# eLaw
# Working Paper Series

No 2021/00" - ELAW– 2021

**`tq,a q,{r,Pm¡m,m ,Q£upqzoq,uz,P¢¡ot, O~uyuzmx,O{¢~¡**

O¢ ¡q~ ,N:T:Y:,mzp,_¡q£qz ,X:,

Universiteit Leiden
eLaw

Discover the world at Leiden University

BRILL
NIJHOFF

EUROPEAN JOURNAL OF CRIME, CRIMINAL LAW AND CRIMINAL JUSTICE 29 (2021) 25-46

brill.com/eccl

# The Use of Data as Evidence in Dutch Criminal Courts

*Bart Custers*
Professor of Law and Data Science, eLaw - Center for Law and Digital Technologies, Leiden University, Leiden, The Netherlands
*b.h.m.custers@law.leidenuniv.nl*

*Lonneke Stevens*
Professor of Criminal Law and Criminal Procedure, Department of Criminal Law & Criminology, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands
*l.stevens@vu.nl*

## Abstract

Digital traces that people leave behind in our digitalized society can be useful evidence in criminal courts. The central question of this article (how is the use of data as evidence in Dutch criminal courts regulated and, considering how these courts deal with such data as evidence in practice, what is needed?) is answered by analyzing the relevant legal frameworks for processing data in Dutch criminal courts: criminal law and data protection law. Next, current court practices are examined, by looking at typical case law and current developments in society and technology. Comparing the legal framework and actual practices, we conclude that the existing legal framework in the Netherlands does not obstruct the collection of data for evidence, but that regulation on collection (in criminal law) and regulation on processing and analysis (in data protection law) are not integrated. Remarkable is the almost complete absence of regulation of automated data analysis – in contrast with the many rules for data collection.

## Keywords

Dutch criminal law – Dutch criminal procedure – data as evidence – law enforcement directive – directive 2016/680 – witness statements

## 1 Introduction[1]

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'.[2] Lots of data can be retraced to find out more about the whereabouts, behavior, networks, intentions and interests of people. Such information can be very useful in a criminal law context, mainly for guiding criminal investigation (as it may provide clues on potential suspects, witnesses, etc.) and for evidence in courts (as the data may confirm specific actions and behavior of actors). Or, in other words, to find out what exactly happened (finding the truth) and trying to prove this (providing evidence). This article focusses on the use of such (digital) data as evidence in criminal courts. The large amounts of potentially useful data may cause a shift in the types of evidence presented in courts, with 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.[3] Hence, this article tries to answer the question: how is the use of (digital) data as evidence regulated in Dutch criminal courts and, considering how these courts deal with such data as evidence in practice, what is needed?

We 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, but also identify caveats and several 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 jurisdictions and similar across countries. This also applies to the forensic standards that are applied, these also have an international scope and nature, usually established by international standardization organizations (like ISO, CEN-CENELEC and ETSI) or, if created on a national level, often at least aligned by 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 EU. Criminal law may not be harmonized that much across the EU, but the norms

1 The authors would like to thank prof.dr.iur. Sabine Gless for feedback on a previous version of this article. The idea for this article was initiated by the project (Ro)Bot-Human Interaction, funded by the Swiss National Research Foundation, that she is leading.

2 Schneier, B. (2013) The Battle for Power on the Internet, *Internet and Security* 19. https://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

3 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.

and standards for evidence and fair trial are fleshed out in a large amount of ECHR and CJEU case law. All this means that the basic situation regarding technology and forensic practices and the legal boundaries are more or less the same across the EU, but national interpretations and practices within these confines may vary.

The central question of this article (how is the use of data as evidence in Dutch criminal courts regulated and, considering how these courts deal with such data as evidence in practice, what is needed?) is firstly and mainly answered by analyzing the relevant legal frameworks for processing data in Dutch criminal courts, which are Dutch criminal (procedure) law and Dutch data protection law. After this legal analysis, also current court practices are examined, mainly by looking at typical case law and current developments in society and technology.

