent to which the expert has the ability to apply these methods in a professional manner.[148] Yet, Dutch courts (so far) have ruled that in relation to the use of Hansken there can be no reference to expertise, so that the data gathered with – or, rather, produced through – Hansken is not considered as expert evidence.[149] The only resort left to the defence to examine the reliability of the Hansken system is to request the investigatory judge to appoint an expert (according

[145] The provision lists the following types of evidence, which are admissible in court: what the judge perceives on their own, statements by suspect, statements by witnesses, statements by an expert, and written documents.

[146] Custers and Stevens (n 8) 36.

[147] ibid 36–37. This is due to a very restricted interpretation of Article 359a stemming from the case law of the Dutch Supreme Court. See, e.g., Supreme Court of the Netherlands, judgment of 19 February 2013, NJ 2013, 308.

[148] Supreme Court of the Netherlands, judgment of 27 January 1998, NJ 1984, 404; see also Custers and Stevens (n 8) 36.

[149] See e.g., District Court of Amsterdam, judgment of 19 April 2018, ECLI:NL:RBAMS:2018:2504 (case nr. 13/997097-16), para. 7.3.

to Article 227 CCP), who would provide information on the functioning of Hansken.[150]

There are hardly any content-related changes concerning evidence law in the latest version of the draft new Dutch Code of Criminal Procedure (draft CCP). Two developments, however, merit mentioning.

First, the draft CCP introduces a new provision, according to which the public prosecutor may order companies or institutions, which can 'reasonably be suspected of having access to certain data' relevant for the investigation, to process these data and then submit the result of this processing to law enforcement (Article 2.7.51(1) draft CCP). Google, Facebook and Apple are given as examples of companies that may be asked to perform such processing.[151] Simple types of processing of data needed to provide information (e.g., first finding a customer number in one system, and then using that customer number to find the name and address data in another system) do not fall under this provision (this is covered by the classic disclosure order). Instead, the legislator had a more complex type of processing in mind, where the analysis of data would lead to the creation of new data, thus potentially including analysis performed by AI:

> 'The power in this Article concerns operations that go beyond multiple searches, for example comparing all data in one dataset with all data in another dataset, in order to identify data that appear in both sets. The main feature of this power, which is distinct from the normal supply of data, is that the operation produces "new" data which are then supplied.'[152]

According to the Explanatory Memorandum, the idea behind this provision is to protect the private life of individuals. This provision namely enables the limitation of the amount of data that is provided to law enforcement. As such, the police only receive the results of the data analysis performed by a company that collects the data.[153] However, another, more practical goal is clearly sought through this provision: limiting the influx of data for the police. By ordering certain third parties to perform the initial 'sifting' through data, the police receive a lesser amount of data

[150] See e.g., District Court of Amsterdam, intermediate decision of 29 September 2020, ECLI:NL:RBAMS:2020:4764 (case nr. 26Marengo), p 16; District Court of Amsterdam, intermediate decision of 17 November 2020, ECLI:NL:RBAMS:2020:5585 (case nr. case nr. 26Marengo), p. 7.

[151] 'Ambtelijke Versie Juli 2020 Memorie van Toelichting Wetboek van Strafvordering' (Ministerie van Justitie en Veiligheid, 30 July 2020) 442 <https://www.rijksoverheid.nl/documenten/publicaties/2020/07/30/ambtelijke-versie-juli-2020-memorie-van-toelichting-wetboek-van-strafvordering> accessed 14 January 2022.

[152] ibid 443.

[153] ibid 441.

already considered relevant. In this sense, the new provision aims at enhancing the efficiency of police work (this provision is further discussed in 3.2.4).[154]

The second development in the draft CCP, is the introduction of a special 'technical tool' (*technisch hulpmiddel*) assisting the investigatory judge in his task to sift the data protected by the legal professional privilege (LPP) out of the data set relevant for the criminal investigation. While not mentioned explicitly in the Explanatory Memorandum, this tool is understood as an AI-based system and is seen as a solution to the lack of practical resources and expertise of the investigatory judge to sift out privileged data from large digital data sets. A lot of trust is placed into this tool.[155] In the Explanatory Memorandum it is, for instance, assumed that the tool will enable the sifting of LPP-data, where the person conducting the sifting via the tool would not gain any knowledge into the LPP-data. This would allow the investigating officer to conduct the sifting, instead of the investigatory judge, who is the only authority that may gain knowledge of LPP-data (Art. 2.7.65(4) draft CCP).

