10

Data as Evidence in Criminal Courts

Comparing Legal Frameworks and Actual Practices

BART CUSTERS AND LONNEKE STEVENS

I. Introduction*

Technology has rapidly changed our society over the past decades. As a result of the ubiquitous digitalization of our society, people continuously leave digital traces behind. Some have already referred to this as "digital exhaust."[1] People are often monitored without being aware of it, not only by camera surveillance systems, but also by their own smartphones and by other devices they use to access the internet.

Information about the whereabouts, behavior, networks, intentions, and interests of people can be very useful in a criminal law context. It is used mainly for guiding criminal investigations, as it may provide clues on potential suspects, witnesses, etc., but it can also constitute evidence in courts, as the data may confirm specific actions and behavior of actors. In other words, digital data can be used to find out exactly what happened, understood in the legal context as finding the truth, and try to prove what happened, understood in the legal context as providing evidence. This chapter focuses on the use of digital data as evidence in criminal courts. The large amounts of potentially useful data now available may cause a shift in the types of evidence presented in courts, in that there may be more digital data as evidence, in addition to or at the cost of other types of evidence, such as statements from suspects, victims, and witnesses.[2]

* A preliminary version of this chapter was published as Bart Custers & Lonneke Stevens, "The Use of Data as Evidence in Dutch Criminal Courts" (2021) 29:1 *European Journal of Crime, Criminal Law and Criminal Justice* 25.

[1] Bruce Schneier, "The Battle for Power on the Internet," *The Atlantic* (October 24, 2013), www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

[2] Data within a criminal procedural context means information that needs to be found and/or understood by means of certain techniques and expertise; thus, a witness statement is not data, but a DNA profile is.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

However, in many jurisdictions, the legal provisions setting the rules for the use of evidence in criminal courts were formulated long before these digital technologies existed. As a result of ongoing technological developments, there seems to be an increasing discrepancy between legal frameworks and actual practices. The chapter investigates this disconnect by analyzing the relevant legal frameworks in the European Union for processing data in criminal courts and then comparing and contrasting these with actual court practices.

The relevant legal frameworks are criminal law and data protection law. Data protection law is mostly harmonized throughout the European Union, via the General Data Protection Regulation (GDPR)[3] and by regulation more specifically tailored to the criminal law context, via Directive 2016/680, also known as the Law Enforcement Directive (LED).[4] Criminal law, however, is mostly national law, with limited harmonization throughout the European Union. For this reason, criminal law is considered from a national perspective in this chapter. Criminal law in the Netherlands is taken as an example to illustrate the issues that may arise from using data as evidence in criminal courts.

Although Dutch criminal law may not be representative for all EU Member States, the discrepancies between EU data protection law and Dutch criminal law may be similar to other EU Member States. As such, the Netherlands may serve as a helpful example of how legal provisions dealing with the use of evidence in criminal courts is not aligned with developments in data as evidence.

We also think that reviewing the use of data as evidence in courts in the Netherlands may be interesting for other jurisdictions, because it can provide some best practices as well as identify caveats and pitfalls that can perhaps be avoided in other countries. We see two major arguments supporting such a claim. First, the issues of using data as evidence in courts are likely to be the same across Europe, as the technologies available are not confined to one or particular jurisdictions. This point also applies to the forensic standards that are applied, as these also have an international scope and nature, either because they are established by international standardization organizations such as ISO,[5]

[3] General Data Protection Regulation, EU 2016, Regulation (EU) 2016/679 (with effect from May 25, 2018) [GDPR].

[4] The Data Protection Law Enforcement Directive, EU 2016, Directive (EU) 2016/680 (with effect from May 5, 2016) [LED].

[5] International Organization for Standardization, www.iso.org/home.html.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

CEN-CENELEC,[6] and ETSI[7], or, if created on a national level, are at least aligned among forensics experts from different countries. Second, the legal frameworks for using data as evidence in courts are highly comparable. This is particularly the case for data protection law, which is highly harmonized across the European Union. Criminal law may not be harmonized that much across the European Union, but the norms and standards for evidence and fair trial are fleshed out in large part by the European Convention on Human Rights (ECHR) and Court of Justice of the European Union (CJEU) case law. All this means that the basic situation regarding technology and forensic practices and the relevant legal boundaries are more or less the same across the European Union, although national interpretations and practices within these confines may vary.

There are two other reasons to use the Netherlands as an example in this chapter, both related to the fact that the Netherlands is in the forefront of relevant regulation. First, international legal comparisons show that the Netherlands is a front runner in privacy and data protection law in several aspects.[8] The Netherlands implemented national legislation with higher levels of data protection than strictly necessary for compliance with EU data protection laws. Typical examples are data breach notification laws and mandatory privacy impact assessments that already existed in the Netherlands before the GDPR came into force in 2018.[9] Also, when looking at the criminal law context, the Netherlands was among the first countries to have specific acts for the police and the judiciary dealing with the processing of personal data in criminal law, long before EU Directive 2016/680 (the LED, see section III.C) came into force.[10] If there exists a

[6] CEN stands for European Committee for Standardization (*Comité Européen de Normalisation*) and CENELEC stands for European Committee for Electrotechnical Standardization (*Comité Europeén de Normalisation Électrotechnique*), www.cencenelec.eu/.

[7] European Telecommunications Standards Institute, www.etsi.org/.

[8] Bart Custers, Alan M. Sears, Francien Dechesne *et al.*, *EU Personal Data Protection in Policy and Practice* (Heidelberg, Germany: Asser/Springer, 2019) [*EU Personal Data*].

[9] Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law" (2012) *Bloomberg BNA Privacy and Security Law Report* 1.

[10] The introduction of EU Directive 2016/680 required few changes in the Dutch legal framework for processing personal data in criminal law. In comparison, in Italy, there were no specific laws or regulations for the protection of personal data in criminal law, apart from the general legislation for criminal investigation and the GDPR. As such, Italy needed to draft entirely new legislation. In other countries, such as Germany, Sweden, and Romania, this topic was dealt with in their Police Acts, which often needed further elaboration to comply with this EU Directive. *EU Personal Data*, note 8 above.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

disconnect between legal frameworks and actual practices with regard to data as evidence in criminal courts in a country that seems to be a regulatory front runner, in this case the Netherlands, similar problems may also exist in other EU Member States.

Second, the Netherlands is among the front runners in digital forensics and cybercrime legislation.[11] The Netherlands was among the initiators of the Convention on Cybercrime, adopted by the Council of Europe in 2001, which includes provisions that relate to the processing of police data.[12] This Convention regulates, among other things, the protection of personal data and international cooperation, including the exchange of personal data in criminal law cases between authorities of different countries. Also, the Netherlands ratified a series of legal instruments that aim to advance the cooperation and sharing of information between Member States, such as the Prüm Treaty[13] (for exchanging DNA data, fingerprints, and traffic data), the Schengen Information System[14] (for international criminal investigation information), the Visa Information System[15] (for visa data, including biometrical data), and the Customs Information System[16] and Eurodac[17] (for fingerprints

[11] Susan Brenner & Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) 4:1 *Journal of High Technology Law* 1; Bert-Jaap Koops, "Cybercrime Legislation in the Netherlands" (2005) 2005:4 *Cybercrime and Security* 1.

[12] European, Council of Europe, Convention on Cybercrime, ETS No. 185 (Budapest: Council of Europe, 2001) Arts. 19–21.

[13] European Union, The Council of the European Union, Council Decision 2008/615/JHA on the Stepping Up of Cross-border Cooperation, Particularly in Combating Terrorism and Cross-border Crime, OJ 2008 L 210 (EU: Official Journal of the European Union, 2008).

[14] European Union, The Council of the European Union, Council Decision 2007/533/JHA on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II), OJ 2007 L 205 (EU: Official Journal of the European Union, 2007).

[15] European Union, The European Parliament, & The Council of the European Union, Regulation (EC) No. 767/2008 of The European Parliament and of The Council Concerning the Visa Information System (VIS) and the Exchange of Data Between Member States on Short-Stay Visas (VIS Regulation), OJ 2008 L 218 (EU: Official Journal of the European Union, 2008).

[16] European Union, The Council of the European Union, Council Decision 2009/917/JHA on the Use of Information Technology for Customs Purposes, OJ 2009 L 323 (EU: Official Journal of the European Union, 2009).

