Digital Information in Criminal Proceedings

The need to change laws on criminal procedure

dr. Bas de Wilde, LLM
dr. Anne de Hingh, LLM
prof. dr. Arno R. Lodder

Summary

Introduction

This report contains the results of research conducted by researchers of VU University Amsterdam as commissioned by the Research and Documentation Centre (Dutch: *Wetenschappelijk Onderzoek- en Documentatiecentrum*), based on the following main research question:

> *Which amendments are needed to laws on criminal procedure to ensure that one can in the future process and take cognizance of information from digital information products and the decisions based on them in the future?*

This research aims to contribute to the modernisation of the Dutch Code of Criminal Procedure. Criminal procedures are digitalised more and more. Information is more often available in a digital form and work processes are becoming increasingly more digital too. It is considered desirable to promote and advance digitalisation further. The modernised code should not constitute impediments to attain this goal. The Dutch Minister of Justice and Security has taken the position that the code should be as technology-neutral as possible. Our research has found an answer to the question whether the current Code of Criminal Procedure contains such obstacles and, if so, how they can be removed. However, not all aspects of criminal procedure have been examined. The research was based on the starting point that information becomes available during the criminal proceedings. This means, for instance, that the rules on investigative powers has not been taken into consideration. This research has focused on three main themes: (1) the forms that digital information can take, (2) the way in which digital information is processed and how one can take cognizance of such information, and (3) the use of digitally available information as evidence.

This report makes use of the terms information, information product and source material. 'Information' refers to data that can be given a certain meaning. 'Information product' is the term used for the format in which information can be recorded and examined, such as a paper document, a video or a digital file. The term 'source material' is used to refer to an information product that forms the basis for an official report or an expert opinion, such as a consignment of drugs or video footage.

In this report we present a vision for the year 2033. A future scenario has been described for various sub themes that is deemed to be realistic. The scenario is largely based on the current state of the art. It has been developed also using information collected through interviews with individuals from various organisations and professional fields. Six sub question have been answered, and these answers form the basis for the answer to the main research question. The sub questions will be dealt with below.

The research has been performed by examining literature, parliamentary documents, policy documents and court decisions, and by conducting interviews. We have interviewed a judge, an investigating judge, a criminal court clerk, a lawyer, two employees of Victim Support Netherlands, three experts in information technology, five staff members of the Dutch Public Prosecution Service, including three public prosecutors, and nine employees working in several police units.

Sub question 1: What is the current state of affairs in digitisation and digitalisation with regard to the creation, processing and reading of digital information products in criminal procedure?

This sub question is dealt with in chapter 2. The Dutch term 'digitalisering' has two meanings. First, it refers to the conversion of non-digital data into a digital format (*digitisation)*. Second, the word 'digitalisering' is used to describe the current development where the processing of information products is performed or supported by computers (*digitalisation*).

Information products, including official reports, are increasingly made available in a digital form. Some are *digital born*, others are digitised. Work processes are also more and more digitised. 90% of all case files are already available digitally. It must be noted here that digital case files are usually created by the (repeated) digitisation of information products. This also happens where information products are already available in a digital format. Digital files and digital information products are not stored in one central location. They are made available by their dispatch to the parties involved in the criminal procedure.

The cooperating organisations in criminal procedure are not yet making use of shared systems to a large extent. However, several projects have been initiated with the aim of creating work processes in the criminal justice system that allow the electronic sharing, exchanging, processing and reading of files and information products. Legislation has been introduced that enables further digitalisation of criminal procedure. For example, procedural actions could be taken in a digital manner – such as the submission of requests – and judicial notifications could be served or sent in a digital format.

The digitalisation of criminal justice has been a trend for several decades now, but it proves to be very slow-moving. This is mainly due to cultural differences and incompatible systems. It is important to put an end to the distribution of paper documents as soon as possible, and to the digitisation of documents that are already available in a digital form. A sense of urgency to bring digitalisation further is strongly felt by the cooperating organisations. Efficiency, quality improvement, time saving and the reduction of administrative burdens are important reasons to give high priority to digitalisation.

Sub question 2: Which fundamental rights, principles in criminal justice and interests must be taken into consideration when creating, processing and taking cognizance of digital information products?

This sub question is addressed in chapter 3. The preparation of files and the examination of documents involves personal data processing. In case processing is in the hands of judicial authorities or the police, Directive 2016/680 on the processing of personal data by judicial authorities and the police must be complied with, which directive was implemented by the Dutch Police Data Act (Dutch: *Wet politiegegevens*) and the Dutch Judicial Data and Criminal Records Act (Dutch: *Wet justitiële en strafvorderlijke gegevens*). As part of these acts it is specified which data can be processed and which party is responsible for this. Notable with respect to the provision of data is that some of the participants in the proceedings have the right to take cognizance of documents. On the part of the suspect, this right follows from the right to a fair trial (art. 6 ECHR). Additionally, EU regulations imply that victims also have the right to be informed about the criminal case.