However, the Explanatory Memorandum does not include much discussion of the actual functioning of this tool and whether this would actually be possible from a technical perspective. According to the Explanatory Memorandum, the functioning of the tool is very crude: the investigatory judge and officers compose a list of search terms, which can include telephone numbers and email addresses of a lawyer. On this basis, the tool would then sift out certain protected data. However, as Stevens and Galič point out, it remains completely unclear, how the tool will be able to determine, which communications stemming from this telephone number or email are actually protected by LPP.[156] Not every communication between a client and his lawyer (or a doctor), is namely protected by the privilege (e.g., a discussion about the Tour de France between the two would not fall under the privilege). On the basis of this description, the tool is likely to lead to a large number of false positives and false negatives.

### *ii. Case law and defence rights: access to the data set, to the AI-tool and information concerning the functioning of the AI-tool*

There are no provisions in the law (or lower types of legal instruments), which oblige the prosecution to provide the defence with information about a particular AI-based system used to gather evidence. Consequently, the case law of Dutch courts plays a key part in the development of defence rights in the context of gathering (in fact,

[154] ibid 442.

[155] See Lonneke Stevens and Maša Galič, 'Bescherming van Het Professionele Verschoningsrecht in Geval van Doorzoeking van Een Smartphone: Het EHRM Eist Een Concrete Basis En Een Praktische Procedurele Regeling in Het Recht' (2021) 70 Ars Aequi 845.

[156] ibid 851.

producing) data through AI-based systems. Since 2018, there has been a surge of court cases concerning cryptophones (phones that use encryption for the purpose of anonymous communication), in which the Hansken system has been used in order to gather evidence from huge digital data sets. In 2016, a whole server was seized by the Dutch police in order to access the content of encrypted communications ('Ennetcom cases'). And in 2020, the EncroChat cryptophones of more than 30.000 users were hacked by the French police, acting in cooperation with the Dutch police ('EncroChat cases').

Dutch courts are generally rather reluctant to request information on the functioning of Hansken from the NFI or to provide such information to the defence. Courts also quickly reject motions questioning the reliability of the functioning of Hansken (and the evidence gathered through it) from the defence. In general, Dutch judges seem to consider that the functioning of this AI-based system is unproblematic. For instance, the Amsterdam court stated in a 2018 judgment, that Hansken was merely used in order to *view* (not even to gather) the evidence already collected, so that no specific legal basis is needed for its use.[157] Judges also seem to have a largely uncritical belief into the proper functioning of Hansken, perhaps related to the fact that the system has been developed 'in house', rather than by a private actor with commercial interests in mind. This 'presumed correctness' can be seen in a judgment by the Gelderland court, which ruled with very brief reasoning that the incompleteness of the results due to a software update, had no bearing on the integrity of the results and that the defence did not manage to prove otherwise.[158] Such attitude of the judges has important consequences, as it reduces the possibility of the defence to question and test the reliability of evidence gathered in this way.

Nevertheless, based on Article 182 CCP, the defence has the possibility to request the investigatory judge to carry out certain additional investigative acts. This general provision is in principle broad enough so as to enable the defence to propose their own search terms for the purpose of sifting through the data set with Hansken, as well as to request access to the data set and Hansken itself.[159] Dutch courts have already recognised the right of the defence to propose additional search terms, with which the prosecution will then search the whole data set (where the court reserves

[157] District Court of Amsterdam, judgment of 19 April 2018, ECLI:NL:RBAMS:2018:2504 (case nr. 13/997097-16), para. 7.3.

[158] District Court of Gelderland, judgment of 26 June 2019, ECLI:NL:RBGEL:2019:2833 (case nr. 05/780092-17), p. 9.