[17] European Union, The Council of the European Union, Council Regulation (EC) 2725/2000 Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin Convention, OJ 2000 L 316 (EU: Official Journal of the European Union, 2000); European Union, The Council of the European Union, Council Regulation (EC) 407/2002 Laying Down Certain Rules to Implement Regulation

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

of asylum seekers and stateless people). The institutional regulations for Europol, Eurosur, and Eurojust contain provisions for the exchange of criminal law information between Member States.

In short, the Netherlands appears to be among the first countries in the European Union to develop both privacy and data protection, and digital forensics and cybercrime legislation. This characteristic is relevant because if there is a disconnect between legal frameworks and actual practices with regard to data as evidence in criminal courts in a country that seems to be in the forefront of regulation, in this case the Netherlands, it may be expected that similar problems also exist in other EU Member States.

In the Netherlands, a founding member of the European Union and its predecessors, there has been an extensive debate in society and in politics on how to balance using data in a criminal law context and protecting the right to privacy.[18] This debate has influenced the legal frameworks that regulate the use of data in criminal law. There are competing legal frameworks regulating this area: on the one hand, criminal law, including both substantive and procedural criminal law, and, on the other hand, privacy law, more specifically data protection law. It is important to note that both legal frameworks provide rules for allowing and restricting the use of personal data in criminal law, as sometimes there is a misunderstanding that criminal law would only or mainly allow the collection and processing of data, whereas data protection law would only or mainly restrict such data collection and processing.

The focus of this chapter is the discrepancy between legal frameworks and actual practices. First, the relevant legal frameworks for processing data in Dutch criminal courts are analyzed, i.e., Dutch criminal procedure law and EU data protection law). After this legal analysis, current court practices are examined, mainly by looking at typical case law and current developments in society and technology.

2725/2000 Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin Convention, OJ 2002 L 62 (EU: Official Journal of the European Union, 2002).

[18] Together with France and Italy, the Netherlands had a debate focused on privacy versus security. This culminated in a referendum on the proposed Intelligence Agencies Act that extended powers for intelligence agencies, which voters turned down. Since this referendum was not binding, the Dutch government accepted the act anyway and abolished this type of referendum; see Charlotte Wagenaar, "Beyond For or Against? Multi-Option Alternatives to a Corrective Referendum" (2019) 62:1 *Electoral Studies* Article 102091. This case shows a clear tension between the general public's commitment to privacy issues versus the government's priority of national security, and perhaps also of criminal law enforcement.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

This chapter is structured as follows. Section II provides a brief general introduction to Dutch criminal procedure law. Section III provides a brief general introduction to EU data protection law and to some extent its implementation in Dutch data protection law, focusing on the GDPR and the LED respectively. Section IV investigates the actual use of evidence in Dutch criminal courts by focusing first on current court practices as reflected in case law, and second on current developments in society and technology. Section V compares current court practices with the developments in society and technology, in order to see whether there is a need to change court practices or the underlying legal frameworks.

II Criminal Procedure Law: The Example of the Netherlands

As the Netherlands is used as an example of national law in this chapter, some background information is provided regarding Dutch criminal law. The Dutch Code of Criminal Procedure (Dutch CCP)[19] dates back to 1926. Back then, the Code was characterized as "moderately accusatorial" since it introduced more rights for the defense than before that time.[20] Today, however, the suspect remains to a large extent the object of investigation, rather than, e.g., the victim, which has become increasingly important in Dutch criminal law in recent decades.[21] This is especially the case in the stages of police investigation, before the start of the trial. Although over the years more possibilities for the defense to influence the earlier investigation were introduced, such as the right to contra-expertise during police investigation in Article 150b of the Dutch CCP, the defense and the prosecutor are far from equal parties. Basically, the room for maneuver for the defense largely depends on the prosecutor's goodwill, as it is the prosecutor who leads the criminal investigation.[22]

[19] *Wetboek van Strafrecht* (Dutch Code of Criminal Procedure), Netherlands (1926) [Dutch CCP].

[20] See Lonneke Stevens, *Het nemo-teneturbeginsel in strafzaken: van zwijgrecht naar containerbegrip* (The Nemo Tenetur Principle in Criminal Cases: From the Right to Remain Silent to an All-Purpose Concept, PhD thesis, Tilburg University) (Nijmegen, Netherlands: Wolf Legal Publishers, 2005) at ch. 3.

[21] Cf. Jo-Anne Wemmers, Rien van der Leeden, & Herman Steensma, "What Is Procedural Justice: Criteria Used by Dutch Victims to Assess the Fairness of Criminal Justice Procedures" (1995) 8:4 *Social Justice Research* 329.

[22] For more details, see Jeroen Chorus, Ewoud Hondius, & Wim Voermans (eds.), *Introduction to Dutch Law*, 5th ed. (Alphen aan den Rijn, Netherlands: Kluwer Law International, 2016).

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

A more accurate description of Dutch criminal procedure would therefore be "moderately inquisitorial."[23]

Fundamental to the position of the defense is the right to silence in Article 29 of the Dutch CCP. Rights and principles such as the privilege against self-incrimination, the equality of arms, and the presumption of innocence are not explicitly laid down in the Dutch CCP. They apply, however, directly to Dutch criminal procedure through Article 6 of the ECHR.

The Dutch CCP has been amended and supplemented many times since its creation in 1926. As a result, the Dutch CCP now looks more like a patchwork instead of structured and clear-cut Code. This is also one of the reasons that the legislator started the major, still-running project "Modernisation Criminal Procedure" (*Modernisering Strafvordering*) in 2014. This revision of legislation was not finished as of 2023, and it will take several more years before it is finished. The idea is to revise the Dutch CCP in order to make criminal procedure, among other things, more accessible and efficient.[24] Another aim of the revision is to tackle one of the greater challenges criminal procedures face nowadays, those of keeping up with technological developments in criminal investigation practice and developing an overall framework for regulating criminal investigation in the digital era. The Dutch CCP is still very much an analog-style Code that regulates the searching of homes, the seizure of letters, wiretapping, the questioning of witnesses, etc. Various digital investigation methods can be conducted on the basis of existing powers, e.g., a computer that was seized in a home can be searched just like a diary or a pistol that was seized in a home,[25] and several new digital investigation methods have been laid down in the Dutch CCP, e.g., the network search of Article 125j of the Dutch CCP or the hacking powers in Article 126nba of the Dutch CCP,[26] but many digital methods

[23] Geert Corstens, Matthias Borgers, & Tijs Kooijmans, *Het Nederlands strafprocesrecht* (Dutch Criminal Procedure Law) (Deventer, Netherlands: Kluwer, 2018) [*Het Nederlands*] at 10.

[24] See Documenten Modernisering Wetboek van Strafvordering, www.rijksoverheid.nl/documenten/publicaties/2017/11/13/documenten-modernisering-wetboek-van-strafvordering; Platform Modernisering Strafvordering, www.moderniseringstrafvordering.nl/.

[25] See Bert-Jaap Koops & Jan-Jaap Oerlemans, "Formeel strafrecht en ICT" (Substantive Criminal Law and ICT) in Bert-Jaap Koops & Jan-Jaap Oerlemans (eds.), *Strafrecht en ICT* (The Hague, Netherlands: Sdu Uitgevers, 2018) 117 at 125–127.

[26] Introduced with the Computer Crime Law III, Netherlands (in force since March 2019). See also Ronald Pool & Bart Custers, "The Police Hack Back: Legitimacy, Necessity and Privacy Implications of the Next Step in Fighting Cybercrime" (2017) 25:2 *European Journal of Crime, Criminal Law and Criminal Justice* 123.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

are still unregulated. Awaiting legislation, some gaps have been filled provisionally by the Supreme Court, in cases where the defense questioned the legitimacy of certain methods. One important discussion concerns the legitimacy of searching a smartphone that was seized from a suspect after arrest. In 2017, the Supreme Court ruled that the general power of a policeman to "seize and search objects the suspect carries with him when arrested" in Articles 94 and 95 of the Dutch CCP can be the basis of a smartphone search under the condition that the infringement on the right to privacy remains limited.[27] In cases where the infringement exceeds a limited search, such a search should be conducted or authorized by the public prosecutor. When it is foreseeable that the privacy-infringement will be "serious" (*zeer ingrijpend*), the investigatory judge needs to be involved.