This article is structured as follows. Section 2 provides a brief general introduction to procedural Dutch criminal law. Section 3 provides a brief general introduction to Dutch data protection law, focusing on the implementation of the GDPR and the Law Enforcement Directive respectively. Section 4 investigates the actual use of evidence in Dutch criminal courts by focusing first on current court practices, including case law, and second on current developments in society and technology. Section 5 provides an analysis comparing and contrasting 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.

## 2 Dutch Criminal Procedure Law

The Dutch Code of Criminal Procedure (CCP) dates back to 1926. Back then the Code was characterized as 'moderately accusatorial' since it introduced more rights for the defense.[4] The suspect however, remains to a large extent the object of investigation. This is especially the case in the stages of police investigation, before the start of the trial. Although over the years more possibilities to influence the earlier investigation were introduced – such as the right to contra-expertise during police investigation (article 150b CCP) – the defense and the prosecutor are far from equal parties. Basically, the margins for the defense largely depend on the prosecutor's goodwill. Therefore, a more accurate description of Dutch criminal procedure

4 See L. Stevens, *Het nemo-teneturbeginsel in strafzaken: van zwijgrecht naar containerbegrip* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2005, chapter 3.

would be: 'moderately inquisitorial'.[5] Fundamental to the position of the defense is his right to silence (article 29 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 CCP. They apply however, directly to Dutch criminal procedure through article 6 of the European Convention on Human Rights.

The CCP has been amended and supplemented many times since 1926. As a result, the CCP now looks more like a patchwork-style Code instead of structured and clear-cut. This is also one of the reasons the legislator started the (still running) major project 'Modernisation Criminal Procedure' (Modernisering Strafvordering) in 2014. The idea is to revise the CCP in order to make criminal procedure, amongst other things, more accessible and efficient.[6] Another aim of the revision is to tackle one of the greater challenges criminal procedure faces nowadays: keeping up with technological developments in criminal investigation practice and developing an overall framework for regulating criminal investigation in the digital era. The CCP is still very much an analogue-style Code that regulates the searching of homes, the seizure of letters, wiretapping, the questioning of witnesses, etc. Although various digital investigation methods can be conducted on the basis of existing powers (for example, a computer that was seized in a home can be searched just like a diary or a pistol that was seized in a home),[7] and several new digital investigation methods have been laid down in the CCP (e.g. the network search of art. 125j CCP; or the hacking powers in 126nba CCP[8]), many methods are still left unregulated. Some gaps are filled (provisionally; awaiting legislation) by the Supreme Court in cases the defense questions 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' (article 94 and 95 CCP) *can* be the basis of a smartphone search under the condition that the infringement on the right to privacy

5 G.J.M. Corstens, M.J. Borgers, T. Kooijmans, *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2018, p. 10.

6 See www.rijksoverheid.nl/documenten/publicaties/2017/11/13/documenten-moderniseringwetboek-van-strafvordering and www.moderniseringstrafvordering.nl/.

7 See B.J. Koops & J.J. Oerlemans, 'Formeel strafrecht en ICT', p. 125–127, in B.J. Koops & J.J. Oerlemans (red.), *Strafrecht en ICT*, Den Haag: Sdu Uitgevers 2018.

8 Introduced with the 'Cybercrime Law III", Law of 27 June 2018, *Staatsblad* 2018, 322, in force since March 2019. See also Pool, R.L.D., and Custers, B.H.M. (2017) The Police Hack Back: Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime, *European Journal of Crime, Criminal Law and Criminal Justice,* 25 (2017), p. 123–144.