Not only rights, but also principles in criminal justice, requirements and interests must be taken into consideration in the (further) digitalisation of criminal procedure. This includes the principle of legality, the importance of transparency and verifiability of government actions, the principle of immediacy, the principle of external publicity, the importance of diligent handling of criminal cases and the principle of careful decision-making.

Next to that, information-technical principles must be taken into account, such as the fact that data stored must be correct and complete, that the context within which information is relevant must be recorded, availability of information must be sustainable, data systems must be designed in accordance with requirements laid down by law and – in so far as possible and necessary – it must be possible to identify with certainty who the author or distributor of a specific information product is.

And finally, several other interests have been identified that cannot be neglected in further digitalisation: a clear and logical distribution of responsibilities for the processing of digital information products, the importance of an efficient use of capacities, sustainability and – of utmost importance – a design of data systems that corresponds as closely as possible with the needs of the users of that system.

Sub question 3: Which types of digital information products are available, in 2019 and in the future?

This sub question is covered in chapter 4. A distinction can be made between digitised information products and information products created digitally. Information products created in a digital form are referred to as *digital born* information products. An original paper version can also be digitised by means of a scan. This is, in fact, very common in current practice. A precondition for the use of *digital born* documents in case these documents must be signed, such as official reports, is that they can be signed electronically. Electronic signatures are allowed pursuant to articles 138e and 138f of the Dutch Code of Criminal Procedure. Limited use has so far been made of electronic signatures for official reports. This use includes both tablet signatures and electronic signatures that do not resemble hand drawn signatures. The Rotterdam District Court ruled that official reports signed in such a manner are compliant with statutory rules.

New technologies will be developed in the future. This may result in source material in new file formats. The forms that 'new' information products may take are however not expected to differ significantly from information products becoming available in 2019.

Sub question 4: How does the formation of criminal files take place, and how can one take cognizance of information products that are relevant for criminal proceedings, in 2019 and in the future?

This sub question is addressed in chapter 5. In current practice, a set of paper document forms the basis for a case file. Case files mainly consist of official records. This is the same in case of a digital case file, which usually contains a set of digitised (paper) documents. The original paper files are forwarded from, for instance, the police to the public prosecutor, and from the district court to the court of appeal, whilst being digitised in each step. All cooperating organisations within the criminal-law justice chain make use of their own data systems. Information products are however increasingly exchanged digitally.

Documents that must reasonably be considered to be relevant for the decision of the court, must in principle be defined as case documents and as such be added to the case file. It can be concluded from rulings of the Dutch Supreme Court that information products designated as source material do in principle not form part of the case file. The defence has the right to take cognizance of case documents. If a document is not a case document, the principle of due process of law may imply that the defence must be enabled to take cognizance of these documents anyway. In practice, lawyers and victims more and more often take cognizance of procedural documents through a web portal. Lawyers conducting a case before the Supreme Court can also take procedural actions through a web portal. Other organisations do not yet offer this option. It has been regulated by law that judicial notifications can be served or sent digitally, but this act has not yet entered into force.

In our vision of the future, all information products will be published on an Information Products Server (IPS). Parties specifically authorised to do so can take cognizance of information products through a link. The cooperating organisations use their own data systems if this is thought to be desirable in the performance of their duties. Next to these individual data systems, a data system will be set up to be used by all cooperating organisations, for both the compilation of case files and to support digital procedural actions and decisions. We refer to this system as the Central Facility for Criminal Proceedings (Dutch: *Centrale Voorziening Strafvordering*). This system will be used for the creation and management of case files. In deviation from current practice – in which case files are in principle dynamic sets of documents, as information can be added or removed during the criminal procedure – files will at a certain point in time have one fixed form only. This means that files will no longer be distributed.

From a technical point of view, a case file will consist of a set of links to information products in IPS. Files can be either investigation files or prosecution files. Investigation files will be used for the collection of results from ongoing investigations. Case files will be used to settle criminal cases and will consists of case documents. The scope of what is deemed to be a case document will be broader compared to the scope under current law. It includes all information products that are relevant for the assessment of a criminal case, in principle also including source materials that form the basis for official reports and expert reports.