The smartphone ruling of the Supreme Court needs to be understood from the perspective of the procedural legality principle that is laid down in Article 1 of the Dutch CCP. This article states that criminal procedure can only take place as foreseen by law,[28] which means that the police cannot use investigation methods that infringe fundamental rights which are not explicitly grounded in a sufficiently detailed and explicit statutory investigation power. However, investigation methods that are not explicitly regulated in the Dutch CCP, like the seize and search powers in Articles 94 and 95 of the Dutch CCP mentioned above, and that only cause minor infringements, can be based on Article 3 of the Police Act.[29] This Article contains the general description of the task carried out by the police: "it is the task of the police to maintain the legal order in accordance with the rules and under the subordination of the competent authority."[30] In case law, several digital investigation methods have been found to constitute only a minor infringement and therefore did not need to be explicitly regulated.[31] For example, sending stealth text

[27] Dutch Supreme Court (via www.rechtspraak.nl), HR 4 April 2017, *NJ* 2017, 229, ECLI:NL:HR:2017:584; see also the case note of Lonneke Stevens, "Onderzoek in een smartphone: Zoeken naar een redelijke verhouding tussen privacybescherming en werkbare opsporing" (Smartphone Searches: Balancing Privacy Protection and Criminal Investigation Practices) (2017) *Ars Aequi* 730 at 730–735. For an explanation in English, see Bryce Clayton Newell & Bert-Jaap Koops, "From Horseback to the Moon and Back: Comparative Limits on Police Searches of Smartphones upon Arrest" (2020) 72:1 *Hastings Law Journal* 229 ["From Horseback"].

[28] "Law" meaning formal acts of Parliament.

[29] *Het Nederlands*, note 23 above, at 29–30.

[30] Police Act 1993, Netherlands (with effect from December 9, 1993), Art. 3.

[31] This approach is also taken in some proposals in the United States, such as the American Bar Association (ABA) Model Standards for Criminal Justice: Law Enforcement Access

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

messages[32] to someone's cell phone can in principle be based on the general police task description, except when this is done for such a period or with such frequency and intensity that a complete image is revealed of certain aspects of someone's private life.[33] The smartphone case, in which a very general power to seize was found to be a sufficient statutory basis for a limited smartphone search, builds on this settled case law.[34] In its legislative draft on digital investigation, the "Modernisation" legislator has incorporated the so-called "pyramid-structure" of the smartphone case, i.e., within the categories of limited, more than limited, and serious intrusions. A larger privacy infringement demands a higher approval authority, so instead of the police, a prosecutor or investigatory judge is required. Also, limited intrusions do not have to be explicitly regulated, while more than limited and serious intrusions are in need of more detailed and stringent legislation. To distinguish between the different levels of privacy intrusion, the legislator uses the concept of "systematicness" (*stelselmatigheid*).[35] This means that, e.g., a "forseeably systematic" computer or network search can be ordered by the public prosecutor, while a "foreseeably serious systematic" computer or network search also needs a warrant from the investigating judge.[36] The same regime applies to research in open sources.[37] The post-smartphone case law already demonstrates that the category of seriously systematic is almost nonexistent in practice.[38] Although the introduction of the pyramid structure is also based on the practical premise that the investigating judge should not be overburdened within the context of digital investigations, this does raise serious concerns about the level of legal protection.

to Third Party Records (2013), www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access/. US courts have so far largely rejected this approach.

[32] Stealth text messaging refers to sending a text message to a cell phone without the phone acknowledging receipt, in order to generate traffic data with the phone's location that can be ordered from a telecoms provider.

[33] Dutch Supreme Court, HR 1 July 2014, *NJ* 2015, 114, ECLI:NL:HR:2014:1563.

[34] See Dutch Supreme Court, HR 4 April 2017, *NJ* 2017, 229, ECLI:NL:HR:2017:584.

[35] It was initially the Commission "Modernisation of criminal investigation in the digital era" (Koops-Commission) that suggested the use of *systematicness* as a structuring concept; see the advice in: Netherlands, Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving* (Regulating Criminal Investigation Powers in Digital Environments), s. l. (Netherlands: Commissie modernisering opsporingsonderzoek in het digitale tijdperk, 2018) ["Koops-Commission"].

[36] See the proposal for the *Nieuw Wetboek van Strafvordering* (Proposed Code of Criminal Procedure), Netherlands (as amended July 2020) [Proposed CCP], Arts. 2.7.39 and 2.7.41.

[37] Ibid., Art. 2.8.8.

[38] "From Horseback", note 27 above, at 264–268.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

III Dutch and EU Data Protection Law

III.A GDPR and LED

In 2016, the European Union issued the final text for the GDPR, revising the EU legal framework for personal data protection. This legislative instrument, well known throughout the European Union, is directly binding for all EU Member States and their citizens.[39] To a large extent, the GDPR carried over the contents of the EU Data Protection Directive from the 1995 version it replaced, most notably the so-called principles for the fair processing of personal data, although the GDPR, which came into force in May 2018, received a lot of attention, probably due to the significant fines that were introduced for non-compliance. The European Union also issued with comparatively little fanfare Directive 2016/680, on protecting personal data processed for the purposes of law enforcement.[40] This much less well-known directive, referred to as the LED, which can be considered a *lex specialis* for the processing of personal data in the context of criminal law, had to be implemented into national legislation of each EU Member State by May 2018, coinciding with the date the GDPR came into force.

III.B The GDPR

Since the GDPR is directly binding for all Member States and their citizens, strictly speaking no further implementation is required. Nevertheless, some countries, including the Netherlands,[41] implemented national legislation to further implement the GDPR. The GDPR allows EU Member States to further elaborate on provisions in the GDPR that leave room for additional provisions at a national level.

The scope of the GDPR is restricted to personal data, which is defined in Article 4(1) as any information relating to an identified or identifiable natural person (the data subject). This excludes anonymous data and data

[39] GDPR, note 3 above, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119.

[40] LED, note 4 above, 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 offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

[41] In the Netherlands, the GDPR was implemented via the *Uitvoeringswet AVG* (GDPR Execution Act), Netherlands (with effect from May 25, 2018).

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

relating to legal persons. Data on deceased people is not personal data and therefore beyond the scope of the GDPR.[42] For collecting and processing personal data, there are several provisions that data controllers have to take into account. First of all, all processing has to be lawful, fair, and transparent under Article 5(1). Furthermore, the purposes for which the data are collected and processed have to be stated in advance (purpose specification), the data may not be used for other purposes (purpose or use limitation), and data may only be collected and processed when necessary for these purposes (collection limitation or data minimization). Data has to be accurate and up to date (data quality). When data is no longer necessary, it has to be removed (storage limitation). The data needs to be processed in a way that ensures appropriate security and has to be protected against unlawful processing, accidental loss, destruction, and damage (data integrity, confidentiality). Furthermore, the data controller is responsible for compliance under Article 5(2) (accountability).

Data subjects have several so-called data subject rights regarding their personal data under the GDPR, including a right to transparent information on the data collected and the purposes for which it is processed (Articles 12–14), a right to access to their data (Article 15), a right to rectification (Article 16), a right to erasure (Article 17), a right to data portability (Article 20), and a right not to be subject to automated decision-making (Article 22).

The GDPR is relevant in a criminal law context for all data controllers that are not within the scope of the LED. For example, private investigators and government agencies in the migration domain are subjected to the GDPR. Also, when companies apply camera surveillance or other technologies that collect personal data, the data collected and processed are subject to the GDPR. As soon as the police or the public prosecution service request such data for criminal investigation, the data comes within the scope of the LED rather than the GDPR.[43] Law enforcement agencies can request data from individuals and companies at any time during a criminal investigation, but handing over such data is on a voluntary basis. It is only when law enforcement agencies have obtained a court warrant that handing over the data is mandatory. If relevant, any such information may be used as evidence in court cases.

[42] Edina Harbinja, "Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives?" (2013) 10:1 *SCRIPTed* 19.