[159] In the Ennetcom-Tandem case (District Court of Amsterdam, judgment of 19 April 2018, ECLI:NL:RBAMS:2018:2504, para. 7.3), the Amsterdam court stated that the defence had the possibility to expand the Tandem data set by asking the investigatory judge to approve additional search terms (but the defence did not make use of this possibility).

the right to assess, whether the proposed search terms are of sufficient relevance).[160] In this context, it should be noted that in Dutch law, it is for the prosecution generally to determine what information is relevant in the case. Only this information will then form part of the case file (Article 149a CCP) and be made available to the defence (Arts. 30-34 CCP).[161] While the defence can request the prosecutor to add information to the case file (Art. 34 CCP; e.g., by proposing additional search terms, with which a data set is to be searched), the prosecutor – with approval from the investigatory judge – may deny this request, if they consider it unsubstantiated. However, substantiating such a request can be a difficult task for the defence when it comes to huge data sets. After all, such data sets are comprised of hundreds of thousands (or even millions) of data points, stemming from numerous persons, so that specifying what one is looking for might be compared to looking for a needle in a haystack. Thus, if the requirement to substantiate such a request is set too high, the defence may be largely excluded from participating in the process of determining what is relevant in the case (this issue and the requirements of Art. 6 ECHR are further discussed in section 2.3).

In order for the defence to participate in this process, direct access to both the data set as well as to Hansken is thus desirable. However, according to Art. 182(3) CCP this request needs to be justified. While the law itself does not specify how precise this justification needs to be, Dutch courts generally require rather concrete specification of what the defence is looking for and why. Initially, requests for access by the defence – both to the data set and the Hansken tool itself – were rejected by courts, considered to be mere 'fishing expeditions.'[162] This began to change in 2021, with courts recognising that the defence needs to be afforded with the opportunity not only to examine the evidence against the defendant, but also to search for exculpatory evidence in the data set gathered by the prosecution. Nevertheless, Dutch courts still grant different scopes of access to the secondary data set (that is, the data set resulting from the initial searches with the search terms proposed by the prosecution and the defence in the full data set gathered in the case) to the defence. Some courts still deny access to this data set, considering that the request of the defence for such access was not substantiated enough.[163] Other courts either grant

[160] See e.g., Court of Appeal Amsterdam, intermediate decision of 8 July 2020, ECLI:NL:GHAMS:2020:1904 (case nr. 23-002697-19), p. 13.

[161] This arrangement will not change much in the modernisation process of the CCP. The provisions regulating this are still based on the assumption that we are dealing with physical (i.e., paper) documents, which include findings including the reporting and interpretation of a selection of those data, rather than digital data sets themselves.

[162] See e.g., Court of Appeal Amsterdam, judgment of 14 December 2018, ECLI:NL:GHAMS:2018:4620 (case nr. 23-00107717), section 8 (concerning a large data set gathered through the means of a key-logger).

[163] See e.g., District Court of The Hague, judgment of 25 August 2021, ECLI:NL:RBDHA:2021:9368 (case nr. 09/095750-21).

access to those messages and other data directly pertaining to the accused person, or the whole secondary data set to which the prosecution has access.[164] Nevertheless, based on case law from 2018 to 2021, it seems that with time, courts are granting broader access to the secondary data set to the defence.

Another issue concerns the *form* of the access to the secondary data set. Again, courts are granting different types of access, something which is also changing with time. Defence lawyers are generally provided with an Excel and/or PDF file with the relevant data. In addition, courts increasingly grant access to the same data set via Hansken, but this can only take place during a scheduled appointment at the Netherlands Forensics Institute. According to the prosecution, this limitation is due to practical considerations, which is planned to change in the near future, therefore granting access to defence lawyers to the data set with the use of Hansken via their own computers (something that should indeed be possible, considering that Hansken functions as a cloud-based service).[165]

Hansken, which was developed with the values of security and transparency in mind, also provides for automatic logging of activity while searching for evidence in the mass of data. As such, it would be fairly easy – at least from a technological perspective – to grant the defence (or an expert acting on behalf of the defence) access to these logging data in order to check, whether the prosecution's search activity was done in accordance with the law (e.g., whether they also gathered exculpatory evidence, and whether the system was functioning properly). This right has, however, not yet been granted to the defence.

### c. Legal commentary

There is quite some discussion among Dutch scholars on the way Hansken, and similar AI-based system for the gathering of evidence, affect the right to a fair trial, especially equality of arms. Scholars generally argue for broader access of the defence to the gathered data set (in particular, the secondary data set, which is the

[164] See e.g., District Court of Rotterdam, intermediate decision of 25 January 2021, ECLI:NL:RBROT:2021:396; District Court of Rotterdam, intermediate decision of 15 July 2021, ECLI:NL:RBROT:2021:6853, para. 4; District Court of Amsterdam, intermediate decision of 1 April 2021, ECLI:NL:RBAMS:2021:1507 (case nr. 26Marengo); District Court of Rotterdam, intermediate decision of 25 June 2021, ECLI:NL:RBROT:2021:6113.