The cooperating organisations take cognizance of the case file by logging on to the Central Facility for Criminal Proceedings in so far as they are authorised to do so. Others, including the suspect, victims, witnesses and their lawyers, can take cognizance of the case file through a web portal. All persons involved can log on to the same web portal. Not only case documents are made available through this web portal; it is also used for the service and dispatch of judicial notifications. Additionally, the portal can be used for procedural actions. All procedural actions, such as the calling of witnesses or the lodging of a legal remedy will be taken through the web portal. Dedicated staff at the Central Facility for Criminal Proceedings will take care of the compilation of case files. They will also ensure that procedural actions performed digitally will become available to the relevant decision-maker in a digital form. Once the decision-maker has taken a decision, it will be announced through the web portal to the party that has taken the procedural action.

Sub question 5: Under which conditions can criminal court judges use information products as evidence, in 2019 and in the future?

This sub question is dealt with in chapter 6. In the current situation, it is not always clear in which way certain digital material can be used as evidence. Moreover, the use of digital – and especially *digital born* – evidence that is not available in a written form is unnecessary complex under current statutory rules, as it can only serve as evidence based on the personal observation of the judge or as an appendix to an official report. It is therefore necessary to amend the rules concerning evidence. Adding one or several articles of evidence to the list to be used by the judge is not a solution. It has not proved possible to develop a definition of evidence that covers all digital evidence without creating a regulation that is excessively complex. Alternatively, the creation of an additional category of evidence will in any case be an only temporary solution. New technological developments will inevitably create the need to introduce new categories of evidence in the future, whereas the starting point of a technology-neutral code is that it is resistant to new developments. The categorisation of legal means of evidence is strongly connected to the form in which the court takes cognizance of the evidence. A technology-neutral code should focus not on the form, but on the substance of that evidence. We therefore conclude that it is necessary to no longer limit criminal courts to an exhaustive list of evidence.

It is not necessary to abandon the formal principle of immediacy altogether. We do however recommend to further qualify the rule from the Code of Criminal Procedure in which it is stipulated that material not submitted must be ignored in the decision of the court: this rule should only be applied if the interests of the suspect can be harmed by taking such material into consideration.

Sub question 6: Which digital information products can be produced by specific criminal cases in the future, how will these be processed and in which manner can parties involved in the criminal procedure take cognizance of such products?

This sub question is covered in chapter 7. The question is answered by the description of a fictitious criminal case taking place in the year 2033. It illustrates how investigation, prosecution, trial and execution of sentences take place, the types of information products these result in, how these information products are processed, in which way they come to the knowledge of others and in which way they can be used as evidence.

Main research question: the need to modernise the Dutch Code of Criminal Procedure

Chapter 8 provides an answer to the main research question. Current laws on criminal procedure contain only few obstacles for further digitalisation since the introduction of the Dutch Act on digital case documents in criminal proceedings (Dutch: *Wet digitale processtukken strafvordering*). Most of the Dutch Code of Criminal Procedure is technology-neutral. Case documents can be *digital born*, in which case it is important that the law allows electronic signing. Articles 138e and 138f of the Dutch Code of Criminal Procedure are however unclear about the question whether this applies to all types of documents. It is important for further digitalisation that there is no room for misunderstanding about the fact that all documents to be signed can be signed electronically. In order to create a technology-neutral code, a governmental decree can be used to stipulate that documents can be signed using an electronic signature, adding requirements to be met when making use of this option. The same can apply to the certification of documents.

It is unnecessary to replace the terms ‘document’, ‘case document’, ‘writing’ or ‘official record’, as these terms can be understood in such a manner that they also include digital

information products. This already happens in current practice. We do however recommend to replace the Dutch term 'bescheiden' by using 'writings' instead (Dutch: *geschriften*). 'Bescheiden' in normal usage refers to paper documents. Several legal provisions (art. 175 sub 1 and 204 of the Dutch Code of Civil Procedure) contain outdated provisions that can only refer to paper information products. These elements must be modernised. The verb 'to attach' (Dutch: *aanhechten*) can also be used in a digital context.

Article 149a sub 3 of the Dutch Code of Criminal Procedure stipulates that it must be possible to assess the integrity of digital case documents by tracking each change made therein. This requirement seems to imply, for instance, that an e-mail message copied into a pdf file cannot serve as a case document, as there is no guarantee that the pdf file is identical to the original e-mail. This cannot have been the intention of the legislator and it is undesirable to exclude this type of potential evidence. It is necessary to amend the code in such a way that this type of material is legally admissible as a case document.