[43] Although the GDPR is less relevant than the LED in a criminal law context, we use the GDPR as a starting point in this section, because we expect Europeans readers of this chapter to be more familiar with the GDPR.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

III.C The Law Enforcement Directive (LED)

In 2012, the European Commission presented the first draft of a Directive that would harmonize the processing of personal data in criminal law matters.[44] The debate regarding the Directive between the European Parliament, the Commission, and the Council continued for four years. After amendments, the legislative proposal was adopted in 2016, in its current version as EU Directive 2016/680 (the LED). The deadline for implementation in national legislation was two years, with a final deadline in May 2018. Directive 2016/680 repealed the Framework Decision 2008/977/JHA as of that date.

The aim of the LED is twofold. It ensures the protection of personal data processed for the prevention, investigation, detection and prosecution of crimes, and the execution of criminal penalties. It also facilitates and simplifies police and judicial cooperation between Member States and, in general, more effectively addresses crime. This two-pronged approach is similar to that of the GDPR and the Framework Decision.

The LED is a data protection regime alongside the GDPR. The LED specifically focuses on data processing by "competent authorities," as defined in Article 3(7). Competent authorities include:

> (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or
> (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Perhaps the most obvious competent authorities are police forces and public prosecution services, but there may be a variety of competent

[44] This section of the chapter is partially based on Mark Leiser & Bart Custers, "The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680" (2022) 5:3 *European Data Protection Law Review* 367 ["Conceptual Issues"].

European Union, European Commission, Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM (2012) 10 final (EU: European Commission, 2012).

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

authorities in the national criminal law of EU Member States. For example, in the domain of execution of criminal penalties, competent authorities may include the "regular" prison system, juvenile correction centers, forensic psychiatric centers, probation authorities, etc.

The scope of the LED is limited to the processing of personal data by the competent authorities for the specific purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties (Articles 1 and 2). This includes the safeguarding against and the prevention of threats to public security (Recital 11). As such, it should be noted that not all personal data processed by law enforcement agencies and the judiciary is within the scope of the LED. For example, when law enforcement agencies or the judiciary are processing personnel data regarding their staff, for paying wages or assessing employee performance, the GDPR applies rather than the LED. The GDPR is also applicable to personal data processing regarding borders, migration, and asylum.

With regard to the protection of personal data, the LED includes, similar to the GDPR, a set of principles for the fair processing of information, such as lawful and fair processing, purpose limitation, accuracy of data, adequate security safeguards, and responsibility of the data controller in Article 4 of the LED. Transparency is strived for as much as possible, but it is obvious that there are clear limitations to transparency in the interest of ongoing criminal investigations. This can lead to interference with the principle of equality of arms (Article 6 of the ECHR), as the defense may not be entitled to review some relevant data, and in practice, the defense may only get what the prosecutor decides to give. Essentially, the rights granted to data subjects can be difficult to invoke, at least in a meaningful way. National data protection authorities are eligible to handle any complaints regarding actors in the criminal justice system that do not comply with the LED provisions, and such cases can also be brought to courts. However, for data subjects, it can be hard to get access to data on themselves if they do not know which data actually exists. Contrary to the GDPR regime of high fines, the LED regime leaves setting maximum fines to national legislation. No EU Member State has implemented significant fines for LED non-compliance, something that obviously does not contribute to strict enforcement.

Personal data should be collected for specified, explicit, and legitimate purposes within the LED's scope, and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

of criminal penalties, including the safeguarding against and the prevention of threats to public security. Some of these principles are problematic, particularly when data is transferred from a GDPR regime into the context of law enforcement.[45] Also, the protection provided under the GDPR may decrease, from a data subject's perspective, when law enforcement agencies get access to data collected by private parties.[46] While the GDPR is not very specific about time limits for data storage and review,[47] the LED requires clear establishment of time limits for storage and review.[48] The LED states that Member States should provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Article 5(1)(e) of the GDPR states that personal data should be kept no longer than necessary, but does not mention a number of days, months, or years. The Article 29 Working Party issued an opinion that argues that time limits should be differentiated.[49] Storage time limits vary across Member States and for different situations, including different types of data subjects and different crimes. For example, in Germany, data storage duration is limited depending on the types of persons: ten years for adults, five years for adolescents, and two years for children.[50] Data on whistleblowers and informants can only be stored for one year, but can be extended to three years. In the Netherlands, the storage of personal data by the police is limited to one year, which can be extended to five years if the data is necessary for the police tasks.[51] In the United

[45] Catherine Jasserand, "Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?" (2018) 4:2 *European Data Protection Law Review* 152.

[46] Catherine Jasserand, "Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?" (2018) 34:1 *Computer Law & Security Report* 154.

[47] GDPR, note 3 above, Art. 5(1)(e) states that personal data should be kept no longer than necessary, but does not mention a number of days, months, or years. Note that Arts. 13 and 14 of the GDPR require data controllers to inform the data subject on storage times if they inquire about this.

[48] LED, note 4 above, Art. 5; see also Teresa Quintel, "European Union – Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive" (2018) 4:1 *European Data Protection Law Review* 104.

[49] European Union, European Commission, Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680) – wp258, WP 2017/258 (EU: European Commission, 2017).

[50] *Bundesgrenzschutzgesetz 1994* (Federal Border Protection Act 1994), Germany (with effect from/as amended 1994), § 35.

[51] *Wet Politiegegevens* (Police Data Act), Netherlands (with effect from/as amended 1 October 2022) [Police Data Act], Art. 8.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

Kingdom, section 39(2) of the Data Protection Act 2018[52] requires that appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.[53]

The LED offers explicit protection for special, i.e., sensitive, categories of data, such as data relating to race, ethnicity, political opinions, religion, trade union membership, sexual orientation, genetic data, biometric data, health data, and sex life data. The use of perpetrator profiles and risk profiles is explicitly allowed.

The LED also provides a list of data subject rights, such as the right to information, the right to access, the right to rectification, the right to erasure, and the right to restriction of the processing. Since these data subject rights can only be invoked if this does not interfere with ongoing investigations, these rights can be somewhat misleading. Some data subject rights mentioned in the GDPR, such as the right to data portability and the right to object to automated individual decision-making, are not included in the LED. The absence of the right to object to automated decision-making offers more leeway for law enforcement to use profiling practices, such as perpetrator profiling and risk profiling.

In the Netherlands, there already existed specific legislation for the processing of personal data in criminal law before the LED came into force. The Police Data Act (*Wet politiegegevens*) ("Wpg")[54] regulated the use of personal data for police agencies, and the Justice and Prosecution Data Act (*Wet justitiële en strafvorderlijke gegevens*) ("Wjsg")[55] regulates the use of personal data by the public prosecution services and the judiciary. Contrary to other EU Member States, where sometimes entirely new legislation had to be drafted, the Netherlands merely had to adjust existing legislation when implementing Directive 2016/680.

Both the Wpg and the Wjsg already strongly resembled the LED in terms of structure, scope, and contents, which meant that only a few changes were required. Also, the rights of data subjects, international cooperation, and supervision by data protection authorities were already regulated. Elements that were missing included concepts like Privacy

[52] Data Protection Act 2018, UK, c. 12 (with effect from May 25, 2018).
[53] In comparison, this feature is largely missing in US regulatory frames.
[54] Police Data Act, note 51 above.
[55] *Wet justitiële en strafvorderlijke gegevens* (Justice and Prosecution Data Act), Netherlands (with effect from/as amended July 1, 2022).

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

by Design, Privacy by Default, and Privacy Impact Assessments.[56] The Netherlands already introduced data breach notification laws in 2016, prior to the GDPR, but these laws did not apply to the police, prosecution services, and the judiciary – a change brought about by the LED.