remains minor.[9] In case the infringement is more than minor a search should be conducted or authorized by the public prosecutor. When it is foreseeable that the privacy-infringement will be 'profound' ('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 CCP. This article states that criminal procedure can only take place as foreseen by law,[10] which means that the police cannot use investigation methods – that is: those that infringe fundamental rights – that are not explicitly grounded in a (sufficiently detailed and explicit) statutory investigation power. However, investigation methods that are not explicitly regulated in the CCP (like the seize and search powers in article 94 and 95 CCP mentioned above) and that only cause minor infringements can be based on article 3 Police Act.[11] This article contains the general task description of 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'). In case law several (digital) investigation methods have been ruled to constitute only a minor infringement and therefore did not need to be explicitly regulated. For example, sending stealth text messages[12] to someone's cell phone can in principal 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.[13] The Smartphone-case (in which a very general power to seize is found to be a sufficient statutory basis for a limited smartphone search) builds upon this settled case law. On his turn, the 'Modernisation' legislator incorporates the so called 'pyramid-structure' of the Smartphone-case – i.e. a larger privacy infringement (minor, major, profound) demands a higher authority (police, prosecutor, investigatory judge) – in its legislative draft on digital investigation. Minor intrusions do not have to be explicitly regulated, while major and profound intrusions are in need of more detailed and stringent legislation. To distinguish minor privacy intrusions from major privacy intrusions the legislator uses the concept of 'systematicness'

9 ECLI:NL:HR:2017:584, Supreme Court of the Netherlands, 4 April 2017, *NJ* 2017, 229. See also the case note of L. Stevens, Onderzoek in een smartphone. Zoeken naar een redelijke verhouding tussen privacybescherming en werkbare opsporing', *Ars Aequi* 2017, p. 730–735.

10 'Law' meaning formal acts of Parliament.

11 Corstens/Borgers/Kooijmans 2018, p. 29–30.

12 Sending an 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.

13 ECLI:NL:HR:2014:1563, Supreme Court of the Netherlands, 1 July 2014, *NJ* 2015, 114.

(*stelselmatigheid*).[14] A police officer is allowed to search a computer (e.g. a smartphone) except when the search is foreseeably systematic. A systematic computer search has to be ordered by the public prosecutor. In comparison, cloud searching can only be done by order of the prosecutor.[15]

## 3 Dutch Data Protection Law

### 3.1 *GDPR and LED*

In 2016, the EU issued the final text for the General Data Protection Regulation (GDPR), revising the EU legal framework for personal data protection. This legislative instrument is directly binding for all EU Member States and its citizens.[16] To a large extent, the GDPR carried over the contents of the EU Data Protection Directive from 1995 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 EU also issued with comparatively little fanfare Directive 2016/680 on protecting personal data processed for the purposes of law enforcement.[17] This directive, referred to as the Law Enforcement Directive (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. In this section, we discuss the implementation of the GDPR and the LED respectively in the Netherlands.

14 It was initially the Commission 'Modernisation of criminal investigation in the digital era' (Koops-Commission) that suggested the use of *systematicness* as structuring concept. See the advice 'Regulering van opsporingsbevoegdheden in een digitale omgeving', s.l. 2018.

15 See Legislative proposal 'Conceptwetsvoorstel Boek 2 onderdeel opsporing in een digitale omgeving', article 2.7.3.2.2 and 2.7.3.2.3.

16 European Parliament and Council Regulation (EU) 2016/679 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.

17 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penal- ties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89 ('LED').

### 3.2 *Implementation of the GDPR*

Since the GDPR is directly binding for all Member States and its citizens, strictly speaking, no further implementation is required. Nevertheless, the Netherlands, implemented the GDPR Execution Act (Uitvoeringswet AVG) in 2018, 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 relating to legal persons. Data on deceased people is not personal data and therefore beyond the scope of the GDPR.[18] 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 (art. 5.1). Furthermore, the purposes for which the data are collected and processed have to be stated in advance (purpose specification) and 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 (accountability, art. 5.2).

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 (art. 12–14), a right to access to their data (art. 15), a right to rectification (art. 16), a right to erasure (art. 17), a right to data portability (art. 20), and a right not to be subject to automated decision-making (art. 22).