Under the current Dutch Code of Criminal Procedure, it is already possible to a large extent to use a digital case file, consisting of digital documents stored in one location. This is however not the case for the lodging of legal remedies. In that case, the registry of the court must send the case file to another court (art. 409 sub 1 and 434 sub 1 of the Dutch Code of Criminal Procedure). In the event of a fully digital work process, a notification that a legal remedy has been exercised is sufficient. We consider the verbs 'to send' or 'to forward' to be inappropriate in case judicial notifications are served or sent digitally, as these notifications are in fact not 'sent', but the relevant individual is enabled to take cognizance of them.

The rules on case documents are unclear. It is necessary that a clear distinction is introduced in the Dutch Code of Criminal Procedure between documents and case documents on the one hand, and the case file on the other. A definition must be added on what is considered to be a case file. This definition must also clarify which party is responsible for its compilation during each phase of the criminal procedure. This is currently only clear for the criminal investigation phase. It must also be stipulated unambiguously which criteria are used to determine whether a document can be designated as a case document. Is that the case once it meets specific criteria, or once the public prosecutor has added it to a case file?

Article 149a sub 2 of the Dutch Code of Criminal Procedure must be amended. Under this provision, case documents are 'all documents that may reasonably be of importance for the decisions to be made by the court during the hearing'. The wording 'during the hearing' is infelicitous here. After all, documents to be considered case documents are in general not relevant for decisions taken by the court during the hearing, but for decisions taken after the court hearing has come to an end. The case file can moreover be important not only for decisions to be taken during the hearing, but also for other decisions, such as decisions in chambers, decisions taken by the investigating judge and a decision by the public prosecutor to issue a penalty order.

In our future scenario, source materials are in principle designated as case documents, in so far as these materials meet the relevance criterion. Under current legislation, this is generally not the case. We think it is advisable that all participants in the proceedings can take cognizance of the source materials that form the basis of official reports and expert reports, without any request being necessary. A broader scope could be realised by the introduction of a governmental decree (or explanatory notes to it) that defines which types of documents are case documents pursuant to the relevance criterion. In this context, we believe that it is important at all times that source material is

described and analysed by investigating officers or (other) experts. It is in our view not advisable to substitute, for instance, an official report of a witness examination by a recording of that same examination. Should the legislator however deem such desirable, it could be stipulated in legislation that specific events must be recorded in a report. Recording could in that case take place in both an audio (and video) report and in an official report.

If it is indicated that a specific procedural action can be taken using electronic means, it can be performed digitally under current law only if a special provision has been laid down in a governmental decree. It is necessary to amend criminal procedural law in this respect, as it can be interpreted in such a way that, for example, a suspect cannot submit any requests by e-mail, given the fact that article 36e of the Dutch Code of Criminal Procedure stipulates that such requests can be made electronically whereas no specific provision has been designated yet.

Additionally, the rules on the performance of procedural actions by electronic means are limited to procedural actions performed by suspects and victims. It is necessary that explicit provisions are added to the Dutch Code of Criminal Procedure, stating that procedural actions in general can be conducted electronically.

In the Dutch Code of Criminal Procedure, provisions on the right to take cognizance of (case) documents are technology-neutral. However, there are no statutory rules on web portals through which (case) documents can be read, such as the portal for lawyers and the portal for victims, which are both already operational. As these portals involve privacy-sensitive information products, it is our opinion that legal guarantees must also apply to web portals only meant for the publication of information products. The web portal of the future can be used for both reading and uploading information products. Rules relating to this must be laid down in a governmental decree.

The defence should be able to receive copies of most case documents. The term ‘copy’ is sufficiently appropriate for the digital work processes we have described. Article 126a of the Dutch Code of Criminal Procedure stipulates that a copy of an authorisation must be shown before a criminal financial investigation can be conducted. If, in a digital working environment, a smartphone is used to log on to a data system in which the original (*digital born*) authorisation is saved, there is no question of a copy of that authorisation being shown; it is the original. The legal stipulation must therefore be formulated in a more technology-neutral manner.

Article 32 of the Dutch Code of Criminal Procedure indicates that the suspect can receive a copy of documents ‘at the public prosecutor’s office or at the court registry’. When documents are made available digitally through a web portal or by e-mail, no location needs to be mentioned here. It is even unnecessarily restrictive. It must be noted here that even when working with paper documents, it is not necessary to mention a specific location. And finally, the submission of a copy (art. 126a sub 4 of the Dutch Code of Criminal Procedure) is not very technology-neutral, as this term implies that a physical copy must be submitted.