Across the European Union, implementation of the LED in national legislation proceeded slowly. In February 2018, a few months before the implementation deadline of May 2018, only a few countries, such as Germany, Denmark, Ireland, and Austria, had implemented the directive. The Netherlands had implemented the directive with some delay: the revised Wpg and Wjsg came into force in January 2019, more than half a year after the May 2018 deadline. Other countries, such as Belgium, Finland, and Sweden, were later, but they implemented the directive by 2019. However, there was also a group of countries, including Spain, France, Latvia, Portugal, and Slovenia, that had not yet accomplished implementation by 2019. In January 2019, the European Commission sent reasoned opinions to Bulgaria, Cyprus, Greece, Latvia, the Netherlands, Slovenia, and Spain for failing to implement the LED, and urged the Czech Republic and Portugal to finalize the LED's implementation.[57] In July 2019, the European Commission lodged an infringement action against Greece and Spain before the CJEU for failing to transpose the LED into national legislation.[58] Since then, Greece passed Law 4624/2019 of August 29, 2019, implementing the LED. Latvia and Portugal transposed the LED in August 2019, while Spain had not yet adopted such an act. Also as of August 2019, six out of the 16 federal states (*Länder*) of Germany had not yet passed laws transposing the LED, which led the European Commission to send a formal notice, the first step of infringement proceedings.[59] As of May

[56] Privacy by design and privacy by default are based on the idea that technology usually can be designed in different ways within provided requirements, resulting in the same functionality. However, some designs can be more privacy-friendly and other less privacy-friendly. Privacy by design aims to include privacy as a value into the design. Privacy by default aims to set defaults in technology in a privacy-friendly mode, e.g., opt-in instead of opt-out. Privacy impact assessments are risk assessments of new technologies, business models, policies, or other plans in which personal data are being processed. The risk assessments focus on privacy risks of the data subjects.

[57] European Commission, "January Infringements Package: Key Decisions" (January 24, 2019), https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_462.

[58] European Commission, "Data Protection: Commission Decides to Refer Greece and Spain to the Court for Not Transposing EU Law" (July 25, 2019), https://ec.europa.eu/commission/presscorner/detail/EN/IP_19_4261.

[59] European Commission, "Infringement Proceedings: Commission Takes Legal Action against Germany in 17 Cases" (July 25, 2019), https://ec.europa.eu/commission/presscorner/detail/en/inf_23_142.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

2020, Germany had not yet fully transposed the LED, and the European Commission has sent a reasoned opinion. The same action was taken against Slovenia, which also failed to transpose the LED.[60] On February 25, 2021, the CJEU sanctioned Spain with a €15 million fine and a daily penalty of €89,000 for its ongoing failure to transpose the LED into national legislation.[61] In April 2022, the European Union launched an infringement procedure against Germany after detecting a gap in the transposition of the LED in relation to activities of Germany's federal police.[62]

IV Evidence in Dutch Criminal Law

IV.A Basic Principles

As in many countries, the evidentiary system in criminal cases in Dutch criminal law is based on the principle of establishing the substantive truth. This goal is expressed in the Dutch CCP by the requirement that a judge may assume that the offense charged is proven only if the judge "is convinced."[63] This means that a high degree of certainty must exist that the suspect has committed the offense. The judge must be convinced by the contents of legal evidence. The latter is the evidence that the Dutch CCP considers admissible in criminal proceedings. It includes the judge's own perception, statements by the suspect, statements by a witness, statements by an expert, and written documents per Article 339 of the Dutch CCP. This summary is so broad that hardly any evidence can be indicated that the law does not consider admissible.[64] Digital data as evidence will usually be submitted in the form of written police statements that report the results of an investigation.[65]

There are only few rules in the Dutch CCP that govern the reliability of evidence. Relevant to any kind of evidence is the obligation for the judge

[60] European Commission, "May Infringements Package: Key Decisions" (May 14, 2020) at "Data Protection: Commission Urges GERMANY and SLOVENIA to Complete the Transposition of the Data Protection Law Enforcement Directive," https://ec.europa.eu/commission/presscorner/detail/en/inf_20_859.

[61] C-658/19, Court of Justice of the European Union, February 25, 2021, ECLI:EU:C:2021:138.

[62] European Union, European Commission, First Report on Application and Functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ("LED"), COM/2022/364 final (Brussels: European Commission, 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022DC0364&from=EN.

[63] There is no constitutional provision with the same content.

[64] An example of such an exception is what the lawyer puts forward during the hearing.

[65] The data itself is often stored in police databases or at the Netherlands Forensic Institute (NFI).

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

to justify his rejection of a "plea against the use of unreliable evidence" in Article 359, paragraph 2 of the Dutch CCP, i.e., a defense objection to evidence. This means that if the judge decides *not* to exclude the contested evidence, he or she must give reasons why. The better the defense substantiates the plea of unreliability, the more an explanation is required from the court. Furthermore, there are the so-called minimum evidence rules in relation to statements. For example, the judge may not convict[66] on the basis of a statement by only one witness or by the suspect only. Because there is always a chance that the witness or the suspect will not tell the truth, the law requires a second piece of evidence for conviction. However, case law demonstrates that this requirement is very easily met.[67] A final and increasingly important example concerns criteria for assessing expert evidence. These criteria, developed by the Supreme Court, hold that if the reliability of expert evidence is disputed, the judge should examine whether the expert has the required expertise and, if so, which method(s) the expert used, why the expert considers that the method(s) is (are) reliable, and the extent to which the expert has the ability to apply that method in a professional manner.[68]

Apart from reliability, the legitimacy of evidence may also be challenged in court. Article 359a of the Dutch CCP provides for attaching 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 declare the case inadmissible for prosecution.[69] In practice, cases are almost never affected by unlawfully obtained evidence. Courts rarely impose consequences for unlawfully obtained evidence, and if they do, cases may not be affected by this, because the requirements the Supreme Court laid down in its case law regarding the scope of Article 359a of the Dutch CCP are rather restricted.[70]

[66] An important exception is that evidence that the suspect has committed the offense charged *can* – not *must* – be assumed by the judge on the basis of an official report by an investigating officer. See Dutch CCP, note 19 above, § 344(2).

[67] For an overview and interpretation of the case law, see the case note M. J. Borgers in Dutch Supreme Court, July 7, 2015, *NJ* 2015, 488, ECLI:NL:HR:2015:1817.

[68] HR 27 January 1998, *NJ* 1984, 404. Assessing the reliability of the ways in which data is secured may depend on the methods and technologies used; see e.g. Eric Van Buskirk & Vincent Liu, "Digital Evidence: Challenging the Presumption of Reliability" (2006) 1:1 *Journal of Digital Forensic Practice* 19.

[69] If the case is declared inadmissible for prosecution, the court will not allow litigation to start because the eligibility criteria of procedural criminal law are not met.

[70] See e.g. HR 19 February 2013, *NJ* 2013, 308; see also *Het Nederlands*, note 23 above, at 884–886.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

IV.B Current Court Practices: Increasing Use of Digital Evidence

Traditionally, statements of witnesses and suspects are important evidence in criminal cases. The general feeling is, however, that things are changing. Criminal investigations into organized crime in particular do not rely on witnesses, and investigations increasingly build a case by combining location data via phone locations or automatic number plate recognition, user data of phones and computers, the internet, etc.[71] The Dutch police increasingly and with success invest in "data-driven investigation," and high-tech detectives have gained access to various encrypted communication providers that were used by organized crime groups such as Ennetcom, EncroChat, and Sky ECC.[72] An international coalition of investigators even built their own communication app "Anom," which was gladly used by ignorant criminals. The downside of these celebrated successes, however, is that there is no capacity to read the millions of intercepted messages.[73]

Moreover, the absence of adequate rules discussed in Section II, and the legitimacy of digital investigation methods, are serious issues. But due to the restricted interpretation of Article 359a of the Dutch CCP (discussed above), the courts almost never attach a serious consequence to the fact that evidence was gathered illegally. Next, there is the problem of territorial jurisdiction.[74] The data in the Ennetcom-seizure, e.g., was owned by a Dutch company, but stored on a Canadian server. As a result of this, the Dutch police could not investigate the data without permission of the Canadian authorities. In order to comply with the Canadian judicial requirements for access to the data, the Dutch investigatory judge and the prosecutor interpreted the Dutch

[71] Desiree de Jonge, "Verdediging in tijden van digitale bewijsvoering" (Legal Defense in the Age of Digital Evidence) in Patrick Petrus Jacobus van der Meij (ed.), *Aan de slag. Liber amicorum Gerard Hamer* (The Hague, Netherlands: Sdu Uitgevers, 2018) 125 ["Verdediging"].

[72] See "Dutch Police 'Read' Blackberry Emails," *BBC News* (January 12, 2016), www.bbc.com/news/technology-35291933; Robert Wright, "Hundreds Arrested across Europe as French Police Crack Encrypted Network," *The Financial Times* (June 8, 2021).

[73] "Judicial System Overwhelmed after Gaining Access to Encrypted Chats," *NL Times* (June 14, 2021), https://nltimes.nl/2021/06/14/judicial-system-overwhelmed-gaining-access-encrypted-chats.