The GDPR is relevant in a criminal law context for all data controllers that are not within the scope of the LED Directive. For instance, private investigators and government agencies in the migration domain are subjected to the GDPR. Also, for instance, when companies apply camera surveillance or other technologies that collect personal data, the data collected and processed is subject to the GDPR. As soon as the police or the public prosecution service requests such data for criminal investigation, the data get in the scope of the LED rather than the GDPR. Law enforcement agencies can request data from

18 E. Harbinja, *Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?*, 10 SCRIPTED 19 (2013).

individuals and companies at any time during a criminal investigation, but handing over such data is on a voluntary basis. Only when law enforcement agencies have obtained a court warrant, handing over the data is mandatory. If relevant, any such information may be used as evidence in court cases.

### 3.3 *Implementation of the Law Enforcement Directive*[19]

In 2012 the European Commission presented the first draft for a Directive that would harmonize the processing of personal data in criminal law matters.[20] After that, a debate started between the European Parliament, the Commission and the Council, which took four years. In 2016 the legislative proposal was adopted, after amendments, in its current version as EU Directive 2016/680. In this Directive the deadline for implementation in national legislation is two years, with a final deadline in May 2018. Directive 2016/680 (the LED) repealed the Framework Decision 2008/977/JHA as of that date.

The aim of the LED is two-fold: 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, more in general, effectively addressing 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 and 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, and;

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 of- fences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

19 This section is partially based on Leiser, M.R. and Custers, B.H.M. (2019) The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, *European Data Protection Law Review*. Vol. 5, nr. 3, p. 367–378.

20 Proposal or 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 [2012] COM(2012) 10 final.

Perhaps the most obvious competent authorities are police forces and public prosecution services, but there may be a variety of competent authorities in national criminal law of EU Member States. For instance, 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 offences 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 instance, 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 (Article 4 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.

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 offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Some of these principles are problematic, particularly when data are transferred from a GDPR regime into the context of law enforcement[21] 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.[22] Whereas the GDPR is not very specific about time limits for

21 C Jasserand (2018) Subsequent Use of GDPR Data for a Law Enforce- ment Purpose: The Forgotten Principle of Purpose Limitation? 4(2) *European Data Protection Law*, p. 152–167.

22 C Jasserand (2018) Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in Directive 2016/680? 34(1) *Computer Law & Security Review* 154–165.

data storage and review,[23] the LED requires clear establishment of time limits for storage and review.[24] 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) 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.[25] Storage time limits vary across Member States and for different situations, including different types of data subjects and different crimes. For instance, 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.[26] Data on whistleblowers and informants can only be stored for one year, but can be extended to three years. For instance, 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 are necessary for the police tasks.[27] In the United Kingdom, Section 39(2) of the Data Protection Act 2018 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.

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. Also the use of perpetrator profiles and risk profiles is explicitly protected.

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

23 GDPR, 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 data subject on storage times if they inquire about this.

24 LED, art 5. See also T Quintel, 'European Union – Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive' (2018) 4(1) EDPL 104–109.

25 WP29, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) (20 November 2017) WP 2017/258.

26 Bundesgrenzschutzgesetz 1994, art 35.

27 Wet Politiegegevens, art 8.

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) regulates the use of personal data for police agencies and the Justice and Prosecution Data Act (Wet justitiële en strafvorderlijke gegevens, Wjsg) 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 few changes were required. Also, the rights of data subjects, international cooperation and supervision by data protection authorities were already regulated. Elements that were still missing, were concepts like Privacy by Design, Privacy by Default and Privacy Impact Assessments.[28] Although, the Netherlands already introduced data breach notification laws in 2016, prior to the GDPR, these did not apply to the police, prosecution services and the judiciary.

Across the EU, the implementation of the LED in national legislation goes 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 have implemented the directive with some delay: the revised Wpg and Wjsg came into force on January 2019, more than half a year after the May 2018 deadline. Other countries, like Belgium, Finland and Sweden were later, but have implemented the directive by 2019. However, there is also a group of countries, including Spain, France, Latvia, Portugal and Slovenia, that have not yet realized implementation by early 2020.