In the future, judicial notifications, such as summons, notices to appear and court decisions, will in principle be submitted electronically through a web portal. The current Dutch Code of Criminal Procedure does not rule out the electronic service or dispatch of documents. Once the ‘Reviewed Enforcement of Criminal Law Decisions Act’ (Dutch: *Wet herziening tenuitvoerlegging strafrechtelijke beslissingen*) will have fully entered into force, the Dutch Code of Criminal Procedure must provide for specific stipulations on the digital service of judicial notifications. This will result in a code that is not completely technology-neutral, as specific acts will be defined that can be performed in a digital manner. We therefore believe that it is necessary to amend the relevant

provision. In this context, we think there are two other elements that require a legislative change. First, it is necessary to remove the suggestion that information products can only be sent digitally if this is stated explicitly in the provision containing obligations on dispatch. Second, it must be made clear that information products, including (copies of) judicial notifications, can be exchanged between government officials in a digital manner.

In order to create a technology-neutral code, it is necessary to lay down rules specifically relating to digital aspects in a governmental decree, also including requirements on digital case files. This in any case involves the technological requirements for the system, the parties authorised to take cognizance of information products or to add documents, the way in which access is given to the system and the responsibility for the system as a whole. The decree can also stipulate that procedural actions may be performed electronically, and in which manner. As far as we are concerned, all aspects of criminal procedure in the field of digitalisation may be laid down in a governmental decree, whether they relate to digital case documents, electronic signatures, digital case files, procedural actions performed digitally or the digital service of documents. This would allow for a technology-neutral text of the provisions in the Dutch Code of Criminal Procedure.

To ensure a sustainable and technology-neutral code of criminal procedure, it is necessary that the trial judge in his ruling on the evidence is no longer bound to an exhaustive list of legal means of evidence. This requires significant amendments to the rules concerning evidence. The enumeration of legal means of evidence under article 339 of the Dutch Code of Criminal Procedure can be removed. Some of the conditions on evidence to be used in decisions can be transformed into prohibitions on the use of articles of evidence. Should the legislator decide to maintain the obligations relating to legal means of evidence, it is necessary to expand the list of legal means of evidence, so as to ensure that digital evidence can contribute to decision-making without the necessity of showing it during the hearing and without the obligation to transform the articles of evidence into writing. In that case, it is also necessary to replace the article of evidence referred to as ‘written document’ by ‘document’, in order to make it unambiguously clear that digital documents also fall under the definition of this article of evidence. And finally, we are of the opinion that it is still of great importance that evidence is discussed during the hearing. The principle of immediacy must therefore be upheld.

Recommendations

We make the following five recommendations.

1. *Invest in culture*
   The digitalisation process is not progressing at the desirable pace. This may have several causes. An important cause is the existence of cultural differences between the cooperating organisations. For further digitalisation to become successful, it is important that investments are made in mutual relationships inside the criminal justice system. We therefore recommend to have research carried out into the reasons why joint initiatives do not come off the ground.

2. *Give the Minister of Justice and Security responsibility for the Central Facility for Criminal Proceedings and the Information Products Server*

   We have suggested to enable all cooperating organisations to work in one data system, referred to as the Central Facility for Criminal Proceedings. We have also suggested to save all (digital) information products in one central location, referred to as the Information Products Server (IPS). Given the cultural differences that we have identified, there is a much greater chance that the Central Facility and the IPS are indeed realised if the responsibility for the design of the system is not given to the parties responsible for the processing of data, but to the party responsible for criminal procedure in general: the Minister of Justice and Security.

3. *Create one act on the processing of police and criminal-law personal data*

   It is very difficult to tell which rules from which act apply to which kind of information. When using the Central Facility for Criminal Proceedings, all data are saved in one central location. These data can in principle be examined using any computer and a (secure) internet connection. Various cooperating organisations will be able to upload and read documents. It is therefore recommendable to create one act on the processing of personal data for the entire criminal justice system.

4. *Include general provisions in the new code relating to the conditions applicable to procedural actions and decisions*

   The current Dutch Code of Criminal Procedure contains conditions to be met by many types of procedural actions and decisions. These have been defined for each of those actions and decisions separately. However, the act does not contain any conditions on several other (and sometimes similar) procedural actions and decisions. We recommend that general provisions be included in the code with conditions to be met by procedural actions and decisions. For instance, it can be stipulated that all decisions made by judges must be laid down in writing, signed, dated and substantiated.

5. *Include a general provision in the new code on the joinder of documents in the case file*

   In the current Dutch Code of Criminal Procedure, it is stipulated in various instances that specific documents must be added to the case file. However, most documents are not subject to any such stipulations. Specific provisions on this can be missed here. It is sufficient to include one general provision, based on which all case documents must be added to the case file.