[74] In relation to investigation in the cloud, see also Jan-Willem van den Hurk & Sander de Vries, "Cybercrime. Waar worden gegevens in de 'cloud' opgeslagen en welke juridische consequentie heeft het antwoord op die vraag? Een speurtocht langs het traditionele juridisch kader en actuele wetgeving en jurisprudentie leidt tot een opmerkelijke conclusie" (2019) *Strafblad* 34.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

procedural rules very broadly. The defense objected, but in the end the trial judge authorized the course of action.[75]

Next to issues of legitimacy, digital evidence raises questions of reliability as well as on defense rights. We illustrate this with the case of the "Webcam blackmailer," in which the reliability of a keylogger and the right to equality of arms were both discussed.[76] In this case, the suspect was tried, among other things, for threatening and spreading sexual images of underage girls via the internet, as well as for extorting various males with information on them having "webcam sex." The discussion regarding the keylogger,[77] elaborately described in the verdict, clearly demonstrates the effort non-expert litigants have to make to understand how these kinds of technical devices work. To a large extent, they need to rely on expert witnesses for determining reliability. Even more interesting in this case are the attempts of the defense to get access to all the data that was found and produced by the police, including the complete copies that were made of the computers, all the results of the keylogger, all the Skype conversations with the victims, WE-logs, VPN-logs, etc. The defense brought forward an alternative scenario, and argued that in order to properly assess the selection and interpretation of the incriminating evidence, it is necessary to have access to all the data. Indeed, this request seems reasonable from the perspective of the right to equality of arms. All information that can be relevant for the case must be seen and checked by the defense. However, by Dutch law, the prosecution determines what is relevant and made available. This rule has always been the object of discussion between defense attorneys and prosecution, but this debate is given a new dimension in the context of big sets of technical data.[78] The police have their own software to search and select data, and they may not always be willing to provide insight into their investigative methods. Furthermore, the amount of data can be enormous, as in the Ennetcom, EncroChat, and Sky ECC examples above, and for that reason the effort to make it accessible for the defense will be too. There now seems to be a court policy developing in early cases in which decrypted data is used, allowing the defense to search the secondary dataset at the Netherlands Forensic Institute (NFI) with the

[75] See e.g. para. 6 of the verdict of the Court of Amsterdam, April 19, 2018, ECLI:NL:RBAMS:2018:2504.

[76] Court of Appeal Amsterdam, December 14, 2018, ECLI:NL:GHAMS:2018:4620.

[77] A keylogger is a device or software that registers, typically in a covert manner, all keystrokes on a keyboard.

[78] See also "Verdediging", note 71 above.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

search engine "Hansken."[79] Hansken was developed by the NFI to investigate large amounts of seized data. In the Webcam blackmailer case, the Court of Appeal dismissed the request of the defense with the argument that they were on a phishing expedition and had had plenty of opportunity to challenge the evidence. Nonetheless, this case illustrates that the Dutch CCP needs provisions to ensure insight into issues generated by automated data analysis, for the defense, but also for the judge.[80]

IV.C Developments in Society and Technology: New Issues of Quality and Assessment of Evidence

As observed in the beginning of the chapter, people are increasingly leaving digital traces everywhere all the time. People are often monitored without being aware of it, by camera surveillance systems, by their own smartphones, and on other devices they use to access the internet. This generates data that can be useful for law enforcement to collect evidence and to find out what happened in specific cases. In the Netherlands, many surveillance systems are in place for law enforcement to rely on. These are mostly private systems from which data is requested if needed.

The data we are referring to here is digital data, usually large amounts of data, in different formats such as statistics, as well as audio, video, etc., that can only be accessed via technological devices. In the past, forensic experts also provided technical data, such as fingerprints or ballistics, to criminal investigations and provided clarifications when testifying in courts, but the current use of data as evidence is significantly different. In the past, forensic data was collected in a very specific, controlled, and targeted way, mostly at the crime scene. Currently, it is possible to collect very large amounts of data, not necessarily specifically targeted to one individual or connected to a specific crime scene. For some of these relatively new data collection methods, no protocols even exist yet. In this subsection, we discuss three issues regarding the quality of evidence that arise as a result of the characteristics of digital data.

[79] See e.g. the rulings of the Court of Amsterdam, April 19, 2018 ECLI:NL:RBAMS:2018:2504 and April 1, 2021, ECLI:NL:RBAMS:2021:1507.

[80] See Koops-Commission, note 35 above, at 27; see also Maša Galič, "De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding" (Rights of the Defendant in the Context of Large Datasets and Advanced Search Engines in Criminal Cases) (2021) 2:2 *Boom Strafblad* 41 ["De rechten"].

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

The first issue concerns the reliability of data. Digital data can be volatile and manipulated, which means that the litigating parties and the judge would need an instrument to assess the originality of the data. This instrument can be found in procedures on how to seize digital data in a controlled and reproducible way. For example, when a copy of a hard disc of a computer is made, it is very important to have a fixed procedure or protocol, including timestamps, so that it is clear to all litigating parties that the data was not tampered with or accidentally altered. Even with such procedures and protocols in place, creating a copy of the data on a seized computer can be complicated. For example, Bitcoin and other cryptocurrencies cannot be copied, even though they are essentially data on a computer. Seizure of cryptocurrencies therefore requires specific protocols. Another technological issue is that of streaming data and data in the cloud. Such data can also be hard to record or securely copy, and if so, much depends on the timing. Forensic experts in the Netherlands and other countries are working on new methods and protocols for securing digital data. A detailed discussion is beyond the scope of this chapter.[81]

The second issue concerns the large amounts of data that can arise during criminal investigations in relation to the principle that the litigating parties need to have access to all relevant data, incriminating and exonerating. For example, in the Netherlands, law enforcement uses a significant amount of wiretapping to find clues for further investigation in criminal cases. This yields large amounts of data that can be hard to process by humans, as it would require listening to all audio files collected. Voice recognition technologies may be helpful to process such data in automated ways. Also, camera surveillance, including license plate recognition systems, may yield large amounts of data. Again, such data can be hard to process by humans going through all images. Analytics software may be useful to speed up such processes.

The large amounts of data routinely collected in criminal cases therefore calls for automated search and analysis. When using software tools to go through large amounts of data to find specific data or to disclose specific patterns, one problem may be that humans may find it hard to follow how the software works, particularly when such tools are very advanced. However, if it is not transparent how particular conclusions

[81] For more details, see e.g. Jan-Jaap Oerlemans, *Investigating Cybercrime*, PhD thesis, Leiden University (Leiden, Netherlands: Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University, 2017).

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

were drawn from the data, this could be an issue when such conclusions are used in courts as evidence.[82] According to the principle of equality of arms, it should be possible to contest all evidence brought up by any of the process parties. However, search and analysis tools may be programmed in such a way that they aim to find incriminating evidence in datasets, and there may be exonerating pieces of evidence in the databases that the tools may not show.[83]

A detailed legal framework may be lacking, but courts still seem increasingly reliant on experts and computer systems. A typical example here are risk assessment models, usually based on algorithms, that provide risk scores for recidivism rates. In several of the United States, the system Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is used to assess recidivism risks.[84] In their decisions, courts place considerable weight on these models, or rather the results they spit out. In the Netherlands, the probation services use a system called RISC (*Recidive inschattings schalen*). Part of that system is the Oxford Risk of Recidivism Tool, an actuarial risk assessment tool that can be used to predict statistical risks.[85] These models increasingly play a role in the work of probation services and the decisions of courts.

The use of such models offers several benefits, such as fair assessments done in more structured and objective ways. Subjective assessors can be prone to human failure or can be influenced by bias and prejudice. If the models are self-learning, they can also recognize and

[82] The increasing use of AI in a criminal law context can raise such issues; see Bart Custers, "Artificiële intelligentie in het Strafrecht: een overzicht van actuele ontwikkelingen" (Artificial Intelligence in Criminal Law: An Overview of Current Developments) (2021) 4 *Computerrecht* 330; for a more general discussion, see Daniel Solove, *The Digital Person; Technology and Privacy in the Information Age* (New York, NY: New York University Press, 2004). Regarding the interpretation of equality of arms in relation to large datasets, see "De rechten", note 80 above. See also *Sigurður Einarsson and others* v. *Iceland*, App. No. 39757/15, ECtHR (June 4, 2019); and see Sabine Gless, "AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials" (2020) 51:2 *Georgetown Journal of International Law* 195; Sabine Gless, Xuan Di, & Emily Silverman, "Ca(r)veat Emptor: Crowdsourcing Data to Challenge the Testimony of In-Car Technology" (2022) 62:3 *Jurimetrics* 285.