[165] The NFI are already working on this possibility, as presented by Hans Henseler and Harm van Beek, 'Hands-on with Hansken' (Bijzonder Strafrecht Cybercrime Congres, Den Haag, 3 December 2021) <https://www.hansken.nl/latest/news/2021/12/08/hands-on-with-hansken-at-the-cybercrime-congress-2021> accessed 14 January 2022.

result of the initial search of the full data set searched with the AI-tool) and to the AI-tool itself.[166]

On the basis of recent case law of the ECtHR concerning large data sets and Article 6 ECHR,[167] Galič argues that the defence is entitled to broad access to the secondary data set, without a strict requirement to justify such access. While the defence generally needs to justify any further search activity it is requesting (so as to prevent fishing expeditions), the particular context of huge data sets calls for a looser standard. When searching an enormous data set with millions of data points, one generally does not – in fact, cannot – know what one is searching for until they actually find it. In the case of the Ennetcom server, which contained data of about 19.000 users (at least some of whom might in some way be related to the accused), the accused simply could not have a proper idea of what might be found there. A requirement to specify what is being searched for would thus severely underestimate the complexities of analysing huge and interconnected amounts of data. It also does not offer the defence a comparable opportunity to that of the prosecution, which can search this data set repeatedly in order to refine their search terms; that is, in order to refine what exactly they are looking for. This has a serious effect on the principle of equality of arms.[168]

Scholars also argue that the defence should have access to the AI-tool itself, as they can hardly efficiently and effectively search the data set without it. As such, adequate access to the secondary data set must include access to the tool. Schermer and Oerlemans have, for instance, proposed granting access to the tool via a 'data room', where the defence could easily – but in a controlled environment – search the data set with Hansken.[169]

Furthermore, Galič argues for an expansion of the right of the defence to test the reliability of evidence produced with AI-based tools.[170] For this purpose, she first argues for increased transparency concerning the use of the AI-tool (rather than transparency concerning the source code, which is not likely to become public in relation to Hansken and similar systems), such as access to the logging reports

[166] Maša Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding' (2021) 2 Boom Strafblad 41; Bart Schermer and Jan-Jaap Oerlemans, 'AI, Strafrecht En Het Recht Op Een Eerlijk Proces' (2020) 1 Computerrecht 14.

[167] In particular, the following two judgments from 2019: ECtHR, 4 June 2019, ECLI:CE:ECHR:2019:0604JUD003975715, app. no. 39757/15 (Sigurður Einarsson and others v. Iceland); ECtHR, 25 July 2019, ECLI:CE:ECHR:2019:0725JUD000158615, app. no. 1586/15 (Rook v. Germany).

[168] See e.g., Galič (n 30); Custers and Stevens (n 8).

[169] Bart Schermer and Jan-Jaap Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces' [2020] Computerrecht 10; see also JH de Wildt, 'Een Blik over de Grenzen: Vertrouwelijkheid, Data Rooms En Confidentiality Rings' (2017) Sanctierecht & Onderneming.

[170] Galič (n 30).

concerning the search activities that the investigatory officers performed on the data set(s). Hansken already provides for automatic logging of search activities, so this would be simple to implement from a technical point of view. Second, she proposes that AI-based systems such as Hansken should be considered as expert evidence, which allow for additional testing for the purpose of reliability and afford the defence with the right to counter-expertise.

## 3. Production of evidence through AI-based systems

### a. The example of CATCH: a facial recognition system

The Dutch police use facial recognition software called CATCH (short for 'Centrale Automatische TeChnologie voor Herkenning'). CATCH compares an image (a still from a video or a photograph) with a large database of current or past suspects and convicted persons that the Dutch police has gathered (consisting of 2,2 million images of 1,3 million persons).[171] Under certain circumstances, images may also be compared with a database of facial images of foreigners (without any requirement of suspicion), which consist of approximately 7 million images.[172] As such, CATCH does not (yet) perform real-time facial recognition, where the video feed of a particular individual (or set of individuals) from a camera would in real-time be compared with images in a particular database. However, real-time facial recognition is likely to be used by the Dutch police in the near future.[173]