28 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, for instance, 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.

## 4 Evidence in Dutch Criminal Law

### 4.1 *The Basic Principles of Dutch Evidence Law*

The evidentiary system in criminal cases is based on the principle of establishing the substantive truth. This is expressed in the CCP by the requirement that a judge may assume that the offense charged is proven only if he 'is convinced'.[29] 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 Code of Criminal Procedure considers admissible in criminal proceedings. It concerns: the judge's own perception, statements by the suspect, statements by a witness, statements by an expert, and written documents (article 339 CCP). This summary is so broad that hardly any evidence can be indicated that the law does not consider admissible.[30] Digital data as evidence will usually be submitted in the form of written police statements that report the results of an investigation.

There are only few rules in the CCP that govern the reliability of evidence. Relevant for any kind of evidence is the obligation for the judge to motivate his rejection of a 'plea against the use of unreliable evidence' (article 359 par. 2 CCP). Furthermore, there are the so-called minimum evidence rules in relation to statements. The judge may not convict[31] 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 to be used for conviction. However, case law demonstrates that this requirement is very easily met.[32] A final and increasingly important example concerns criteria for assessing expert evidence. These criteria were developed by the Supreme Court and 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.[33]

Apart from reliability, the legitimacy of evidence may also be challenged in court. Article 359a CCP provides for attaching consequences to the unlawful

29 There is no constitutional provision with the same purport.

30 An example of such an exception is what the lawyer puts forward during the hearing.

31 An important exception is contained in the rule that evidence that the suspect has committed the offence charged *can* – not *must* – be assumed by the judge on the basis of an official report by an investigating officer. See Section 344(2) CCP.

32 See for an overview and interpretation of the case law: the case note of M.J. Borgers in *NJ* 2015, 488.

33 Supreme Court of the Netherlands, 27 januari 1998, *NJ* 1984, 404.

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. In practice, cases are almost never affected by unlawfully obtained evidence. Due to the requirements the Supreme Court laid down in its case law the scope of article 359a CCP is rather restricted.[34]

### 4.2 *Current Court Practices: Increasing Use of Digital Evidence and Old Problems in a New Guise*

Traditionally, statements of witnesses and suspects are important evidence in criminal cases. The general feeling is, however, that things are changing. Especially criminal investigations into organized crime do not rely on witnesses, but increasingly build a case on (combining) location data (e.g. via phone locations or automatic number plate recognition), user data of phones and computers, the internet, etc.[35] Moreover, criminal law practitioners believe that suspects more often use their right to silence or bring forward an alternative explanation of the evidence. It can be questioned whether this is actually the case. Possible causes for supposedly increased use of the right to remain silent are thought to be 'television series or Netflix' and the presence and advice of the lawyer during the early stages of police questioning. Dutch empirical research does not substantiate these assumptions. It also shows that the correlation between legal representation and silence are better to be understood in terms of various 'mechanisms depending on the circumstances of a case'.[36] The silent or denying position of the defense could also be related to the increased use of trace evidence such as DNA and the aforementioned location and user data. This kind of evidence is often indirect: there is no ready-made story on the basis of direct evidence (like when a suspect or witness explains that, how, when en why 'he did it'). Instead, the police and the judge have to connect the dots and build a guilty scenario. This usually leaves room for the suspect or his lawyer to bring forward an alternative explanation of the data. An interesting example in this respect is a case in which a woman was convicted for murdering her husband.[37] From telecom data, user activities, and location data of the

34 See for example Supreme Court of the Netherlands, 19 February 2013, *NJ* 2013, 308. See also Corstens/Borgers 2018, p. 884–886.

35 D.N. de Jonge, 'Verdediging In tijden van digitale bewijsvoering', in P.P.J. van der Meij e.a. (red.), *Aan de slag. Liber amicorum Gerard Hamer*, Den Haag: Sdu Uitgevers 2018, p. 125.