[83] Toon Calders & Bart Custers, "What Is Data Mining and How Does It Work?" in Bart Custers, Toon Calders, Bart Schermer *et al.* (eds.), *Discrimination and Privacy in the Information Society*, no. 3 (Heidelberg, Germany: Springer, 2013) 27. For more on the responsibility of programmers, see Chapter 2 in this volume.

[84] "Practitioner's Guide to COMPAS Core" (Northpointe, 2015), https://assets.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf.

[85] OXRISK, "OXREC: Oxford Risk of Recidivism Tool," https://oxrisk.com/oxrec-nl-2-backup/.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

incorporate new trends and developments. This ability obviously can also increase efficiency and reduce costs. However, there is also criticism of these instruments, because they do not seem to outperform assessments by human experts, and there are risks similar to human assessments, such as bias that can lead to discrimination.[86] In the United States, COMPAS seemed to systematically assign higher recidivism risks to Afro-Americans.[87] It is often argued that these models do not process any ethnicity data and, therefore, cannot be discriminating.[88] However, characteristics like ethnicity can easily be predicted and are therefore often reconstructed by self-learning technologies, without being visible to users.[89] Furthermore, it should be noted that the false positive rate for African-Americans is higher in COMPAS, but race has no predictive value. In other words, suspects from different ethnic backgrounds with the same risk score have the same risk of reoffense.

The third issue is related to difficulties in estimating the strength of the evidence. All datasets contain inaccurate data or gaps to some extent. Incorrect or incomplete data is not always problematic from a data analytics perspective, but it may reduce some of the accuracy and reliability of analysis results and thus affect the conclusions that can be drawn from it.[90] When based on large amounts of data, some minor errors and gaps in the data will hardly affect the final results. However, in cases of limited data, errors might have crucial impacts on the evidence. For example, cell phone data can be used in a court case to prove

[86] Gijs Van Dijck, "Algoritmische risicotaxatie van recidive: Over de Oxford Risk of Recidivism tool (OXREC), ongelijke behandeling en discriminatie in strafzaken" (Algorithmic Risk Assessment of Recidivism) (2020) 95:25 *Nederlands Juristenblad* 1784.

[87] Julia Angwin, Jeff Larson, Surya Mattu *et al.*, "Machine Bias," *ProPublica* (May 23, 2016), www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[88] Marjolein Maas, Ellen Legters, & Seena Fazel, "Professional en risicotaxatie-instrument hand in hand: hoe de reclassering risico's inschat" (Professional and Risk Assessment Work Together: How Probation Organisations Assess Risks) (2020) 1814 *Nederlands Juristenblad* 2055.

[89] Cf. Faisal Kamiran, Toon Calders, & Mykola Pechenizkiy, "Techniques for Discrimination-Free Predictive Models" in Bart Custers, Toon Calders, Bart Schermer *et al.* (eds.), *Discrimination and Privacy in the Information Society*, no. 3 (Heidelberg, Germany: Springer, 2013) 223.

[90] Bart Custers, "Effects of Unreliable Group Profiling by Means of Data Mining" in Gunter Grieser, Yuzuru Tanaka, & Akihiro Yamamoto (eds.), *Lecture Notes in Artificial Intelligence*, vol. 2843 (Berlin, Germany; New York, NY: Springer-Verlag, 2003) 290; for more on malfunctioning technology, which is also related to reliability, see Chapter 13 in this volume.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

that a suspect was at the crime scene at a particular time. If this conclusion is based on data from three cell phone masts, but one of them is unreliable, then the result may not be entirely accurate. The conclusion could be, e.g., that the probability that the suspect can be pinpointed to the location is 75 percent. This problem with accuracy also brings in all the assessment problems that humans, including judges, may have when dealing with probabilities and risks, including the so-called prosecutor's fallacy and the defense attorney's fallacy.[91]

Despite all these issues, the changing technological landscape does provide many opportunities for the use of data as evidence in courts. When used properly, the use of data could be more objective than the use of statements from suspects, victims, and witnesses.[92] People may easily forget specific details of a past situation and their memories may even distort after some time. Many psychological mechanisms might be at play. In very stressful situations, when people are the victim of a crime or witnessing serious crime, they may experience time in different ways, often thinking it takes longer than in reality, or they may invoke coping mechanisms that block particular information in their brains. Witnesses who are not directly involved in a crime they are witnessing may be paying less attention to details, and the evidence they can produce in their statements may therefore be limited. Research has shown that memories also fade over time for all actors.[93]

Objective digital data, e.g., from cell phones, may easily fill in the blanks in people's memories and rectify any distortions that have occurred. Such data can readily confirm where people were at a particular moment and can disclose connections between people. The data can help prove that some statements are wrong or confirm that some statements are indeed correct. Data can also help to avoid tunnel vision and other biases that law enforcement officers conducting criminal investigations may have.

[91] Both fallacies are errors in statistical reasoning involving a test for an occurrence, such as a match in fingerprints or DNA; the prosecutor's fallacy exaggerates the probability of a criminal defendant's guilt, whereas the defense attorney's fallacy typically underestimates it. See William Thompson & Edward Schumann, "Interpretation of Statistical Evidence in Criminal Trials: The Prosecutor's Fallacy and the Defense Attorney's Fallacy" (1987) 11 *Law and Human Behavior* 167.

[92] The same applies to statements and testimonies by robots; see Chapters 6 and 8 in this volume.

[93] Geralda Odinot, Amina Memon, David La Rooy *et al.*, "Are Two Interviews Better than One? Eyewitness Memory across Repeated Cognitive Interviews" (2013) 8:10 *PLoS ONE* e76305.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

Altogether, the use of data as evidence in courts can be a valuable asset. It can be more accurate, detailed, unprejudiced, and objective than statements. But this is only the case if some of the pitfalls and issues mentioned above are properly avoided. Data can be manipulated, the tools for analysis can be biased and discriminating, and the probabilities resulting from any analysis can be subject to interpretation fallacies.

Regarding categories of evidence, in general we see an increase in the use of data as evidence in courts, but not necessarily a decrease in the use of statements from suspects, victims, and witnesses. This decrease is not to be expected any time soon, as statements remain important, for more than evidentiary reasons, such as the procedural justice experienced by all parties in court. As such, the use of data as evidence is a valuable addition to statements, but not a replacement.

The European Union seems to expect that data as evidence will become increasingly important. A relevant development on the EU level that needs to be discussed here is the draft Regulation on e-evidence.[94] To make it easier and faster for law enforcement and judicial authorities to obtain electronic evidence needed to investigate and eventually prosecute criminals and terrorists, the European Commission proposed new rules in April 2018 in the form of a Regulation and a Directive. Both proposals focus on swift and efficient cross-border access to e-evidence, in order to effectively fight terrorism and other serious and organized crime.[95] The proposal for the directive focuses on harmonized rules for appointing legal representatives when gathering evidence in criminal proceedings.[96] The proposal for the regulation focuses on European production and preservation orders for electronic evidence in criminal matters.[97] The production order will allow judicial authorities to obtain electronic evidence

[94] European Union, European Commission, Proposal for a Regulation of the European Parliament and of The Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM/2018/225 final – 2018/0108 (COD) (Strasbourg: European Commission, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN [Production and Preservation].

[95] European Council, "European Council Conclusions, 18 October 2018" (October 18, 2018), www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/.

[96] European Union, European Commission, Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, COM/2018/226 final – 2018/0107 (COD) (Strasbourg: European Commission, 2018).

[97] Production and Preservation, note 94 above.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

directly from services in other Member States. These legal instruments have not yet been adopted by the European Union, as strong privacy, data protection, and privacy safeguards are still under scrutiny. However, it may be expected that, once adopted, this regulation will further increase the use of electronic evidence in court cases in the European Union over the next few years.