CATCH may only be used for the purpose of investigation of crimes for which a prison sentence of four years or more is prescribed. However, this set of crimes includes relatively minor crimes, such as theft, (WhatsApp-)scam and car burglary. According to the police, the system is employed, 'if the (possible) identity of the person on an image carrier would substantially contribute to the prevention, detection or prosecution of criminal offences.'[174]

[171] 'Antwoorden Kamervragen over Het Bericht "Gezichtendatabase van Politie Bevat Foto's van 1,3 Miljoen Mensen"' (Ministerie van Justitie en Veiligheid, 10 September 2019) 3 <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/09/10/antwoorden-kamervragen-over-het-bericht-gezichtendatabase-van-politie-bevat-foto-s-van-1-3-miljoen-mensen/antwoorden-kamervragen-over-het-bericht-gezichtendatabase-van-politie-bevat-foto-s-van-1-3-miljoen-mensen.pdf> accessed 14 January 2022.

[172] 'Aanhangsel van de Handelingen: Nr. 584, 2019/2020' (Tweede Kamer, 2019) 1 <https://zoek.officielebekendmakingen.nl/ah-tk-20192020-584.html> accessed 14 January 2022.

[173] See e.g., Anton Mous, 'Gezichtsherkenning in real time vindt wél plaats in Nederland' (*Vpngids* 14 December 2021) <https://www.vpngids.nl/nieuws/gezichtsherkenning-in-real-time-vindt-wel-plaats-in-nederland/> accessed 14 January 2022.

[174] 'Centrale Automatische TeChnologie Voor Herkenning (CATCH) Jaarcijfers 2020' (Politie, 2020) <https://www.politie.nl/binaries/content/assets/politie/onderwerpen/forensische-opsporing/catch-jaarcijfers-2020-hr-online.pdf> accessed 14 January 2022.

### b. The normative framework for the use of facial recognition systems

#### *i. The legal framework*

There are no specific rules concerning the use of facial recognition systems or the evidence produced by such systems in the Netherlands (nor are any proposed in the modernisation project). Such evidence is regulated by general rules concerning the lawfulness and reliability of evidence as described in section 2.2. The evidence generated by such systems can be challenged in the same way as the evidence generated by the Hansken system.

As a consequence of the distinct regulation of the collection of data and the subsequent processing of data for law enforcement purposes (described in the part of the report on predictive policing in the Netherlands), the use of facial recognition systems is regulated only by legal rules for the creation of databases of facial images of persons and general data protection rules for their subsequent processing. As such, there is no specific legal basis for the use of facial recognition technology in the CCP (or elsewhere). Facial recognition is thus seen only as a 'regular' technique for the processing of personal data. In this legal vacuum, comparable to the one relating to predictive policing, the police use facial recognition technology on the basis of the general police task (Article 3 Police Act), in combination with the provisions on the general police tasks as found in Articles 141 and 142 CCP. This also means that the use of this system does not require an authorisation from the investigatory judge.[175] As already discussed, these general legal bases only suffice in cases, leading to a minor intrusion into privacy. It is thus doubtful, whether they may be used in relation to facial recognition, which is commonly considered as highly intrusive, especially considering that it involves the processing of biometric – that is, sensitive – personal data.[176]

The legal basis for the collection of facial images (and the creation of a database) is found in Article 55c CCP. Paragraphs 1-4 of Article 55c CCP regulate the taking of photos and fingerprints of persons suspected of crimes, for which a prison sentence of four years or more is prescribed. According to the fourth paragraph of this

[175] 'Aanhangsel van de Handleidingen, Nr. 3932, 2018/2019' (Ministerie van Justitie en Veiligheid, 13 September 2019) 5 <https://zoek.officielebekendmakingen.nl/ah-tk-20182019-3932.html> accessed 14 January 2022.