36 See C.M. Klein Haarhuis e.a., *Langetermijnmonitor 'Raadsman bij verhoor'*, WODC 2018, p. 97–98. See also L. Stevens & W.J. Verhoeven, Rechtsbijstand bij het politieverhoor, in: *Encyclopedie Empirical Legal Studies*, forthcoming 2021.

37 See District Court of North-Netherlands, 11 July 2019, ECLI:NL:RBNNE:2019:2986.

suspect's Google Account she could be located close to the crime at the time of the murder. The data from the victim's Google Account showed the exact moment at which the mobile phone was moving and later came to a standstill at the crime scene – presumably the moment the victim was hit by the hard object that caused his death. The suspect denied fiercely, pleaded that the data allowed for multiple scenarios, and appealed against the conviction.

Besides interpretation issues, digital data raise old questions in new guises. This concerns not only issues of reliability and legitimacy of digital evidence, but also discussion on the scope of the procedural rights of the defense in relation to the use and gathering of digital information. For example, the reliability of a keylogger and the right to equality of arms were both discussed in the 'Webcam blackmailer case'.[38] In this case the suspect was tried, amongst 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'. In this case, the discussion on the keylogger[39] – elaborately described in the verdict – particularly 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 its reliability. Even more interesting in this case are the attempts of the defense to get access to *all* the data that were found and produced by the police: 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 – that brought forward an alternative scenario – claims 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 lawyers and prosecution, but this debate is given a new dimension in the context of (big) technical data.[40] The police have their own software to search and select data and may not always be willing to provide insight in their investigative methods. Furthermore, the amount of data can be enormous and for that reason the effort to make it accessible for the defense will be too. In the Webcam blackmailer case, the Court of Appeal dismissed the request of the defense

38 Court of Appeal Amsterdam, 14 December 2018, ECLI:NL:GHAMS:2018:4620.

39 A keylogger is a device or software that registers, typically covert, all keystrokes on a keyboard.

40 See also De Jonge 2018.

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 CCP needs provisions to ensure insight – for the defense but also the judge – into decisions that were generated by automated data analysis.[41] For now, practice has to be resourceful and in this respect one specific case is worth mentioning.[42] This case is related to the 'PGP-files' investigation in which the Dutch police managed to decrypt millions of data items from Blackberry phones.[43] The phones were protected with PGP (Pretty Good Privacy) software and therefore a popular communication device within criminal organizations. Drug deals and liquidations could be secretly discussed. The suspect in this case was tried for, i.a., attempted murder and money laundering and several PGP-messages were part of the evidence. The messages that were relevant for evidence were selected with the help of 'Hansken' – a search engine that was developed by the Netherlands Forensics Institute (NFI)[44] to investigate large amounts of seized data. Accompanied by its own expert the defense visited the NFI twice, was given a presentation about the software, and could perform a (limited) search in the PGP protected data.

The PGP-files case also shows how criminal investigation authorities and the judiciary are struggling with the absence of accurate rules and thus the legitimacy of the digital investigation methods. To begin with, this concerns the absence of rules on specific investigation methods. Due to the restricted interpretation of article 359a CCP (see above) the courts almost never attach a (serious) consequence to the fact that evidence was gathered illegally.[45] Next, there is the problem of territorial jurisdiction.[46] The PGP-data for instance, were owned by a Dutch company but stored on a Canadian server. This meant that 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 creatively interpreted the Dutch procedural rules. The defense objected, but in the end the trial judge authorized the course of action.[47]

41 See Koops 2018, p. 27

42 District Court of Amsterdam 19 April 2018, ECLI:NL:RBAMS:2018:2504.

43 See for example https://www.bbc.com/news/technology-35291933.

44 Dutch Forensic Institute.

45 See also B. Groothoff, 'An overview of the case law on smartphone searches', forthcoming.

46 See also in relation to investigation in the cloud: J.W. van den Hurk & S.J. 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', *Strafblad* 2019, p. 34–44.