V Conclusion

In this chapter, we focused on the increasing discrepancy between legal frameworks and actual practices regarding the use of data as evidence in criminal courts. The two legal frameworks under consideration are criminal law and data protection law. Since the EU harmonization of criminal law is very limited, we used the example of the Netherlands to further examine the use of data as evidence in criminal courts. Even though the Netherlands is a front runner in the areas of privacy and data protection law, as well as digital forensics and cybercrime, large parts of its criminal law were developed before digital evidence existed. Data protection law, which is more recent, is highly harmonized throughout the European Union via the GDPR and the LED.

The two major legal frameworks of criminal law and data protection law are not fully integrated and adjusted to each other. There seems to be a structural ambiguity here. When it comes to regulating data as evidence, these frameworks together need to cover three separate but intertwined activities: (1) collection of data; (2) processing and analysis of data, including storage, selecting, combining; and (3) evaluation of data.[98] In the Netherlands, the Dutch CCP covers the collection and evaluation, while the processing is mainly the domain of the Wpg and Wjsg in accordance with the LED.

Based on the analysis of the existing legal frameworks, the actual use of data as evidence in criminal courts, and developments in society and technology, we have four major observations, regarding the final aspect of our research question: i.e., what is needed next. A first observation regarding regulation is that the existing legal frameworks in the Netherlands barely or not at all obstruct the collection of data for evidence. Hence, the legal

[98] Obviously, this is a simplification. A more detailed analysis would need to include more steps, such as access to data, access to evaluations of data, destruction of data, etc.; cf. David Gray, *The Fourth Amendment in an Age of Surveillance* (Cambridge, UK: Cambridge University Press, 2017).

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

frameworks essentially allow law enforcement agencies and public prosecutors to make use of the opportunities that data can offer as evidence in criminal courts. Although many digital investigation methods are not provided for in the Dutch CCP, and as a result, fundamental issues on privacy are debated, this seems to have few consequences for the legitimacy of data as evidence in specific cases. This is partly due to the fact that, in the Netherlands, illegally gathered evidence rarely leads to serious consequences. The Supreme Court case law thus reflects the importance given to crime fighting. Another explanation is that the debate on how to define and protect the right to digital privacy within criminal procedure is still in its infancy.

Our second observation is that regulation regarding collection via the Dutch CCP and regulation on processing and analysis via the Wpg and Wjsg is not integrated. As with other written law, these legal frameworks use different language and definitions, have different structures, and lack any cross-reference to one another. The Dutch CCP is not specifically aimed at what can be done with data once collected, but what can be done with data is also relevant for the evaluation of the extent of the privacy intrusion, and hence the design of the investigation powers. An integrated approach is also necessary for other reasons. Under data protection law, data subjects have a series of data subject rights they can invoke, such as the right to information, transparency, and access. These rights can be somewhat of a farce, as people may not know about them and how to invoke them and, if they do, they may be blocked in cases where a criminal investigation is still ongoing.[99]

Our third observation concerns the absence of regulation of automated data analysis during all stages in the criminal justice system, including the prevention, investigation, detection, or prosecution of criminal offenses, the use of data as evidence in criminal courts, and the execution of criminal penalties. Automated data analysis raises fundamental questions regarding the equality of arms, and because all parties should have access to all relevant data and be able to assess data selection, we would like to argue that introducing some additional provisions for regulating data analytics, subsequent to data collection, would be appropriate. We have not seen any similar provisions in the legislation of other EU Member States,[100] but we did encounter an example of such

[99] "Conceptual Issues", note 44 above.

[100] Bart Custers, Francien Dechesne, Alan M. Sears *et al.*, "A Comparison of Data Protection Legislation and Policies across the EU" (2017) 34:2 *Computer Law & Security Review* 234.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

a provision in the Dutch Intelligence Agencies Act (*Wet Inlichtingen- en Veiligheidsdiensten*).[101] Article 60 of this Act states that the Dutch intelligence agencies are empowered to perform automated data analytics on their own datasets and open sources. The data can be compared and used for profiling and pattern recognition. Since no similar provision exists in criminal law, it is unclear whether law enforcement agencies are allowed to do the same. We are not arguing that they should or should not be allowed to do this, but we would like to argue that there should be more clarity regarding this issue.

The absence of regulation of data analysis raises issues regarding privacy and data protection of the data subjects whose data is being processed, but it can also raise issues regarding equality of arms during litigation in courts. Normally, suspects have access to all evidence brought forward in their case, including any data underlying the evidence. In practice, defendants may only get what prosecutors grant them, and they may not be aware of what is missing. Furthermore, if data analysis is based on large amounts of data, and that data includes the data of others,[102] a suspect may not be granted access to it; the GDPR prevents this in order to protect privacy and personal data. As a result, a suspect may not have full transparency regarding the data on which the analysis was based and may be unable to reproduce the analysis.[103] If the data analytics involve very sophisticated self-learning technology such as AI, the prosecutor may not even know how the data analysis took place.

Finally, as a fourth observation, what may also need further attention is the level of court expertise in dealing with digital data as evidence. Given

[101] *Wet Inlichtingen- en Veiligheidsdiensten* (Intelligence Agencies Act), 2017, Netherlands (as amended 1 January 2022).

[102] E.g. risk assessments of individuals can only be made in comparison with data of others; typically, a suspect has a high risk *in comparison with* other suspects or the general population.

[103] In the United States, a joint working group of the Department of Justice and the Administrative Office of the US Courts drafted guidelines for electronically stored information discovery production in federal criminal cases and how to inform defendants at an early stage about this; see US Department of Justice and Administrative Office of the US Courts Joint Working Group on Electronic Technology in the Criminal Justice System, "Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases" (Washington, DC: Department of Justice, 2012), www.uscourts.gov/sites/default/files/finalesiprotocolbookmarked.pdf. Because technology changes rapidly, there are no specific requirements for the manner or timing of the disclosure of the information. Instead, organizations in the criminal law system are required to develop best practices.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

the increasing importance of data as evidence in criminal courts, it is imperative that judges understand some of the basics of how data is collected and processed before it results in the evidence that is presented to them. In order to evaluate the reliability and strength of the data-evidence, they have to be very aware of any of the pitfalls and issues mentioned in the previous section. Judges should be able to contest different types of data brought forward as evidence, even if the data is not contested by any of the litigating parties. For this reason, further training in this area may be important, as well as procedural rules identifying the basis for judicial assessment of how data was seized.

In view of these observations, we conclude that, on the one hand, there are perhaps no major obstructions in the existing legal frameworks for the use of data as evidence in criminal courts, but that, on the other hand, much of this area is in practice still a work in progress. In order to find the right balance between the interests of law enforcement and the rights of subjects in criminal cases, further work is needed. Further work would include research, but obviously also the development of case law, as the balancing of interests approach is at the heart of what courts do, most notably supreme courts, and particularly in search and seizure jurisprudence. Since criminal law and data protection law are more or less separate legal frameworks, they need to be further aligned, not necessarily by adjusting the legislation, but at least in detailing the actual practices and policies of law enforcement agencies further. The absence of any regulation regarding automated data analysis is a major concern and may have considerable consequences for data subjects and their rights in criminal cases. We suggest that, after further research, regulation be considered. Regulation can be done via legislation, but perhaps also via policies. And, finally, further training of actors in courts may be required to make all of this work.

When looking at the developments in society and technology, we expect that the use of data as evidence in courts will significantly increase in the coming decades. This means that the issues identified in this chapter, such as limited effectiveness of data subject rights provided in the LED and issues regarding the principle of equality of arms during litigation, may become more pressing in the near future. It is therefore important to further prepare both courts and law enforcement agencies for these challenges, as suggested above.

However, having said this, we do not expect that the use of other types of evidence in criminal courts, such as statements from suspects, victims,

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press

or witnesses, will fall out of use. We think it is important to consider the use of digital evidence in criminal courts as an addition to the use of statements and other types of evidence, not as a replacement. Humans seek to understand evidence by means of stories, which means that regardless of its digital nature, data will always need to fit into a story – the stories of suspects, victims, and witnesses.[104]

[104] Kiel Brennan-Marquez, "Plausible Cause: Explanatory Standards in the Age of Powerful Machines" (2017) 70:4 *Vanderbilt Law Review* 1249.

https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press



https://doi.org/10.1017/9781009431453.014 Published online by Cambridge University Press