[176] Cf. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, 'Regulering van opsporingsbevoegdheden in een digitale omgeving' (2018) <https://kennisopenbaarbestuur.nl/documenten/rapport-commissie-koops-regulering-van-opsporingsbevoegdheden-in-een-digitale-omgeving/> accessed 14 January 2022; see also Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 2021 [COM(2021) 206 final].

provision, the images (and fingerprints) can be further processed for the purpose of prevention, detection, prosecution and adjudication of criminal offences. These data can be stored for a very long time, between 20 and 80 years.[177]

The legal basis for further processing is regulated by data protection law in the Police Data Act (PDA). Photographs that are used for facial recognition constitute biometric data and are as such 'sensitive personal data'. In line with EU data protection law, the processing of this type of data is regulated more strictly in the PDA. Processing is only permitted if it is 'unavoidable' (Art. 5 PDA) for the purpose pursued. This means that its processing must be substantiated in a particularly precise manner, including stricter limitations on storage. However, the Dutch police are struggling with these obligations. It was recently revealed that the police are not complying with its obligation to delete photos of persons who are no longer a suspect or were acquitted in subsequent proceedings.[178] In 2020, the police stated that they have deleted more than 200.000 images, but it remains unclear how many individuals have been removed from the database.[179]

### *ii. Reliability and neutrality of AI-based systems producing evidence180*

Specifically in relation to the CATCH facial recognition system, the reliability and neutrality of the technology are preserved in the guidelines for the use of the system, which require a 'double human verification' in the decision-making process.[181] The procedure of double human verification is designed to reduce the risk of false positives (i.e., incorrectly assumed matches) and to protect the rights of data subjects.[182] After the CATCH system performs the comparison between the images, it gives an overview of the faces with the most similarities, including scale scores. After the comparison, the AI-generated list of candidates is presented to a trained expert. If the expert believes that there is indeed a match with one of the candidates, the match is shown to two other experts who assess the match independently (it is unknown what kinds of experts are meant here and in which way they are trained). If the experts do not come to the same conclusion, the most conservative conclusion

[177] 'Aanhangsel van de Handleidingen, Nr. 3932, 2018/2019' (n 39) 2.

[178] 'Police Remove 218,000 Photos from Facial Recognition Database' (*Dutch news*, 23 July 2021) <https://www.dutchnews.nl/news/2021/07/police-remove-218000-photos-from-facial-recognition-database/> accessed 14 January 2022.

[179] ibid.

[180] For a general discussion, see description in relation to Hansken in sections 2.2 and 2.3.

[181] 'Kamerbrief over Gebruik Gezichtsherkenningstechnologie: Waarborgen En Kaders Bij Gebruik Gezichtsherkenningstechnologie' (Ministerie van Justitie en Veiligheid, 20 November 2019) 2–3 <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/11/20/tk-waarborgen-en-kaders-bij-gebruik-gezichtsherkenningstechnologie> accessed 14 January 2022.

[182] ibid.

is reported.[183] Even when the experts come to the same conclusion, this only results in an 'indication' that the suspect matches the person on the image.[184] The use of CATCH therefore does not lead to claims of a definitive identification of the suspect.

This has been confirmed in a 2019 judgment of the Zeeland-West-Brabant District Court,[185] which concluded that the results of the CATCH system, even after they have been 'confirmed' by two human experts, alone do not suffice for a criminal conviction (further discussed in the following section); additional corroborating evidence is necessary. This requirement that AI-generated evidence is corroborated by other evidence thus indirectly guarantees the reliability and neutrality of such systems.

### *iii. Case law*

So far, there has been only one judgment concerning the use of facial recognition software.[186] In the abovementioned 2019 judgment, the Zeeland-West-Brabant court only briefly discussed the validity of evidence that was produced by it, stating:

> 'The court is of the opinion that in this case the "hit" on the suspect in the so-called CATCH system (Central Automatic Technology for Recognition) is insufficient to conclude – beyond reasonable doubt – that the suspect can be designated as the person using the ATM machine. The observation that two investigators saw that there were many similarities and no significant deviations, is not considered so convincing by the court that the "hit" can serve as a basis for a proven conclusion. As there is no other evidence besides the recognition that links the accused to any of the charges, the court is of the opinion that the accused should be acquitted.'[187]

According to Dutch evidence law, one source of evidence does not suffice for a conviction (with the exception of a police officer personally observing a crime taking place; Art. 344(2) CCP). In regard to evidence *linking* the suspect to the offence, however, one source of evidence is sufficient, as long as other evidence of the crime exists, which is independent of the link between the suspect and the crime (e.g., money has been withdrawn from an ATM with a stolen bankcard). Despite the fact that the law does not require this, the Zeeland-West-Brabant court required

[183] 'Antwoorden Kamervragen over Het Bericht "Gezichtendatabase van Politie Bevat Foto's van 1,3 Miljoen Mensen"' (n 35) 5; see also 'Kamerbrief over Gebruik Gezichtsherkenningstechnologie: Waarborgen En Kaders Bij Gebruik Gezichtsherkenningstechnologie' (n 45) 2–3.

