AI SYSTEMS AND EVIDENCE LAW IN THE NETHERLANDS

By Maša Galič, Abhijit Das and Marc Schuilenburg [*]

Abstract

Digital evidence plays an increasingly important role in contemporary criminal proceedings in the Netherlands. Various types of AI-based systems are used for the production of evidence, including: Hansken, a tool for the gathering of data out of huge data sets, and CATCH, a facial recognition tool. Despite this increasing reliance of digital evidence, 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 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 several issues, including with the principle of equality of arms. Considering the way digital evidence is gathered – in fact, produced – 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. Such rights are, however, slowly being developed through case 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.

[*] 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. The authors would like to thank prof. dr. Lonneke Stevens and Thomas van Lieshout for their help with writing the part of the report on evidence.

2 Gathering evidence through AI-based systems

2.1 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.[1] 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.[2]

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).[3] At the moment the tool is said to have the capacity to process three terabytes of data per hour.[4] Hansken includes a wide variety of tools (software),[5] 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.[6] 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.[7]

2.2 The normative framework for the use of AI-based systems for gathering evidence

2.2.1. 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'

[1] Merve Bas Seyyar and Zeno Geradts, 'Privacy Impact Assessment in Large-Scale Digital Forensic Investigations' (2020) 33 Forensic Science International: Digital Investigation 1, 4.
[2] Other national bodies that use them are: the Netherlands Food and Consumer Product Safety Authority and Human Environment and Transport Inspectorate.
[3] 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.
[4] Bas Seyyar and Geradts (n 1) 2.
[5] 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.
[6] ibid 21.
[7] Bas Seyyar and Geradts (n 1) 4.

world are used.[8] However, these provisions are few and mainly 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.[9] 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.[10] 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.[11] 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.[12] 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.[13] 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 to Article 227 CCP), who would provide information on the functioning of Hansken.[14]

---

[8] 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.

[9] 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.

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

[11] 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.

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

[13] 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.

[14] 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. 26Marengo), p. 7.

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.[15] 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.[16]

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.[17] 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 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).[18]

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

---

[15] '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.

[16] ibid 443.

[17] ibid 441.

[18] ibid 442.

digital data sets. A lot of trust is placed into this tool.[19] 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.[20] 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.

2.2.2. 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, 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

[19] 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.
[20] ibid 851.

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.[21] 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.[22] 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.[23] 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 the right to assess, whether the proposed search terms are of sufficient relevance).[24] 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).[25] 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

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

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

[23] In the Ennetcom-Tandem case (District Court of Amsterdam, judgment of 19 April 2018, ECLI:NL:RBAMS:2018:2504 (case nr. 13/997097-16, 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).

[24] 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.

[25] 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.

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.'[26] 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.[27] Other courts either grant 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.[28] 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).[29]

---

[26] 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).
[27] See e.g., District Court of The Hague, judgment of 25 August 2021, ECLI:NL:RBDHA:2021:9368 (case nr. 09/095750-21).
[28] 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.
[29] The NFI are already working on this possibility, as presented by Hans Henseler and Harm van Beek, 'Hands-on with Hansken' (presentation at 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.

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.

2.3 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 result of the initial search of the full data set searched with the AI-tool) and to the AI-tool itself.[30]

On the basis of recent case law of the ECtHR concerning large data sets and Article 6 ECHR,[31] 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.[32]

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,

---

[30] 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.

[31] 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).

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

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.[33]

Furthermore, Galič argues for an expansion of the right of the defence to test the reliability of evidence produced with AI-based tools.[34] 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 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

3.1 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).[35] 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.[36] 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.[37]

---

[33] Schermer and Oerlemans (n 30) 10; see also JH de Wildt, 'Een Blik over de Grenzen: Vertrouwelijkheid, Data Rooms En Confidentiality Rings' (2017) Sanctierecht & Onderneming.

[34] Galič (n 30).

[35] '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.

[36] '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.

[37] 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.

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.'[38]

3.2 The normative framework for the use of facial recognition systems

3.2.1. 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.[39] 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.[40]

---

[38] '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.

[39] '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.

[40] 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

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 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.[41]

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.[42] 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.[43]

3.2.2. Reliability and neutrality of AI-based systems producing evidence[44]

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.[45] 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.[46] 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

down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 2021 [COM(2021) 206 final].

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

[42] '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.

[43] ibid.

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

[45] '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.

[46] ibid.

most conservative conclusion is reported.[47] Even when the experts come to the same conclusion, this only results in an 'indication' that the suspect matches the person on the image.[48] 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,[49] 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.

3.2.3. Case law

So far, there has been only one judgment concerning the use of facial recognition software.[50] 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.[51]

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 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

[47] '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.
[48] District Court of Zeeland-West-Brabant, judgment of 17 May 2019, ECLI:NL:RBZWB:2019:2191 (case nr. 02-665274-18), para. 4.3.
[49] ibid.
[50] ibid.
[51] ibid., para. 4.3; translation by the authors.

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.

3.2.4. 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.'[52]

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 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 mis-

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

placed (e.g., algorithms used by large companies such as Facebook and Google have oftentimes been found biased),[53] 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.[54] 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.

3.2.5. 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,[55] 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 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.[56] Unfortunately, neither of these instruments seems to have touched upon a key problem: the quality – and, thus, admissibility – of what is to be

[53] 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.

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

[55] 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].

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

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.[57]

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.[58]

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 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

[57] 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.

[58] 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.

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.

Selected literature

'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.

'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.

'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.

'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.

Bas Seyyar M and Geradts Z, 'Privacy Impact Assessment in Large-Scale Digital Forensic Investigations' (2020) 33 Forensic Science International: Digital Investigation 1, 4.

Harm van Beek and others, 'Digital Forensics as a Service: Game On' (2015) 15 Digital Investigation 20.

'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.

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.

Custers B and Stevens L, 'The Use of Data as Evidence in Dutch Criminal Courts' (2021) 29 European Journal of Crime, Criminal Law and Criminal Justice 25, 40.

'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.

Galič M, '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.

Garamvölgyi B 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.

Hao K, '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.

Henseler H and Harm van Beek, 'Hands-on with Hansken' (presentation at 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.

'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.

Mous A, '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.

'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.

Schermer B and Oerlemans J-J, 'AI, Strafrecht En Het Recht Op Een Eerlijk Proces' (2020) 1 Computerrecht 14.

Stevens L and Galič M, '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.

'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.

Walker M, '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.

de Wildt J H, 'Een Blik over de Grenzen: Vertrouwelijkheid, Data Rooms En Confidentiality Rings' (2017) Sanctierecht & Onderneming.