47 See paragraph 6 of the verdict.

### 4.3 *Developments in Society and Technology Cause New Issues of Quality and Assessment of Evidence*

Technology has rapidly changed our society over the past decades. As a result, people are increasingly leaving digital traces everywhere all the time. Also, people are often monitored without being aware of it, not only by camera surveillance systems, but also 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 find out what happened in specific cases and to collect evidence. In the Netherlands, relatively many surveillance systems are in place for law enforcement to rely on. These are mostly private systems from which data are requested if needed.

The data we are referring to here is digital data, usually large amounts of data, in different formats (not only statistics, but also audio, video, etc.), that can only be accessed via technological devices. Although in the past forensic experts also provided technical data, such as fingerprints or ballistics, to criminal investigations and provided clarifications when testifying in courts, 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 of quality of evidence that arise as a result of the characteristics of digital data.

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 instance, 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 messed with. Even with such procedures and protocols in place, creating a copy of the data on a seized computer can be complicated. For instance, Bitcoins 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, a lot 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 article.[48]

The second issue concerns the large amounts of data that can become available during criminal investigations in relation to the principle that the litigating parties need to have access to all relevant data, incriminating and exonerating. For instance, in the Netherlands, law enforcement uses a lot of wiretapping, in order 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, for instance, 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.

Therefore, the large amounts of data collected in criminal cases call 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, a problem may be that humans may find it hard to follow how the software works, particularly when such tools are very advanced. If it is not transparent, however, how particular conclusions were drawn from the data, this could be an issue when such conclusions are used in courts as evidence. 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, but in the datasets there may also be exonerating pieces of evidence that the tools may not show.[49]

The third issue is related to difficulties in estimating the strength of the evidence. All datasets contain to some extent inaccurate data or gaps. Incorrect or incomplete data does not always need to be 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.[50] When

48 For more details, see, for instance, Oerlemans, J.J. (2017) Investigating Cybercrime, PhD thesis, Leiden University.

49 Calders T. & Custers B.H.M. (2013), What is data mining and how does it work?. In: Custers B.H.M., Calders T., Schermer B., Zarsky T. (red.) *Discrimination and Privacy in the Information Society.* nr. 3 Heidelberg: Springer.

50 Custers, B.H.M. (2003) *Effects of Unreliable Group Profiling by Means of Data Mining*. In: G. Grieser, Y. Tanaka and A. Yamamoto (eds.) *Lecture Notes in Artificial Intelligence, Proceedings of the 6th International Conference on Discovery Science* (*DS 2003*) Sapporo, Japan. Berlin, Heidelberg, New York: Springer-Verlag, Vol. 2843, p. 290–295.

based on large amounts of data, some minor errors and gaps in the data will hardly affect the final results. However, in case of limited data, errors might be crucial for the evidence. For instance, if cell phone data is used in a court case to prove that a suspect was at the crime scene at a particular time, this can be crucial. Say that 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, for instance, that the probability that the suspect can be pinpointed to the location is 75 %. This 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.[51]

Despite all these issues, the changing technological landscape does provide many opportunities for the use of data as evidence in courts. Typically, the use of data can be more objective than the use of statements from suspects, victims and witnesses. People may easily forget specific details of a past situation and their memories may even distort after some time. A lot of psychological mechanisms might be at play. In very stressful situations, when people are 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 that 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 fade over time for all actors.[52]

Objective data, for instance, on 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 it can disclose connections between people. It can prove that some statements are wrong or it can 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.

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.

51 Thompson, W.C., and Schuman, E.L. (1987) Interpretation of Statistical Evidence in Criminal Trials: The Prosecutor's Fallacy and the Defense Attorney's Fallacy, *Law and Human Behavior* 11, p. 167–187.

52 Odinot, G., Memon, A., La Rooy, D., Millen, A. (2013) Are Two Interviews Better Than One? Eyewitness Memory across Repeated Cognitive Interviews. PLoS ONE 8(10): e76305. https://doi.org/10.1371/journal.pone.0076305.