[184] District Court of Zeeland-West-Brabant, judgment of 17 May 2019, ECLI:NL:RBZWB:2019:2191 (case nr. 02-665274-18), para. 4.3.

[185] ibid.

[186] ibid.

[187] ibid., para. 4.3; translation by the authors.

corroborating evidence for the purpose of establishing the link between the suspect and the crime (e.g., eyewitness testimony or matching DNA at the scene). This means that the court did not consider AI-produced evidence through the CATCH system (despite the confirmation by humans) as sufficient in establishing the link between the suspect and the crime. In this way, the court indirectly ensured the reliability and neutrality of evidence produced by AI-based systems.

### *iv. Information provided by AI-based systems used by non-investigative authorities*

As already mentioned in section 2.2.1, the draft CCP introduces a new provision, on the basis of which the public prosecutor may order companies and institutions to process certain data and then provide only the 'results' to the police (draft Article 2.7.51 CCP). Based on the broad wording of the provision and the Explanatory Memorandum, it seems that non-investigative authorities (e.g., companies such as Google or Facebook) may indeed provide data to law enforcement that has been processed – that is, produced – through an AI-based system. While the Explanatory Memorandum does not speak specifically of AI techniques, it does state that advanced types of processing, which lead to the generation of 'new data', are meant here. This broad definition thus likely includes the use of AI.

The last two paragraphs of the provision provide for important safeguards in relation to the reliability of the data generated in this way. According to paragraph 3 of Article 2.7.51 CCP, the public prosecutor may require that the person carries out the processing in accordance with the instructions of the investigating officer. As the Explanatory Memorandum put it:

> 'This paragraph therefore offers the possibility of setting requirements for the execution, also with regard to the verifiability of the processing afterwards. One of the instructions of the investigating officer could be to describe the exact procedure of the analysis or to have the analysis checked or repeated by a second person. An instruction can also be that the analysis must take place in the presence and under the supervision of an investigating officer or another expert. In this respect, it will play a role whether the order is addressed to a large company that regularly carries out such analyses for the purpose of investigation or to a relatively small company that is perhaps considered less reliable. In the latter case, it is obvious that the investigation will play a major role, for example by supporting the analysis by supplying hardware and software.'[188]

On the one hand, this provision offers a safeguard that is badly needed in order to strengthen the reliability and transparency of the processing and the data generated

[188] Ambtelijke Versie Juli 2020 Memorie van Toelichting Wetboek van Strafvordering' (n 15) 443–444.

through it. On the other hand, the Explanatory Memorandum suggests an assumption of validity and reliability, when the processing is performed by 'large companies' that have knowledge and experience with data analysis. Not only is such an assumption misplaced (e.g., algorithms used by large companies such as Facebook and Google have oftentimes been found biased),[189] it is also unclear what the role of the defence is in this regard. Do they have a say, when the public prosecutor is considering, whether and in which way to instruct the company in regard to the prosecutor? The Explanatory Memorandum does not include any discussion on this.

The power granted in paragraph 3 of the provision is further strengthened by the power in paragraph 4. Paragraph 4 states that companies and institutions may be ordered to provide information 'about the data to which they have access' and about 'the actions required to carry out the processing referred to in the first paragraph'. The possibility of the public prosecutor to ask questions in advance about the (composition of the) data set and the effort that a company must make to perform a certain analysis, namely enables the prosecutor to assess whether an order for data analysis is useful and, if so, which conditions (as referred to in the third paragraph) should be imposed.[190] As such, para. 4 is of particular relevance in regard to AI-systems used for data processing. Depending on the interpretation of this requirement – do the 'actions required to carry out the processing' include technical steps taken by the system? – the prosecution thus might have the power to request further information concerning the manner in which the AI-tool functions and processes the data. A further question, again, relates to the defence: do or could they have access to this information? Such access would surely be needed in order to create an adequate safeguard for the reliability of AI-generated data that might serve as evidence in criminal cases.

### *v. Regional and international agreements on the admissibility of evidence*

Two regional instruments might be mentioned here. The first is the proposed EU e-Evidence Regulation,[191] which is intended to facilitate access to electronic evidence by European police and judicial authorities. The draft e-Evidence Regulation focuses on 'data cooperation' and seeks to provide an alternative to the existing mutual legal

[189] See e.g., Michael Walker, 'Upheaval at Google Signals Pushback against Biased Algorithms and Unaccountable AI' (*The Conversation*, 10 December 2020) <https://theconversation.com/upheaval-at-google-signals-pushback-against-biased-algorithms-and-unaccountable-ai-151768> accessed 14 January 2022; Karen Hao, 'How Facebook Got Addicted to Spreading Misinformation' (*MIT Technology Review*, 11 March 2021) <https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/> accessed 14 January 2022.

[190] 'Ambtelijke Versie Juli 2020 Memorie van Toelichting Wetboek van Strafvordering' (n 15) 444.

[191] Proposal for a Regulation of the European Parliament and of the Council on the European Production and Preservation Orders for electronic evidence in criminal matters 2018 [COM(2018) 225 final].

assistance framework. The second is the second protocol to the Budapest convention (Convention on Cybercrime) of the Council of Europe on enhanced international cooperation and access to evidence in the cloud.[192] Unfortunately, neither of these instruments seems to have touched upon a key problem: the quality – and, thus, admissibility – of what is to be exchanged. To this date, the proposals do not contain a single provision on how to reliably collect, analyse and present the material. There are, however, calls for the EU legislator to incorporate human rights standards in a new harmonising instrument on admissibility of evidence in criminal matters, for example in a dedicated Admissibility Directive.[193]

## 4. Evidence assessed through AI-based systems

To the best of our knowledge, AI-based systems used for assessing evidence are not (yet) used in the Netherlands, nor is there any significant debate on the matter. The only realistic example in which AI-based systems would actually assess criminal evidence, can be found in deepfake detection systems for the purpose of detecting fake images, videos or audio files among evidence. While it is unknown, whether the police already use such systems, on what scale and for which purposes, it can nevertheless be said that the development of such systems to be used in law enforcement has certainly begun in the Netherlands.[194]

## 5. Conclusion

We examined two types of AI-based systems used for the production of evidence: Hansken, a tool for the gathering of data out of huge data sets, and CATCH, a facial recognition tool. Even though Hansken is commonly described as a tool for the gathering of evidence from huge data sets, we argue that such systems actually do more than merely gather evidence that already exists: they produce it. This is so, because the system first needs to interpret the data by itself (e.g., a system searching for images of drugs needs to be able to determine that a particular photo indeed represents drugs). Second, it needs to be able to find relevant correlations (that is, links) between the numerous data points in the data set (e.g., resulting in a convincing time-line and scenario). Consequently, we need to talk about production

[192] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence 2021 [CM(2021)57-final].

[193] See e.g., Balázs Garamvölgyi and others, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 Eucrim: the European Criminal Law Associations' Forum <https://eucrim.eu/articles/admissibility-evidence-criminal-proceedings-eu/ > accessed 6 January 2023.

[194] See 'UvA En NFI Doen Onderzoek Naar Herkennen Deepfakes En Verborgen Berichten van Criminelen' (Universiteit van Amsterdam, 22 May 2021) <https://www.uva.nl/content/nieuws/persberichten/2021/05/uva-en-nfi-doen-onderzoek-naar-herkennen-deepfakes-en-verborgen-berichten-van-criminelen.html?cb> accessed 14 January 2022.

of evidence, both in relation to Hansken as well as the CATCH facial recognition system.

Despite the fact that digital evidence plays an increasingly important role in contemporary criminal proceedings, Dutch law (including the draft Code of Criminal Procedure, which is the result of the ongoing Modernisation project) has yet to implement any significant changes to its rules relating to evidence. As such, the few rules that regulate the gathering of evidence do not fit the particular needs of digital evidence very well. This leads to, for instance, issues with the principle of equality of arms. Considering the way digital evidence is gathered and examined, the defence needs additional or broader rights in order to participate in determining what counts as relevant information in a particular case, to participate in searching for exculpatory evidence, and to question the validity and accuracy of the functioning of AI-based systems. We can see that such rights are slowly being developed through case law.