But this is only the case is some of the pitfalls and issues mentioned above are properly avoided. In general, we see an increase in the use of data as evidence in Dutch courts, but not necessarily a decrease in the use of statements from suspects, victims and witnesses. This is not to be expected any time soon, as statements remain important, also for other reasons than evidence only, such as 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 EU also 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. 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 in April 2018 new rules in the form of a Regulation and a Directive. Both proposals focus on swift and efficient cross-border access to e-evidence should be regulated, in order to effectively fight terrorism and other serious and organized crime.[53] The proposal for the directive focused on harmonized rules for appointing legal representatives when gathering evidence in criminal proceedings.[54] The proposal for the regulation focuses on European production and preservation orders for electronic evidence in criminal matters.[55] The production order will allow judicial authorities to obtain electronic evidence directly from services in other member states. These legal instruments have not yet been adopted by the EU, 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 EU over the next years.

## 5 Discussion and Conclusions

In this article, we focused on the question how the use of data as evidence in Dutch criminal courts is regulated and, considering how these courts deal with such data as evidence in practice, what is needed. There are two major legal frameworks, not fully integrated and adjusted to each other that regulate this: criminal law and data protection law. When it comes to regulating data as evidence, these frameworks together need to cover three separate but

53 https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/.

54 COM/2018/226 final – 2018/0107 (COD).

55 COM/2018/225 final – 2018/0108 (COD).

intertwined activities: 1) collection of data, 2) processing and analysis of data (storage, selecting, combining), and 3) evaluation of data. In the Netherlands, the 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 the developments in society and technology, we have four major observations, addressing the final part of our research question, i.e., what is needed. A first observation regarding regulation is that the existing legal framework in the Netherlands barely or not at all obstructs the collection of data for evidence. Although many digital investigation methods are not provided for in the CCP, and although, as a result, fundamental issues on privacy are debated, this seems to have little consequences for the legitimacy of data as evidence in specific cases. That 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.

In that respect it is interesting to see – this is our second observation – that regulation on collection (CCP) and regulation on processing and analysis (Wpg and Wjsg) is not integrated. The CCP is not specifically aimed at what can be done with data once they are 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 in another respect. 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 these rights and how to invoke them and, if they do, they may be blocked in case the criminal investigation is still ongoing.[56]

Our third observation concerns the absence of regulation of automated data analysis. Since automated data analysis raises fundamental questions regarding the equality of arms – all parties should have access to all relevant data and should be able to assess selection of data – 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,[57] but we did

56 Leiser, M.R. and Custers, B.H.M. (2019) The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, *European Data Protection Law Review*. Vol. 5, nr. 3, p. 367–378.

57 Custers B.H.M., Sears A.M., Dechesne F., Georgieva I.N., Tani T. & Hof S. van der (2019) *EU Personal Data Protection in Policy and Practice*. Heidelberg: Asser/Springer.

encounter an example of such a provision in the Dutch Intelligence Agencies Act (Wet Inlichtingen- en Veiligheidsdiensten, WIV). This act, in Article 60, 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 it should or should not be allowed to do this, but we would like to argue that there should be (more) clarity about this.

Finally, as a fourth observation, what may also need further attention is the level of expertise of courts in dealing with digital data as evidence. Given 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 it 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 on the basis of which judges can assess how data were seized.

Considering all 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 is, in practice, still 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. 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 further detailing actual practices and policies of law enforcement agencies. 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, regulating is considered for this. Regulation can be done via legislation, but perhaps also via policies. And, finally, further training of actors in courts may be required to make this all 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 next decades. Therefore, it is important to further prepare both courts and law enforcement agencies for this, 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 or witnesses, will become disused. We think it is important to consider the use of evidence in criminal courts as an addition to the use of statements and other types of evidence, not as a replacement. For humans seek to understand evidence by means of stories, which means that data always need to fit into a story – the stories of suspects, victims and witnesses.